

Guía de administración del sistema: servicios IP

Copyright © 1999, 2010, Oracle y/o sus subsidiarias. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comuniqué por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera licencias en nombre del Gobierno de EE.UU. se aplicará la siguiente disposición:

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus subsidiarias declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus subsidiarias. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden ofrecer acceso a contenidos, productos o servicios de terceros o información sobre los mismos. Ni Oracle Corporation ni sus subsidiarias serán responsables de ofrecer cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros y renuncian explícitamente a ello. Oracle Corporation y sus subsidiarias no se harán responsables de las pérdidas, los costos o los daños en los que se incurra como consecuencia del acceso o el uso de contenidos, productos o servicios de terceros.

Copyright © 1999, 2010, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.

Contenido

Prefacio	29
 Parte I Introducción a la administración del sistema: servicios IP	 35
1 Conjunto de protocolos TCP/IP de Oracle Solaris (descripción general)	37
Novedades de esta versión	37
Introducción al conjunto de protocolos TCP/IP	37
Capas de protocolo y el modelo de Interconexión de Sistemas Abiertos	38
Modelo de arquitectura del protocolo TCP/IP	39
Cómo manejan las comunicaciones de datos los protocolos TCP/IP	45
Encapsulado de datos y la pila de protocolo TCP/IP	45
Admisión de seguimiento interno de TCP/IP	49
Información adicional sobre TCP/IP e Internet	49
Manuales sobre TCP/IP	49
Páginas web sobre TCP/IP y redes	49
Petición de comentarios y borradores de Internet	50
 Parte II Administración de TCP/IP	 51
2 Planificación de la red TCP/IP (tareas)	53
Planificación de la red (mapa de tareas)	53
Determinación del hardware de red	55
Cómo decidir el formato de las direcciones IP para la red	55
Direcciones IPv4	56
Direcciones IPv4 en formato CIDR	56
Direcciones DHCP	57
Direcciones IPv6	57

Direcciones privadas y prefijos de documentación	57
Cómo obtener el número de IP de la red	58
Cómo diseñar un esquema de direcciones IPv4	58
Cómo diseñar un esquema de direcciones IPv4	60
Número de subred IPv4	61
Cómo diseñar un esquema de direcciones IPv4 CIDR	61
Uso de direcciones IPv4 privadas	62
Aplicación de las direcciones IP a las interfaces de red	63
Entidades de denominación en la red	63
Administración de nombres de host	64
Selección de un servicio de nombres y de directorios	64
Planificación de enrutadores en la red	66
Descripción general de la topología de red	66
Cómo transfieren los paquetes los enrutadores	68
3 Introducción a IPv6 (descripción general)	71
Características principales de IPv6	72
Direcciones ampliadas	72
Configuración automática de direcciones y descubrimiento de vecinos	72
Simplificación del formato del encabezado	72
Más posibilidades en las opciones de encabezado de IP	73
Compatibilidad de aplicaciones con direcciones IPv6	73
Otros recursos de IPv6	73
Descripción general de las redes IPv6	74
Descripción general de las direcciones IPv6	76
Partes de una dirección IPv6	77
Abreviación de direcciones IPv6	78
Prefijos de IPv6	78
Direcciones unidifusión	79
Direcciones multidifusión	81
Grupos y direcciones de difusión por proximidad	82
Descripción general del protocolo ND de IPv6	82
Configuración automática de direcciones IPv6	83
Descripción general de configuración automática sin estado	84
Descripción general sobre los túneles de IPv6	85

4 Planificación de una red IPv6 (tareas)	87
Planificación de IPv6 (mapas de tareas)	87
Situación hipotética de topología de red IPv6	88
Preparación de la red ya configurada para admitir IPv6	90
Preparación de la topología red para admitir IPv6	90
Preparación de servicios de red para admitir IPv6	91
Preparación de servidores para admitir IPv6	91
▼ Cómo preparar servicios de red para admitir IPv6	92
▼ Cómo preparar DNS para admitir IPv6	92
Planificación de túneles en la topología de red	93
Aspectos relacionados con la seguridad en la implementación de IPv6	94
Preparación de un plan de direcciones IPv6	94
Obtención de un prefijo de sitio	94
Creación del esquema de numeración de IPv6	95
5 Configuración de servicios de red TCP/IP y direcciones IPv4 (tareas)	97
Novedades de este capítulo	98
Antes de configurar una red IPv4 (mapa de tareas)	98
Cómo determinar los modos de configuración de host	99
Sistemas que deben ejecutarse en modo de archivos locales	99
Sistemas que son clientes de red	101
Configuraciones mixtas	101
Situación hipotética de topología de red IPv4	101
Cómo agregar una subred a una red (mapa de tareas)	102
Mapa de tareas de configuración de red	103
Configuración de sistemas en la red local	104
▼ Cómo configurar un host para el modo de archivos locales	105
▼ Cómo instalar un servidor de configuración de red	107
Configuración de clientes de red	109
▼ Cómo configurar hosts para el modo de cliente de red	109
▼ Cómo cambiar la dirección IPv4 y otros parámetros de configuración de red	110
Reenvío de paquetes y rutas en redes IPv4	114
Protocolos de enrutamiento admitidos por Oracle Solaris	115
Topología de sistemas autónomos IPv4	118
Configuración de un enrutador IPv4	121

Tablas y tipos de enrutamiento	126
Configuración de hosts múltiples	129
Configuración del enrutamiento para sistemas de interfaz única	132
Supervisión y modificación de los servicios de capa de transporte	137
▼ Cómo registrar las direcciones IP de todas las conexiones TCP entrantes	137
▼ Cómo agregar servicios que utilicen el protocolo SCTP	138
▼ Cómo utilizar los envoltorios TCP para controlar el acceso a los servicios TCP	141
6 Administración de interfaces de red (tareas)	143
Novedades en la administración de interfaces de red	143
Administración de interfaces (mapa de tareas)	144
Aspectos básicos sobre la administración de interfaces físicas	145
Nombres de interfaz de red	145
Conexión de una interfaz	146
Tipos de interfaz de Oracle Solaris	146
Administración de interfaces de red individuales	146
▼ Cómo obtener el estado de una interfaz	147
▼ Cómo configurar una interfaz física tras la instalación del sistema	148
▼ Cómo eliminar una interfaz física	152
▼ SPARC: Cómo asegurarse de que la dirección MAC de una interfaz sea única	152
Administración de redes de área local virtuales	154
Descripción general de una configuración VLAN	154
Planificación de una red para redes VLAN	157
Configuración de redes VLAN	158
Descripción general de agregaciones de vínculos	160
Conceptos básicos de agregaciones de vínculos	160
Agregaciones de vínculos de extremo a extremo	162
Directivas y equilibrio de la carga	163
Modo de agregación y nodos	163
Requisitos para agregaciones de vínculos	164
▼ Cómo crear una agregación de vínculos	164
▼ Cómo modificar una agregación	166
▼ Cómo eliminar una interfaz de una agregación	167
▼ Cómo eliminar una agregación	168
▼ Cómo configurar VLAN a través de una adición de vínculos	169

7 Configuración de una red IPv6 (tareas).	171
Configuración de una interfaz de IPv6	171
Habilitación de IPv6 en una interfaz (mapa de tareas)	172
▼ Cómo habilitar una interfaz de IPv6 para la sesión actual	172
▼ Cómo habilitar interfaces de IPv6 de manera permanente	174
▼ Cómo desactivar la configuración automática de direcciones IPv6	176
Configuración de un enrutador IPv6	177
Configuración de IPv6 en enrutadores (mapa de tareas)	177
▼ Cómo configurar un enrutador habilitado para IPv6	178
Modificación de la configuración de una interfaz de IPv6 para hosts y servidores	181
Modificación de la configuración de una interfaz de IPv6 (mapa de tareas)	181
Uso de direcciones temporales para una interfaz	182
Configuración de un token IPv6	185
Administración de interfaces habilitadas para IPv6 en servidores	188
Tareas de configuración de túneles para compatibilidad con IPv6 (mapa de tareas)	189
Configuración de túneles para compatibilidad con IPv6	190
▼ Cómo configurar manualmente IPv6 a través de túneles IPv4	190
▼ Cómo configurar manualmente túneles IPv6 a través de IPv6	191
▼ Cómo configurar túneles IPv4 a través de IPv6	192
▼ Cómo configurar un túnel 6to4	192
▼ Cómo configurar un túnel 6to4 hasta un enrutador de reenvío 6to4	196
Configuración de la compatibilidad con el servicio de nombres para IPv6	198
▼ Cómo agregar direcciones IPv6 a DNS	198
Adición de direcciones IPv6 a NIS	199
▼ Cómo visualizar información sobre servicios de nombres de IPv6	199
▼ Cómo verificar que los registros PTR de DNS IPv6 se actualicen correctamente	200
▼ Cómo visualizar información de IPv6 mediante NIS	201
▼ Cómo visualizar información relativa a IPv6 al margen del servicio de nombres	201
8 Administración de redes TCP/IP (tareas)	203
Tareas de administración principales de TCP/IP (mapa de tareas)	204
Supervisión de la configuración de interfaz con el comando <code>ifconfig</code>	205
▼ Cómo obtener información sobre una interfaz específica	205
▼ Cómo mostrar asignaciones de dirección de interfaz	207
Supervisión del estado de la red con el comando <code>netstat</code>	209

▼ Cómo visualizar estadísticas por protocolo	209
▼ Cómo visualizar el estado de protocolos de transporte	211
▼ Cómo visualizar el estado de interfaces de red	212
▼ Cómo visualizar el estado de los sockets	212
▼ Cómo visualizar el estado de las transmisiones de paquetes de un determinado tipo de dirección	214
▼ Cómo visualizar el estado de rutas conocidas	215
Sondeo de hosts remotos con el comando ping	216
▼ Cómo determinar si un host remoto está en ejecución	216
▼ Cómo determinar si un host descarta paquetes	216
Administración y registro de la visualización del estado de la red	217
▼ Cómo controlar la salida de visualización de comandos relacionados con IP	217
▼ Cómo registrar acciones del daemon de rutas de IPv4	218
▼ Cómo efectuar el seguimiento de las actividades del daemon de descubrimiento cercano de IPv6	219
Visualización de información de enrutamiento con el comando traceroute	220
▼ Cómo saber la ruta de un host remoto	220
▼ Cómo efectuar el seguimiento de todas las rutas	221
Control de transferencias de paquetes con el comando snoop	221
▼ Cómo comprobar paquetes de todas las interfaces	222
▼ Cómo capturar salida del comando snoop en un archivo	223
▼ Cómo comprobar paquetes entre un cliente y un servidor IPv4	224
▼ Cómo supervisar tráfico de redes IPv6	224
Administración de selección de direcciones predeterminadas	225
▼ Cómo administrar la tabla de directrices de selección de direcciones IPv6	225
▼ Cómo modificar la tabla de selección de direcciones IPv6 sólo para la sesión actual	227
9 Resolución de problemas de red (Tareas)	229
Novedades de Resolución de problemas de red	229
Consejos de resolución de problemas de red generales	229
Ejecución de comprobaciones de diagnóstico básicas	230
▼ Cómo realizar comprobaciones de software de red básicas	230
Problemas comunes al utilizar IPv6	231
El enrutador IPv4 no puede actualizarse a IPv6	231
Problemas tras la actualización de servicios a IPv6	231
El ISP actual no admite IPv6	231

Cuestiones de seguridad al transmitir datos mediante túnel a un enrutador de reenvío 6to4	232
10 Descripción detallada de TCP/IP e IPv4 (referencia)	233
Novedades de TCP/IP e IPv4	233
Archivos de configuración TCP/IP	233
Archivo <code>/etc/hostname.interfaz</code>	234
Archivo <code>/etc/nodename</code>	235
Archivo <code>/etc/defaultdomain</code>	235
Archivo <code>/etc/defaultrouter</code>	235
Base de datos <code>hosts</code>	235
Base de datos <code>ipnodes</code>	239
Base de datos <code>netmasks</code>	240
Daemon de servicios de Internet <code>inetd</code>	244
Bases de datos de red y el archivo <code>nsswitch.conf</code>	244
Cómo afectan los servicios de nombres a las bases de datos de red	245
Archivo <code>nsswitch.conf</code>	247
Base de datos <code>bootparams</code>	249
Base de datos <code>ethers</code>	250
Otras bases de datos de red	251
Base de datos <code>protocols</code>	252
Base de datos <code>services</code>	252
Protocolos de enrutamiento en Oracle Solaris	253
Protocolo Routing Information Protocol (RIP)	253
Protocolo ICMP Router Discovery (RDISC)	254
Clases de red	254
Números de red de clase A	254
Números de red de clase B	255
Números de red de clase C	255
11 IPv6 en profundidad (referencia)	257
Novedades de IPv6 en profundidad	257
Formatos de direcciones IPv6 que no son los básicos	258
Direcciones 6to4 derivadas	258
Direcciones multidifusión IPv6 en profundidad	260

Formato del encabezado de los paquetes de IPv6	261
Encabezados de extensión de IPv6	262
Protocolos de pila doble	263
Oracle Solaris implementación de IPv6	263
Archivos de configuración de IPv6	264
Comandos relacionados con IPv6	269
Daemons relacionados con IPv6	275
Protocolo ND de IPv6	278
Mensajes de ICMP del protocolo ND	278
Proceso de configuración automática	279
Solicitud e inasequibilidad de vecinos	281
Algoritmo de detección de direcciones duplicadas	281
Anuncios de proxy	282
Equilibrio de la carga entrante	282
Cambio de dirección local de vínculo	282
Comparación del protocolo ND con ARP y protocolos relacionados con IPv4	283
Encaminamiento de IPv6	284
Anuncio de enrutador	285
Túneles de IPv6	286
Túneles configurados	288
Túneles automáticos 6to4	290
Extensiones de IPv6 para servicios de nombres de Oracle Solaris	295
Extensiones de DNS para IPv6	295
Cambios en el archivo <code>nsswitch.conf</code>	296
Cambios en los comandos de servicio de nombres	297
Admisión de NFS y RPC IPv6	297
Admisión de IPv6 en ATM	298
 Parte III DHCP	 299
 12 Acerca de DHCP (descripción general)	 301
Acerca del Protocolo DHCP	301
Ventajas del uso de DHCP	302
Funcionamiento de DHCP	303
El servidor DHCP	306

Administración del servidor DHCP	307
Almacén de datos de DHCP	307
Administrador de DHCP	309
Utilidades de la línea de comandos de DHCP	310
Control de acceso basado en roles para los comandos DHCP	311
Configuración del servidor DHCP	311
Asignación de direcciones IP	312
Información de configuración de red	312
Acerca de las opciones DHCP	313
Acerca de macros DHCP	313
El cliente DHCP	315
13 Planificación del servicio DHCP (tareas)	317
Preparación de la red para el servicio DHCP (mapa de tareas)	317
Asignación de topología de red	318
Cómo determinar el número de servidores DHCP	319
Actualización de archivos de sistema y tablas de máscara de red	320
Toma de decisiones para la configuración del servidor DHCP (mapa de tareas)	322
Selección de un host para ejecutar el servicio DHCP	322
Selección del almacén de datos DHCP	323
Configuración de una directiva de permiso	324
Cómo determinar los enrutadores para clientes DHCP	325
Toma de decisiones para la administración de direcciones IP (mapa de tareas)	325
Número e intervalos de direcciones IP	326
Generación de nombres de host de cliente	326
Macros de configuración de cliente predeterminadas	327
Tipos de permiso dinámico y permanente	328
Tipos de permisos y direcciones IP reservadas	328
Planificación de múltiples servidores DHCP	329
Planificación de la configuración DHCP de las redes remotas	330
Selección de la herramienta para configurar DHCP	330
Funciones del Administrador de DHCP	330
Funciones de dhcpconfig	331
Comparación del Administrador de DHCP y dhcpconfig	331

14 Configuración del servicio DHCP (tareas)	333
Configuración y desconfiguración de un servidor DHCP utilizando el Administrador de DHCP	333
Configuración de servidores DHCP	334
▼ Cómo configurar un servidor DHCP (Administrador de DHCP)	337
Configuración de los agentes de reenvío de BOOTP	338
▼ Cómo configurar un agente de reenvío de BOOTP (Administrador de DHCP)	338
Desconfiguración de servidores DHCP y agentes de reenvío de BOOTP	339
Datos DHCP en un servidor desconfigurado	340
▼ Cómo desconfigurar un servidor DHCP o un agente de reenvío de BOOTP (Administrador de DHCP)	341
Configuración y desconfiguración de un servidor DHCP mediante los comandos dhcpconfig	341
▼ Cómo configurar un servidor DHCP (dhcpconfig -D)	342
▼ Cómo configurar un agente de reenvío de BOOTP (dhcpconfig -R)	343
▼ Cómo desconfigurar un servidor DHCP o un agente de reenvío de BOOTP (dhcpconfig -U)	343
15 Administración de DHCP (tareas)	345
Acerca del Administrador de DHCP	346
Ventana del Administrador de DHCP	346
Menús del Administrador de DHCP	348
Cómo iniciar y detener el Administrador de DHCP	348
▼ Cómo iniciar y detener el Administrador de DHCP	348
Configuración del acceso de usuario a los comandos de DHCP	349
▼ Cómo conceder a los usuarios acceso a los comandos de DHCP	349
Cómo iniciar y detener el servicio DHCP	350
▼ Cómo iniciar y detener el servicio DHCP (Administrador de DHCP)	351
▼ Cómo habilitar e inhabilitar el servicio DHCP (Administrador de DHCP)	351
▼ Cómo habilitar e inhabilitar el servicio DHCP (dhcpconfig -S)	351
Servicio DHCP y Utilidad de gestión de servicios	352
Modificación de las opciones del servicio DHCP (mapa de tareas)	353
Cómo cambiar las opciones de registro de DHCP	355
▼ Cómo generar mensajes de registro DHCP detallados (Administrador de DHCP)	357
▼ Cómo generar mensajes de registro DHCP detallados (línea de comandos)	357
▼ Cómo habilitar e inhabilitar el registro de transacciones DHCP (Administrador de	

DHCP)	358
▼ Cómo habilitar e inhabilitar el registro de transacciones DHCP (línea de comandos)	359
▼ Cómo registrar transacciones DHCP en un archivo syslog independiente	359
Habilitación de las actualizaciones DNS dinámicas por parte del servidor DHCP	360
▼ Cómo activar la actualización de DNS dinámica para los clientes DHCP	361
Registro de nombres de host de cliente	362
Personalización de las opciones de rendimiento del servidor DHCP	363
▼ Cómo personalizar las opciones de rendimiento DHCP (Administrador de DHCP)	364
▼ Cómo personalizar las opciones de rendimiento DHCP (línea de comandos)	365
Cómo agregar, modificar y eliminar redes DHCP (mapa de tareas)	366
Especificación de interfaces de redes para la supervisión de DHCP	367
▼ Cómo especificar interfaces de red para la supervisión de DHCP (Administrador de DHCP)	368
▼ Cómo especificar las interfaces de red para la supervisión de DHCP (dhcpconfig)	368
Cómo agregar redes DHCP	369
▼ Como agregar una red DHCP (Administrador de DHCP)	370
▼ Cómo agregar una red DHCP (dhcpconfig)	371
Modificación de configuraciones de redes DHCP	371
▼ Cómo modificar la configuración de una red DHCP (Administrador de DHCP)	372
▼ Cómo modificar la configuración de una red DHCP (dhtadm)	373
Eliminación de redes DHCP	374
▼ Cómo eliminar una red DHCP (Administrador de DHCP)	375
▼ Cómo eliminar una red DHCP (pntadm)	375
Clientes BOOTP con el servicio DHCP (mapa de tareas)	376
▼ Cómo configurar la compatibilidad de cualquier cliente BOOTP (Administrador de DHCP)	377
▼ Cómo configurar la compatibilidad de los clientes BOOTP registrados (Administrador de DHCP)	378
Uso de direcciones IP en el servicio DHCP (mapa de tareas)	379
Cómo agregar direcciones IP al servicio DHCP	383
▼ Cómo agregar una única dirección IP (Administrador de DHCP)	385
▼ Cómo duplicar una dirección IP existente (Administrador de DHCP)	385
▼ Cómo agregar varias direcciones IP (Administrador de DHCP)	386
▼ Cómo agregar direcciones IP (pntadm)	386
Modificación de direcciones IP en el servicio DHCP	387
▼ Cómo modificar las propiedades de direcciones IP (Administrador de DHCP)	388

▼ Cómo modificar las propiedades de direcciones IP (pntadm)	389
Eliminación de direcciones IP del servicio DHCP	389
Cómo marcar direcciones IP como inutilizables para el servicio DHCP	390
▼ Cómo marcar direcciones IP como no utilizables (Administrador de DHCP)	390
▼ Cómo marcar direcciones IP como inutilizables (pntadm)	391
Eliminación de direcciones IP del servicio DHCP	391
▼ Cómo eliminar direcciones IP del servicio DHCP (Administrador de DHCP)	392
▼ Cómo eliminar direcciones IP del servicio DHCP (pntadm)	392
Asignación de una dirección IP reservada a un cliente DHCP	393
▼ Cómo asignar una dirección IP coherente a un cliente DHCP (Administrador de DHCP)	394
▼ Cómo asignar una dirección IP coherente a un cliente DHCP (pntadm)	395
Cómo usar macros DHCP (mapa de tareas)	395
▼ Cómo visualizar las macros definidas en un servidor DHCP (Administrador de DHCP)	397
▼ Cómo ver las macros definidas en un servidor DHCP (dhtadm)	398
Modificación de macros DHCP	398
▼ Cómo cambiar los valores de las opciones en una macro DHCP (Administrador de DHCP)	399
▼ Cómo cambiar los valores de las opciones en una macro DHCP (dhtadm)	400
▼ Cómo agregar opciones a una macro DHCP (Administrador de DHCP)	400
▼ Cómo agregar opciones a una macro DHCP (dhtadm)	401
▼ Como eliminar opciones de una macro DHCP (Administrador de DHCP)	402
▼ Como eliminar opciones de una macro DHCP (dhtadm)	402
Creación de macros DHCP	403
▼ Cómo crear una macro DHCP (Administrador de DHCP)	403
▼ Cómo crear una macro DHCP (dhtadm)	404
Eliminación de macros DHCP	405
▼ Cómo eliminar una macro DHCP (Administrador de DHCP)	405
▼ Cómo eliminar una macro DHCP (dhtadm)	406
Uso de opciones DHCP (mapa de tareas)	406
Creación de opciones DHCP	409
▼ Cómo crear opciones DHCP (Administrador de DHCP)	410
▼ Cómo crear opciones DHCP (dhtadm)	411
Modificación de opciones DHCP	412
▼ Cómo modificar las propiedades de opciones DHCP (Administrador de DHCP)	412
▼ Cómo modificar las propiedades de opciones DHCP (dhtadm)	413

Eliminación de opciones DHCP	414
▼ Cómo eliminar opciones DHCP (Administrador de DHCP)	414
▼ Cómo eliminar opciones DHCP (dhtadm)	415
Modificar la información de opciones de cliente DHCP	415
Instalación en red de Oracle Solaris con el servicio DHCP	415
Inicio remoto y clientes de inicio sin disco (mapa de tareas)	416
Configuración de clientes DHCP sólo para recibir información (mapa de tareas)	418
Conversión a un nuevo almacén de datos DHCP	418
▼ Cómo convertir el almacén de datos DHCP (Administrador de DHCP)	420
▼ Cómo convertir el almacén de datos DHCP (dhcpconfig -C)	421
Transferencia de datos de configuración entre servidores DHCP (mapa de tareas)	421
▼ Cómo exportar datos de un servidor DHCP (Administrador de DHCP)	424
▼ Cómo exportar datos de un servidor DHCP (dhcpconfig -X)	424
▼ Cómo importar datos en un servidor DHCP (Administrador de DHCP)	426
▼ Cómo importar datos en un servidor DHCP (dhcpconfig -I)	426
▼ Cómo modificar datos de DHCP importados (Administrador de DHCP)	427
▼ Cómo modificar datos DHCP importados (pntadm, dhtadm)	428
16 Configuración y administración del cliente DHCP	429
Acerca del cliente DHCP	429
Servidor DHCPv6	430
Diferencias entre DHCPv4 y DHCPv6	430
El modelo administrativo	430
Detalles del protocolo	432
Interfaces lógicas	432
Negociación de opciones	433
Sintaxis de configuración	433
Inicio de cliente DHCP	434
Comunicación con DHCPv6	434
Cómo gestionan los protocolos del cliente DHCP la información de configuración de red	435
Cierre del cliente DHCP	437
Activación y desactivación de un cliente DHCP	437
▼ Cómo habilitar el cliente DHCP	437
▼ Cómo deshabilitar un cliente DHCP	438

Administración del cliente DHCP	439
Opciones del comando <code>ifconfig</code> que se utilizan con el cliente DHCP	439
Asignación de los parámetros de configuración del cliente DHCP	440
Sistemas cliente DHCP con varias interfaces de red	441
Nombres de host de cliente DHCPv4	442
▼ Cómo habilitar un cliente DHCPv4 para que solicite un nombre de host específico	443
Sistemas cliente DHCP y servicios de nombres	443
Configuración de clientes DHCP como clientes NIS+	445
Secuencias de eventos de cliente DHCP	448
17 Solución de problemas de DHCP (referencia)	453
Solución de problemas del servidor DHCP	453
Problemas de NIS+ y el almacén de datos DHCP	453
Errores de asignación de dirección IP en DHCP	457
Solución de problemas de configuración del cliente DHCP	459
Problemas de comunicación con el servidor DHCP	460
Problemas por información de configuración DHCP incorrecta	468
Problemas con el nombre de host proporcionado por el cliente DHCP	469
18 Comandos y archivos DHCP (referencia)	473
Comandos DHCP	473
Ejecución de comandos DHCP en secuencias	474
Archivos que utiliza el servicio DHCP	480
Información de opciones DHCP	482
Cómo determinar si su sitio se ve afectado	482
Diferencias entre los archivos <code>dhcptags</code> e <code>inittab</code>	483
Conversión de entradas de <code>dhcptags</code> en entradas de <code>inittab</code>	484
Parte IV Seguridad IP	485
19 Arquitectura de seguridad IP (descripción general)	487
Novedades de IPsec	487
Introducción a IPsec	489
RFC IPsec	490

Terminología de IPsec	490
Flujo de paquetes IPsec	491
Asociaciones de seguridad IPsec	494
Administración de claves en IPsec	494
Mecanismos de protección de IPsec	495
Encabezado de autenticación	496
Carga de seguridad encapsuladora	496
Algoritmos de autenticación y cifrado en IPsec	497
Directivas de protección IPsec	499
Modos de transporte y túnel en IPsec	499
Redes privadas virtuales e IPsec	502
Paso a través de IPsec y NAT	503
IPsec y SCTP	504
IPsec y Zonas de Solaris	504
IPsec y dominios lógicos	504
Archivos y utilidades IPsec	505
Cambios en IPsec para la versión Solaris 10	507
20 Configuración de IPsec (tareas)	509
Protección del tráfico con IPsec (mapa de tareas)	509
Protección del tráfico con IPsec	510
▼ Cómo proteger el tráfico entre dos sistemas con IPsec	511
▼ Cómo utilizar IPsec para proteger un servidor web del tráfico que no procede de Internet	515
▼ Cómo visualizar las directivas de IPsec	518
▼ Cómo generar números aleatorios en un sistema Solaris	519
▼ Cómo crear manualmente asociaciones de seguridad IPsec	520
▼ Cómo verificar que los paquetes estén protegidos con IPsec	525
▼ Cómo configurar una función para la seguridad de la red	526
▼ Cómo administrar servicios de IPsec e IKE	528
Protección de una VPN con IPsec	530
Ejemplos de protección de una VPN con IPsec mediante el uso de túneles en modo túnel	530
Protección de una VPN con IPsec (mapa de tareas)	532
Descripción de la topología de red para la protección de una VPN por parte de las tareas de IPsec	533

▼ Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4	535
▼ Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv6	545
▼ Cómo proteger una VPN con un túnel IPsec en modo transporte mediante IPv4	551
▼ Cómo proteger una VPN con un túnel IPsec en modo transporte mediante IPv6	557
▼ Cómo evitar la falsificación de la IP	563
21 Arquitectura de seguridad IP (referencia)	567
Utilidad de gestión de servicios de IPsec	567
Comando ipsecconf	568
Archivo ipsecinit.conf	569
Archivo ipsecinit.conf de ejemplo	569
Consideraciones de seguridad para ipsecinit.conf e ipsecconf	570
Comando ipsecalg	570
Base de datos de asociaciones de seguridad para IPsec	571
Utilidades para la generación de claves en IPsec	571
Consideraciones de seguridad para ipseckey	572
Extensiones IPsec para otras utilidades	573
Comando ifconfig e IPsec	573
Comando snoop e IPsec	574
22 Intercambio de claves de Internet (descripción general)	575
Novedades de IKE	575
Administración de claves con IKE	576
Negociación de claves IKE	576
Terminología de claves IKE	576
Intercambio de IKE de fase 1	577
Intercambio de IKE de fase 2	578
Opciones de configuración de IKE	578
IKE con claves previamente compartidas	578
IKE con certificados de claves públicas	579
IKE y aceleración de hardware	580
IKE y almacenamiento de hardware	580
Archivos y utilidades IKE	580
Cambios de IKE en Solaris 10	582

23 Configuración de IKE (tareas)	583
Configuración de IKE (mapa de tareas)	583
Configuración de IKE con claves previamente compartidas (mapa de tareas)	584
Configuración de IKE con claves previamente compartidas	585
▼ Cómo configurar IKE con claves previamente compartidas	585
▼ Cómo actualizar las claves IKE previamente compartidas	588
▼ Cómo ver las claves IKE previamente compartidas	589
▼ Cómo agregar una clave IKE previamente compartida para una nueva entrada de directiva en <code>ipsecinit.conf</code>	591
▼ Verificación de que las claves IKE previamente compartidas sean idénticas	594
Configuración de IKE con certificados de clave pública (mapa de tareas)	595
Configuración de IKE con certificados de clave pública	596
▼ Cómo configurar IKE con certificados de clave pública autofirmados	596
▼ Cómo configurar IKE con certificados firmados por una autoridad de certificación	602
▼ Cómo generar y almacenar certificados de clave pública en el hardware	608
▼ Cómo administrar una lista de revocación de certificados	612
Configuración de IKE para sistemas portátiles (mapa de tareas)	614
Configuración de IKE para sistemas portátiles	614
▼ Cómo configurar IKE para sistemas remotos	615
Configuración de IKE para buscar el hardware conectado (mapa de tareas)	622
Configuración de IKE para buscar el hardware conectado	622
▼ Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 1000	622
▼ Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 4000	623
Cambio de los parámetros de transmisión de IKE (mapa de tareas)	625
Cambio de los parámetros de transmisión de IKE	625
▼ Cómo cambiar la duración de la negociación de claves IKE de fase 1	626
24 Intercambio de claves de Internet (referencia)	629
Utilidad de gestión de servicios de IKE	629
Daemon IKE	630
Archivo de directiva IKE	630
Comando de administración de IKE	631
Archivos de claves IKE previamente compartidas	632
Comandos y bases de datos de claves públicas IKE	632
Comando <code>ikecert tokens</code>	633

Comando <code>ikecert certlocal</code>	633
Comando <code>ikecert certdb</code>	634
Comando <code>ikecert certldb</code>	635
Directorio <code>/etc/inet/ike/publickeys</code>	635
Directorio <code>/etc/inet/secret/ike.privatekeys</code>	635
Directorio <code>/etc/inet/ike/crls</code>	636
25 Filtro IP en Oracle Solaris (descripción general)	637
Novedades del filtro IP	637
Enlaces de filtros de paquetes	637
Filtros de paquetes IPv6 para el filtro IP	638
Introducción al filtro	638
Orígenes de información para el filtro IP de código abierto	639
Procesamiento de paquetes del filtro IP	639
Directrices para utilizar el filtro IP	642
Uso de archivos de configuración del filtro IP	642
Cómo trabajar con conjuntos de reglas del filtro IP	643
Uso de la función de filtros de paquetes del filtro IP	643
Uso de la función NAT del filtro IP	646
Uso de la función de agrupaciones de direcciones del filtro IP	647
Enlaces de filtros de paquetes	649
El filtro IP y el módulo <code>pfil STREAMS</code>	649
IPv6 para filtro IP	650
Páginas del comando <code>man</code> del filtro IP	651
26 Filtro IP (tareas)	653
Configuración de filtro IP	653
▼ Cómo habilitar el filtro IP	654
▼ Cómo rehabilitar el filtro IP	655
▼ Cómo habilitar los filtros en bucle de retorno	656
Desactivación y deshabilitación de filtro IP	657
▼ Cómo desactivar los filtros de paquetes	657
▼ Cómo desactivar NAT	658
▼ Cómo deshabilitar los filtros de paquetes	659
Cómo trabajar con el módulo <code>pfil</code>	659

▼ How to Enable IP Filter in Previous Solaris Releases	660
▼ Cómo activar una NIC para los filtros de paquetes	662
▼ Cómo desactivar el filtro IP en una NIC	664
▼ Cómo visualizar las estadísticas de <code>pf</code> para el filtro IP	665
Cómo trabajar con conjuntos de reglas del filtro IP	666
Gestión de conjunto de reglas de filtro de paquetes para filtro IP	667
Gestión de reglas NAT para filtro IP	674
Gestión de agrupaciones de direcciones para el filtro IP	676
Cómo visualizar las estadísticas e información sobre el filtro IP	678
▼ Cómo ver las tablas de estado para el filtro IP	679
▼ Cómo ver las tablas de estado para el filtro IP	679
▼ Cómo visualizar las estadísticas de NAT para el filtro IP	680
▼ Cómo visualizar las estadísticas de la agrupación de direcciones para el filtro IP	681
Cómo trabajar con archivos de registro para el filtro IP	681
▼ Cómo configurar un archivo de registro para el filtro IP	682
▼ Cómo visualizar los archivos de registro del filtro IP	683
▼ Cómo vaciar el archivo de registro de paquetes	684
▼ Cómo guardar paquetes registrados en un archivo	684
Creación y edición de archivos de configuración del filtro IP	685
▼ Cómo crear un archivo de configuración para el filtro IP	686
Ejemplos de archivos de configuración del filtro IP	687
Parte V IP móvil	693
27 IP para móviles (Descripción general)	695
Novedades de IP para móviles	695
Introducción a IP para móviles	696
Entidades funcionales de IP para móviles	698
Funcionamiento de IP para móviles	698
Descubrimiento de agentes	701
Anuncio de agente	701
Solicitud de agente	702
Direcciones de auxilio	702
IP para móviles con túnel inverso	703
Admisión limitada de direcciones privadas	703

Registro de IP para móviles	705
Identificador de acceso de red (NAI)	707
Autenticación mediante mensaje de IP para móviles	707
Solicitud de registro del nodo móvil	707
Mensaje de respuesta de registro	708
Consideraciones del agente externo	708
Consideraciones del agente interno	708
Descubrimiento dinámico de agente interno	709
Encaminamiento de datagramas entre nodos móviles	709
Métodos de encapsulado	709
Encaminamiento de datagramas de unidifusión	709
Datagramas de multidifusión	710
Encaminamiento de datagramas de multidifusión	710
Consideraciones de seguridad para IP para móviles	711
 28 Administración de IP móvil (tareas)	713
Creación del archivo de configuración de IP móvil (mapa de tareas)	713
Creación del archivo de configuración de IP móvil	714
▼ Cómo planificar para IP móvil	714
▼ Creación del archivo de configuración de IP móvil	715
▼ Cómo configurar la sección General	715
▼ Cómo configurar la sección Advertisements	716
▼ Cómo configurar la sección GlobalSecurityParameters	716
▼ Cómo configurar la sección Pool	717
▼ Cómo configurar la sección SPI	717
▼ Cómo configurar la sección Address	717
Modificación del archivo de configuración de IP móvil (mapa de tareas)	718
Modificación del archivo de configuración de IP móvil	719
▼ Cómo modificar la sección General	719
▼ Cómo modificar la sección Advertisements	720
▼ Cómo modificar la sección GlobalSecurityParameters	720
▼ Cómo modificar la sección Pool	721
▼ Cómo modificar la sección SPI	721
▼ Cómo modificar la sección Address	722
▼ Cómo agregar o eliminar parámetros del archivo de configuración	723

▼ Cómo mostrar los valores actuales de los parámetros del archivo de configuración	724
Presentación del estado del agente de movilidad	725
▼ Cómo mostrar el estado del agente de movilidad	726
Presentación de las rutas de movilidad de un agente externo	727
▼ Cómo mostrar las rutas de movilidad de un agente externo	727
29 Archivos y comandos de IP para móviles (referencia)	729
Descripción general de la implementación de IP para móviles en Solaris	729
Archivo de configuración de IP para móviles	730
Formato del archivo de configuración	731
Ejemplos de archivos de configuración	731
Secciones y etiquetas del archivo de configuración	734
Configuración del agente de movilidad IP	743
Estado de un agente de movilidad de IP para móviles	744
Información de estado de IP para móviles	744
Extensiones de netstat para IP para móviles	745
Extensiones snoop de IP para móviles	745
Parte VI IPMP	747
30 Introducción a IPMP (descripción general)	749
Por qué debe utilizar IPMP	749
Componentes IPMP de Oracle Solaris	750
Terminología y conceptos de IPMP	751
Requisitos básicos de IPMP	753
Direcciones IPMP	754
Direcciones de datos	754
Direcciones de prueba	754
Cómo evitar que las aplicaciones utilicen direcciones de prueba	756
Configuraciones de interfaces IPMP	757
Interfaces de reserva en un grupo IPMP	757
Configuraciones comunes de interfaces IPMP	758
Funciones de detección de fallos IPMP y recuperación	758
Detección de fallos basada en vínculos	759

Detección de fallos basada en sondeos	759
Fallos de grupo	760
Detección de reparaciones de interfaces físicas	761
Qué ocurre durante la conmutación por error de la interfaz	761
IPMP y reconfiguración dinámica	763
Conexión de NIC	763
Desconexión de NIC	764
Reconexión de NIC	764
NIC que no estaban presentes durante el inicio del sistema	765
31 Administración de IPMP (tareas)	767
Configuración de IPMP (mapas de tareas)	767
Configuración y administración de grupos IPMP (mapa de tareas)	767
Administración de IPMP en interfaces que admiten reconfiguración dinámica (mapa de tareas)	768
Configuración de grupos IPMP	769
Planificación de un grupo IPMP	769
Configuración de grupos IPMP	771
Configuración de grupos IPMP con una única interfaz física	779
Mantenimiento de grupos IPMP	781
▼ Cómo mostrar la pertenencia de una interfaz a un grupo IPMP	781
▼ Cómo agregar una interfaz a un grupo IPMP	782
▼ Cómo eliminar una interfaz de un grupo IPMP	782
▼ Cómo mover una interfaz de un grupo IPMP a otro grupo	783
Sustitución de una interfaz física fallida en sistemas que admiten reconfiguración dinámica	784
▼ Cómo eliminar una interfaz física que ha fallado (desconexión en DR)	784
▼ Como sustituir una interfaz física que ha fallado (conexión en DR)	785
Recuperación de una interfaz física que no estaba presente durante el inicio del sistema	786
▼ Cómo recuperar una interfaz física que no está presente al iniciar el sistema	786
Modificación de configuraciones IPMP	788
▼ Cómo configurar el archivo /etc/default/mpathd	789

Parte VII	Calidad de servicio IP (IPQoS)	791
32	Introducción a IPQoS (Descripción general)	793
	Conceptos básicos de IPQoS	793
	¿Qué son los servicios diferenciados?	793
	Funciones de IPQoS	794
	Dónde obtener más información sobre la teoría y práctica de la calidad del servicio	794
	Proporcionar calidad de servicio con IPQoS	796
	Utilización de acuerdos de nivel de servicio	796
	Garantizar la calidad de servicio para una organización específica	796
	Introducción a la directiva de calidad de servicio	796
	Mejorar la eficacia de la red con IPQoS	797
	Cómo afecta el ancho de banda al tráfico de red	797
	Utilización de clases de servicio para priorizar el tráfico	798
	Modelo de servicios diferenciados	799
	Descripción general del clasificador (ipgpc)	799
	Descripción general de medidor (tokenmt y tswtclmt)	800
	Descripción general de marcadores (dscpmk y dlcosmk)	801
	Descripción general del control de flujo (flowacct)	801
	Cómo fluye el tráfico a través de los módulos IPQoS	802
	Reenvío del tráfico en una red con IPQoS	804
	Punto de código DS	804
	Comportamientos por salto	804
33	Planificación para una red con IPQoS (Tareas)	809
	Planificación de configuración IPQoS general (Mapa de tareas)	809
	Planificación de la distribución de la red Diffserv	810
	Estrategias de hardware para la red Diffserv	810
	Distribuciones de red IPQoS	811
	Planificación de la directiva de calidad de servicio	813
	Ayudas para planificar la directiva QoS	813
	Planificación de la directiva QoS (Mapa de tareas)	814
	▼ Cómo preparar una red para IPQoS	815
	▼ Cómo definir las clases de la directiva QoS	816
	Definir filtros	818

▼ Cómo definir filtros en la directiva QoS	819
▼ Cómo planificar el control de flujo	820
▼ Cómo planificar el comportamiento de reenvío	823
▼ Cómo planificar la recopilación de datos de flujo	825
Introducción al ejemplo de configuración IPQoS	826
Distribución IPQoS	826
34 Creación del archivo de configuración IPQoS (Tareas)	829
Definición de una directiva QoS en el archivo de configuración IPQoS (Mapa de tarea)	829
Herramientas para crear una directiva QoS	831
Archivo de configuración IPQoS básico	831
Crear archivos de configuración IPQoS para servidores web	832
▼ Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico	834
▼ Cómo definir filtros en el archivo de configuración IPQoS	836
▼ Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS	838
▼ Cómo activar el control para una clase en el archivo de configuración IPQoS	841
▼ Cómo crear un archivo de configuración IPQoS para un servidor web "Best-Effort"	842
Crear un archivo de configuración IPQoS para un servidor de aplicaciones	845
▼ Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones	847
▼ Cómo configurar el reenvío para el tráfico de aplicaciones en el archivo de configuración IPQoS	849
▼ Cómo configurar el control de flujo en el archivo de configuración IPQoS	851
Suministro de servicios diferenciados en un enrutador	854
▼ Cómo configurar un enrutador en una red con IPQoS	855
35 Inicio y mantenimiento de IPQoS (Tareas)	857
Administración IPQoS (Mapa de tareas)	857
Aplicación de una configuración IPQoS	858
▼ Cómo aplicar una nueva configuración a los módulos de kernel IPQoS	858
▼ Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia	859
Activación del registro sys log para mensajes IPQoS	859
▼ Cómo activar el registro de mensajes IPQoS durante el inicio	860
Resolución de problemas con mensajes de error IPQoS	861

36	Uso de control de flujo y recopilación de estadísticas (Tareas)	865
	Establecimiento del control de flujo (Mapa de tareas)	865
	Registro de información sobre flujos de tráfico	866
	▼ Cómo crear un archivo para datos de control de flujo	866
	Recopilación de estadísticas	868
37	IPQoS detallado (Referencia)	871
	Arquitectura IPQoS y el modelo Diffserv	871
	Módulo Classifier	871
	Módulo Meter	874
	Módulo marcador	876
	Módulo flowacct	881
	Archivo de configuración IPQoS	884
	Instrucción action	885
	Definiciones de módulo	886
	Cláusula class	886
	Cláusula filter	887
	Cláusula params	887
	Herramienta de configuración ipqosconf	887
	Glosario	889
	Índice	901

Prefacio

La *Guía de administración del sistema: servicios IP* forma parte de un conjunto de nueve volúmenes que tratan de manera exhaustiva la administración de sistemas Oracle Solaris. Este manual da por supuesto que ya se ha instalado Oracle Solaris 10. La red debe estar configurada o preparada para poder integrar cualquier software de red que se necesite. Oracle Solaris 10 es parte de la familia de productos Oracle Solaris, que incluye también Java Desktop System. Oracle Solaris es compatible con el sistema operativo AT&T's System V, versión 4.

Nota – Esta versión de Oracle Solaris es compatible con sistemas que usen arquitecturas de las familias de procesadores SPARC y x86. Los sistemas compatibles aparecen en *Listas de compatibilidad del sistema operativo Oracle Solaris*. Este documento indica las diferencias de implementación entre los tipos de plataforma.

En este documento, estos términos relacionados con x86 significan lo siguiente:

- x86 hace referencia a la familia más grande de productos compatibles con x86 de 32 y 64 bits.
- x64 hace referencia específicamente a CPU compatibles con x86 de 64 bits.
- "x86 de 32 bits" destaca información específica de 32 bits acerca de sistemas basados en x86.

Para conocer cuáles son los sistemas admitidos, consulte [*Listas de compatibilidad del sistema operativo Oracle Solaris*](#).

Quién debe utilizar este manual

Este manual está destinado a las personas encargadas de administrar sistemas que ejecutan Oracle Solaris configurado en red. Para utilizar este manual, se debe tener como mínimo dos años de experiencia en la administración de sistemas UNIX . Puede resultar útil participar en cursos de formación para administración de sistemas UNIX.

Organización de las guías de administración del sistema

A continuación se enumeran los temas que abarcan las guías de administración del sistema.

Título de manual	Temas
<i>Guía de administración del sistema: administración básica</i>	Grupos y cuentas de usuario, asistencia para clientes y servidores, cierre e inicio de un sistema y administración de servicios
<i>Guía de administración del sistema: Administración avanzada</i>	Terminales y módems, recursos del sistema (cuotas de disco, cuentas y archivos crontab), procesos del sistema y resolución de problemas de software de Oracle Solaris
<i>System Administration Guide: Devices and File Systems</i>	Medios extraíbles, discos y dispositivos, sistemas de archivos y copias de seguridad y restauración de datos
<i>Guía de administración del sistema: servicios IP</i>	Administración de redes TCP/IP, administración de direcciones IPv4 e IPv6, DHCP, IPsec, IKE, filtro IP, IP móvil, rutas múltiples de redes IP (IPMP) e IPQoS
<i>Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)</i>	Servicios de directorios y nombres DNS, NIS y LDAP, incluida la transición de NIS a LDAP y de NIS+ a LDAP
<i>System Administration Guide: Naming and Directory Services (NIS+)</i>	Servicios de directorios y nombres NIS+
<i>Guía de administración del sistema: servicios de red</i>	Servidores de caché web, servicios relacionados con el tiempo, sistemas de archivos de red (NFS y Autofs), correo, SLP y PPP
<i>System Administration Guide: Printing</i>	Tareas y temas de impresión, uso de servicios, herramientas, protocolos y tecnologías para configurar y administrar las impresoras y los servicios de impresión
<i>Guía de administración del sistema: servicios de seguridad</i>	Auditoría, administración de dispositivos, seguridad de archivos, BART, servicios Kerberos, PAM, estructura criptográfica de Oracle Solaris, privilegios, RBAC, SASL y Oracle Solaris Secure Shell
<i>Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris</i>	Tareas y proyectos de temas de administración de recursos, contabilidad extendida, controles de recursos, planificación por reparto equitativo (FSS), control de memoria física utilizando el daemon de limitación de recursos (rcapd) y agrupaciones de recursos; virtualización con la tecnología de partición de software Zonas de Solaris y zonas con la marca lx
<i>Guía de administración de Oracle Solaris ZFS</i>	Creación y administración de sistemas de archivos y agrupaciones de almacenamiento ZFS, instantáneas, clones, copias de seguridad, uso de listas de control de acceso (ACL) para proteger archivos ZFS, uso de Solaris ZFS en un sistema Solaris con zonas instaladas, volúmenes emulados y resolución de problemas y recuperación de datos

Título de manual	Temas
<i>Procedimientos de administradores de Oracle Solaris Trusted Extensions</i>	Administración de sistemas específica de un sistema Oracle Solaris Trusted Extensions
<i>Guía de configuración de Oracle Solaris Trusted Extensions</i>	A partir de la versión Solaris 10 5/08, se explica la forma de planificar, habilitar y configurar inicialmente la función Oracle Solaris Trusted Extensions

Manuales relacionados

En el presente manual se hace referencia a las siguientes obras.

- Stevens, W. Richard. *TCP/IP Illustrated, Volume 1, The Protocols*. Addison Wesley, 1994.
- Hunt Craig. *TCP/IP Network Administration, 3rd Edition*. O'Reilly, 2002.
- Perkins, Charles E. *Mobile IP Design Principles and Practices*. Massachusetts, 1998, Addison-Wesley Publishing Company.
- Solomon, James D. *Mobile IP: The Internet Unplugged*. New Jersey, 1998, Prentice-Hall, Inc.
- Ferguson, Paul y Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Killki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.

Referencias relacionadas con el sitio web de otras empresas

Se hace referencia a direcciones URL de terceras partes para proporcionar información adicional relacionada.

Nota – Sun no se responsabiliza de la disponibilidad de las páginas web de otras empresas que se mencionan en este documento. Sun no garantiza ni se hace responsable de los contenidos, la publicidad, los productos u otros materiales que puedan estar disponibles a través de dichos sitios o recursos. Sun no será responsable de daños o pérdidas, supuestos o reales, provocados por o a través del uso o confianza del contenido, bienes o servicios disponibles en dichos sitios o recursos, o a través de ellos.

El filtro IP de Oracle Solaris se deriva de software de filtro IP de código abierto. Para consultar los términos de la licencia y declaraciones de copyright de filtro IP, la ruta predeterminada es `/usr/lib/ipf/IPFILTER.LICENCE`. Si se ha instalado Oracle Solaris en una ubicación que no sea la predeterminada, modifique la ruta para acceder al archivo en la ubicación correcta.

Acceso a Oracle Support

Los clientes de Oracle tienen acceso a soporte electrónico por medio de My Oracle Support. Para obtener más información, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> o, si tiene alguna discapacidad auditiva, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>.

Convenciones tipográficas

La siguiente tabla describe las convenciones tipográficas utilizadas en este manual.

TABLA P-1 Convenciones tipográficas

Tipos de letra	Significado	Ejemplo
AaBbCc123	Los nombres de los comandos, los archivos, los directorios y los resultados que el equipo muestra en pantalla	Edite el archivo <code>.login</code> . Utilice el comando <code>ls -a</code> para mostrar todos los archivos. <code>nombre_sistema%</code> tiene correo.
AaBbCc123	Lo que se escribe, en contraposición con la salida del equipo en pantalla	<code>nombre_sistema% su</code> Contraseña:
<i>aabbcc123</i>	Marcador de posición: sustituir por un valor o nombre real	El comando necesario para eliminar un archivo es <code>rm nombre_archivo</code> .
<i>AaBbCc123</i>	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el capítulo 6 de la <i>Guía del usuario</i> . Una <i>copia en caché</i> es aquella que se almacena localmente. <i>No</i> guarde el archivo. Nota: algunos elementos destacados aparecen en negrita en línea.

Indicadores de los shells en los ejemplos de comandos

La tabla siguiente muestra los indicadores de sistema UNIX predeterminados y el indicador de superusuario de shells que se incluyen en los sistemas operativos Oracle Solaris. Tenga en cuenta que el indicador predeterminado del sistema que se muestra en los ejemplos de comandos varía según la versión de Oracle Solaris.

TABLA P-2 Indicadores de shell

Shell	Indicador
Shell Bash, shell Korn y shell Bourne	\$
Shell Bash, shell Korn y shell Bourne para superusuario	#
Shell C	nombre_sistema%
Shell C para superusuario	nombre_sistema#

P A R T E I

Introducción a la administración del sistema: servicios IP

Esta sección contiene información de introducción acerca de los protocolos TCP/IP y su implementación en Oracle Solaris.

Conjunto de protocolos TCP/IP de Oracle Solaris (descripción general)

Este capítulo introduce la implementación en Oracle Solaris del conjunto de protocolos de red TCP/IP. Esta información se dirige a los administradores de sistemas y redes que no están familiarizados con los conceptos básicos de TCP/IP. En las demás secciones de esta guía se presupone que el usuario está familiarizado con estos conceptos.

Este capítulo contiene la información siguiente:

- “Introducción al conjunto de protocolos TCP/IP” en la página 37
- “Cómo manejan las comunicaciones de datos los protocolos TCP/IP” en la página 45
- “Información adicional sobre TCP/IP e Internet” en la página 49

Novedades de esta versión

A partir de Solaris 10 5/08, se ha eliminado la función de IP para móviles. IP para móviles está disponible en Solaris 10 8/07 y en las versiones anteriores.

Introducción al conjunto de protocolos TCP/IP

Esta sección incluye una introducción detallada a los protocolos que se incluyen en TCP/IP. Aunque la información es conceptual, debe conocer los nombres de los protocolos. También aprenderá las acciones que lleva a cabo cada protocolo.

"TCP/IP" es el acrónimo que se utiliza comúnmente para el conjunto de protocolos de red que componen el *conjunto de protocolos de Internet*. Muchos textos utilizan el término "Internet" para describir tanto el conjunto de protocolos como la red de área global. En este manual, "TCP/IP" hace referencia específicamente al conjunto de protocolos de Internet. "Internet" hace referencia a la red de área extensa y los elementos que rigen Internet.

Para interconectar la red TCP/IP con otras redes, debe obtener una dirección IP única para la red. En el momento en que se redacta esta guía, esta dirección se obtiene a través de un proveedor de servicios de Internet (ISP).

Si los hosts de la red tienen que participar en el sistema de nombre de dominio (DNS), debe obtener y registrar un nombre de dominio único. InterNIC coordina el registro de nombres de dominio a través de un grupo de registros mundiales. Para obtener más información acerca de DNS, consulte *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*.

Capas de protocolo y el modelo de Interconexión de Sistemas Abiertos

La mayoría de los conjuntos de protocolos de red se estructuran como series de capas, que en ocasiones se denominan *pila de protocolos*. Cada capa está diseñada para una finalidad específica. Cada capa existe tanto en los sistemas de envío como en los de recepción. Una capa específica de un sistema envía o recibe exactamente el mismo objeto que envía o recibe el *proceso equivalente* de otro sistema. Estas actividades tienen lugar independientemente de las actividades de las capas por encima o por debajo de la capa que se está considerando. Básicamente, cada capa de un sistema actúa independientemente de las demás capas del mismo sistema. Cada capa actúa en paralelo con la misma capa en otros sistemas.

Modelo de referencia OSI

La mayoría de los conjuntos de protocolos de red se estructuran en capas. La Organización Internacional para la Estandarización (ISO) ha diseñado el modelo de referencia de Interconexión de Sistemas Abiertos (OSI) que utiliza capas estructuradas. El modelo OSI describe una estructura con siete capas para las actividades de red. Cada capa tiene asociados uno o más protocolos. Las capas representan las operaciones de transferencia de datos comunes a todos los tipos de transferencias de datos entre las redes de cooperación.

El modelo OSI enumera las capas de protocolos desde la superior (capa 7) hasta la inferior (capa 1). La tabla siguiente muestra el modelo.

TABLA 1-1 Modelo de referencia de Interconexión de Sistemas Abiertos

N.º de capa	Nombre de capa	Descripción
7	Aplicación	Se compone de los servicios y aplicaciones de comunicación estándar que puede utilizar todo el mundo.
6	Presentación	Se asegura de que la información se transfiera al sistema receptor de un modo comprensible para el sistema.
5	Sesión	Administra las conexiones y terminaciones entre los sistemas que cooperan.
4	Transporte	Administra la transferencia de datos. Asimismo, garantiza que los datos recibidos sean idénticos a los transmitidos.
3	Red	Administra las direcciones de datos y la transferencia entre redes.

TABLA 1-1 Modelo de referencia de Interconexión de Sistemas Abiertos (Continuación)

N.º de capa	Nombre de capa	Descripción
2	Vínculo de datos	Administra la transferencia de datos en el medio de red.
1	Física	Define las características del hardware de red.

El modelo de referencia OSI define las operaciones conceptuales que no son exclusivas de un conjunto de protocolos de red particular. Por ejemplo, el conjunto de protocolos de red OSI implementa las siete capas del modelo OSI. TCP/IP utiliza algunas de las capas del modelo OSI. TCP/IP también combina otras capas. Otros protocolos de red, como SNA, agregan una octava capa.

Modelo de arquitectura del protocolo TCP/IP

El modelo OSI describe las comunicaciones de red ideales con una familia de protocolos. TCP/IP no se corresponde directamente con este modelo. TCP/IP combina varias capas OSI en una única capa, o no utiliza determinadas capas. La tabla siguiente muestra las capas de la implementación de Oracle Solaris de TCP/IP. La tabla enumera las capas desde la capa superior (aplicación) hasta la capa inferior (red física).

TABLA 1-2 Pila de protocolo TCP/IP

Ref. OSI N.º de capa	Equivalente de capa OSI	Capa TCP/IP	Ejemplos de protocolos TCP/IP
5,6,7	Aplicación, sesión, presentación	Aplicación	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP y otros.
4	Transporte	Transporte	TCP, UDP, SCTP
3	Red	Internet	IPv4, IPv6, ARP, ICMP
2	Vínculo de datos	Vínculo de datos	PPP, IEEE 802.2
1	Física	Red física	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI y otros.

La tabla muestra las capas de protocolo TCP/IP y los equivalentes del modelo OSI. También se muestran ejemplos de los protocolos disponibles en cada nivel de la pila del protocolo TCP/IP. Cada sistema que participa en una transacción de comunicación ejecuta una única implementación de la pila del protocolo.

Capa de red física

La *capa de red física* especifica las características del hardware que se utilizará para la red. Por ejemplo, la capa de red física especifica las características físicas del medio de comunicaciones. La capa física de TCP/IP describe los estándares de hardware como IEEE 802.3, la especificación del medio de red Ethernet, y RS-232, la especificación para los conectores estándar.

Capa de vínculo de datos

La *capa de vínculo de datos* identifica el tipo de protocolo de red del paquete, en este caso TCP/IP. La capa de vínculo de datos proporciona también control de errores y estructuras. Algunos ejemplos de protocolos de capa de vínculo de datos son las estructuras Ethernet IEEE 802.2 y Protocolo punto a punto (PPP).

Capa de Internet

La capa de Internet, también conocida como *capa de red* o *capa IP*, acepta y transfiere paquetes para la red. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).

Protocolo IP

El protocolo IP y sus protocolos de enrutamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP. El protocolo IP se encarga de:

- **Direcciones IP:** Las convenciones de direcciones IP forman parte del protocolo IP. [“Cómo diseñar un esquema de direcciones IPv4” en la página 58](#) introduce las direcciones IPv4 y [“Descripción general de las direcciones IPv6” en la página 76](#) las direcciones IPv6.
- **Comunicaciones de host a host:** El protocolo IP determina la ruta que debe utilizar un paquete, basándose en la dirección IP del sistema receptor.
- **Formato de paquetes:** el protocolo IP agrupa paquetes en unidades conocidas como *datagramas*. Puede ver una descripción completa de los datagramas en [“Capa de Internet: preparación de los paquetes para la entrega” en la página 47](#).
- **Fragmentación:** Si un paquete es demasiado grande para su transmisión a través del medio de red, el protocolo IP del sistema de envío divide el paquete en fragmentos de menor tamaño. A continuación, el protocolo IP del sistema receptor reconstruye los fragmentos y crea el paquete original.

Oracle Solaris admite los formatos de direcciones IPv4 e IPv6, que se describen en este manual. Para evitar confusiones con el uso del Protocolo de Internet, se utiliza una de las convenciones siguientes:

- Cuando se utiliza el término "IP" en una descripción, ésta se aplica tanto a IPv4 como a IPv6.
- Cuando se utiliza el término "IPv4" en una descripción, ésta sólo se aplica a IPv4.
- Cuando se utiliza el término "IPv6" en una descripción, ésta sólo se aplica a IPv6.

Protocolo ARP

El protocolo de resolución de direcciones (ARP) se encuentra conceptualmente entre el vínculo de datos y las capas de Internet. ARP ayuda al protocolo IP a dirigir los datagramas al sistema receptor adecuado asignando direcciones Ethernet (de 48 bits de longitud) a direcciones IP conocidas (de 32 bits de longitud).

Protocolo ICMP

El protocolo de mensajes de control de Internet (ICMP) detecta y registra las condiciones de error de la red. ICMP registra:

- **Paquetes soltados:** Paquetes que llegan demasiado rápido para poder procesarse.
- **Fallo de conectividad:** No se puede alcanzar un sistema de destino.
- **Redirección:** Redirige un sistema de envío para utilizar otro enrutador.

El [Capítulo 8, “Administración de redes TCP/IP \(tareas\)”](#) contiene más información sobre los comandos de Oracle Solaris que utilizan ICMP para la detección de errores.

Capa de transporte

La *capa de transporte* TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos. Este tipo de comunicación se conoce como *transmisión de punto a punto*. Los protocolos de capa de transporte de este nivel son el Protocolo de control de transmisión (TCP), el Protocolo de datagramas de usuario (UDP) y el Protocolo de transmisión para el control de flujo (SCTP). Los protocolos TCP y SCTP proporcionan un servicio completo y fiable. UDP proporciona un servicio de datagrama poco fiable.

Protocolo TCP

TCP permite a las aplicaciones comunicarse entre sí como si estuvieran conectadas físicamente. TCP envía los datos en un formato que se transmite carácter por carácter, en lugar de transmitirse por paquetes discretos. Esta transmisión consiste en lo siguiente:

- Punto de partida, que abre la conexión.
- Transmisión completa en orden de bytes.
- Punto de fin, que cierra la conexión.

TCP conecta un encabezado a los datos transmitidos. Este encabezado contiene múltiples parámetros que ayudan a los procesos del sistema transmisor a conectarse a sus procesos correspondientes en el sistema receptor.

TCP confirma que un paquete ha alcanzado su destino estableciendo una conexión de punto a punto entre los hosts de envío y recepción. Por tanto, el protocolo TCP se considera un protocolo fiable orientado a la conexión.

Protocolo SCTP

SCTP es un protocolo de capa de transporte fiable orientado a la conexión que ofrece los mismos servicios a las aplicaciones que TCP. Además, SCTP admite conexiones entre sistemas que tienen más de una dirección, o de *host múltiple*. La conexión SCTP entre el sistema transmisor y receptor se denomina *asociación*. Los datos de la asociación se organizan en bloques. Dado que el protocolo SCTP admite varios hosts, determinadas aplicaciones, en especial las que se utilizan en el sector de las telecomunicaciones, necesitan ejecutar SCTP en lugar de TCP.

Protocolo UDP

UDP proporciona un servicio de entrega de datagramas. UDP no verifica las conexiones entre los hosts transmisores y receptores. Dado que el protocolo UDP elimina los procesos de establecimiento y verificación de las conexiones, resulta ideal para las aplicaciones que envían pequeñas cantidades de datos.

Capa de aplicación

La *capa de aplicación* define las aplicaciones de red y los servicios de Internet estándar que puede utilizar un usuario. Estos servicios utilizan la capa de transporte para enviar y recibir datos. Existen varios protocolos de capa de aplicación. En la lista siguiente se incluyen ejemplos de protocolos de capa de aplicación:

- Servicios TCP/IP estándar como los comandos ftp, tftp y telnet.
- Comandos UNIX "r", como rlogin o rsh.
- Servicios de nombres, como NIS o el sistema de nombre de dominio (DNS).
- Servicios de directorio (LDAP).
- Servicios de archivos, como el servicio NFS.
- Protocolo simple de administración de red (SNMP), que permite administrar la red.
- Protocolo RDISC (Router Discovery Server) y protocolos RIP (Routing Information Protocol).

Servicios TCP/IP estándar

- **FTP y FTP anónimo:** el protocolo de transferencia de archivos (FTP) transfiere archivos a una red remota y desde ella. El protocolo incluye el comando ftp y el daemon in.ftpd. FTP permite a un usuario especificar el nombre del host remoto y las opciones de comandos de transferencia de archivos en la línea de comandos del host local. El daemon in.ftpd del host remoto administra las solicitudes del host local. A diferencia de rcp, ftp funciona aunque el equipo remoto no ejecute un sistema operativo basado en UNIX. Para realizar una conexión ftp, el usuario debe iniciar sesión en un sistema remoto, aunque éste se haya configurado para permitir FTP anónimo.

Puede obtener una gran cantidad de material de *servidores FTP anónimos* conectados a Internet. Las universidades y otras instituciones configuran estos servidores para ofrecer software, trabajos de investigación y otra información al dominio público. Al iniciar sesión en este tipo de servidor, se utiliza el nombre de inicio de sesión anonymous, que da nombre al "servidor FTP anónimo"

Este manual no describe el uso del FTP anónimo ni la configuración de servidores FTP anónimos. Existen múltiples libros, como *Conéctate al mundo de Internet. Guía y catálogo*, que describen el protocolo FTP anónimo de manera pormenorizada. Encontrará información sobre el uso de FTP en la *Guía de administración del sistema: servicios de red*. La página del comando `man ftp(1)` describe todas las opciones del comando `ftp` que se invocan mediante el intérprete de comandos. La página del comando `man ftpd(1M)` describe los servicios que proporciona el daemon `in.ftpd`.

- **Telnet:** el protocolo Telnet permite la comunicación entre los terminales y los procesos orientados a los terminales de una red que ejecuta TCP/IP. Este protocolo se implementa como programa `telnet` en los sistemas locales y como daemon `in.telnetd` en los equipos remotos. Telnet proporciona una interfaz de usuario a través de la cual se pueden comunicar dos hosts carácter por carácter o línea por línea. Telnet incluye un conjunto de comandos que se documentan de forma detallada en la página del comando `man telnet(1)`.
- **TFTP:** el protocolo de transferencia de archivos trivial (`tftp`) ofrece funciones similares a `ftp`, pero no establece la conexión interactiva de `ftp`. Como consecuencia, los usuarios no pueden ver el contenido de un directorio ni cambiar directorios. Los usuarios deben conocer el nombre completo del archivo que se va a copiar. La página del comando `man tftp(1)` describe el conjunto de comandos `tftp`.

Comandos UNIX "r"

Los comandos UNIX "r" permiten a los usuarios ejecutar comandos en sus equipos locales que se ejecutan en el host remoto. Estos comandos incluyen:

- `rcp`
- `rlogin`
- `rsh`

Encontrará instrucciones sobre estos comandos en las páginas del comando `man rcp(1)`, `rlogin(1)` y `rsh(1)`.

Servicios de nombres

Oracle Solaris proporciona los siguientes servicios de nombres:

- **DNS:** El sistema de nombre de dominio (DNS) es el servicio de nombres que proporciona Internet para las redes TCP/IP. DNS proporciona nombres de host al servicio de direcciones IP. También actúa como base de datos para la administración del correo. Para ver una

descripción completa de este servicio, consulte la [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#). Consulte también la página del comando `man resolver(3RESOLV)`.

- Archivos /etc : El sistema de nombres UNIX basado en host se desarrolló para equipos UNIX autónomos y posteriormente se adaptó para el uso en red. Muchos de los antiguos sistemas operativos y equipos UNIX siguen utilizando este sistema, pero no resulta adecuado para redes complejas de gran tamaño.
- NIS: El Servicio de información de la red (NIS) se desarrolló independientemente de DNS y tiene un enfoque ligeramente distinto. Mientras que DNS trata de facilitar la comunicación con el uso de nombres de equipos en lugar de direcciones IP numéricas, NIS se centra en facilitar la administración de la red al proporcionar control centralizado sobre distintos tipos de información de red. NIS almacena información sobre los nombres de equipo y las direcciones, los usuarios, la red y los servicios de red. La información de espacio de nombres NIS se almacena en asignaciones NIS. Para obtener más información sobre la arquitectura y administración de NIS, consulte la [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

Servicio de directorios

Oracle Solaris admite LDAP (Protocolo ligero de acceso a directorios) junto con el servidor de directorios Sun ONE (Sun Open Net Environment), así como otros servidores de directorios LDAP. La diferencia entre un servicio de nombres y un servicio de directorios radica en la extensión de las funciones. Un servicio de directorios proporciona las mismas funciones que un servicio de nombres, pero además cuenta con funciones adicionales. Consulte la [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

Servicios de archivos

El protocolo de capa de aplicación NFS proporciona servicios de archivos para Oracle Solaris. Encontrará información completa sobre el servicio NFS en la [Guía de administración del sistema: servicios de red](#).

Administración de la red

El Protocolo simple de administración de red (SNMP) permite ver la distribución de la red y el estado de los equipos clave. SNMP también permite obtener estadísticas de red complejas del software basado en una interfaz gráfica de usuario (GUI). Muchas compañías ofrecen paquetes de administración de red que implementan SNMP.

Protocolos de enrutamiento

Los protocolos RIP y RDISC son dos protocolos de enrutamiento disponibles para las redes TCP/IP. Para ver una lista completa de los protocolos de enrutamiento disponibles para Oracle Solaris 10, consulte la [Tabla 5–1](#) y la [Tabla 5–2](#).

Cómo manejan las comunicaciones de datos los protocolos TCP/IP

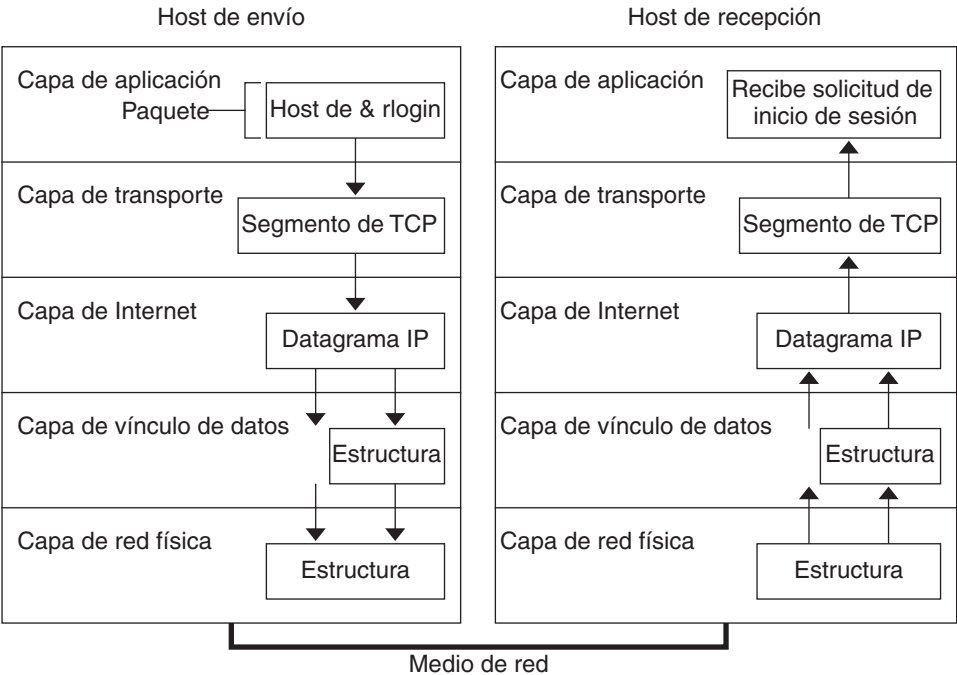
Cuando un usuario ejecuta un comando que utiliza un protocolo de capa de aplicación TCP/IP, se inicia una serie de eventos. El mensaje o el comando del usuario se transfiere a través de la pila de protocolo TCP/IP del sistema local. A continuación, el mensaje o el comando pasa por el medio de red hasta los protocolos del sistema remoto. Los protocolos de cada capa del host de envío agregan información a los datos originales.

Además, dichos protocolos interactúan con sus equivalentes en el host de recepción. La [Figura 1-1](#) muestra la interacción.

Encapsulado de datos y la pila de protocolo TCP/IP

El paquete es la unidad de información básica que se transfiere a través de una red. El paquete básico se compone de un encabezado con las direcciones de los sistemas de envío y recepción, y un cuerpo, o *carga útil*, con los datos que se van a transferir. Cuando el paquete se transfiere a través de la pila de protocolo TCP/IP, los protocolos de cada capa agregan o eliminan campos del encabezado básico. Cuando un protocolo del sistema de envío agrega datos al encabezado del paquete, el proceso se denomina *encapsulado de datos*. Asimismo, cada capa tiene un término diferente para el paquete modificado, como se muestra en la figura siguiente.

FIGURA 1-1 Transferencia de un paquete a través de la pila TCP/IP



Esta sección resume el ciclo de vida de un paquete. El ciclo de vida empieza cuando se ejecuta un comando o se envía un mensaje, y finaliza cuando la aplicación adecuada del sistema receptor recibe el paquete.

Capa de aplicación: el origen de la comunicación

El recorrido del paquete empieza cuando un usuario en un sistema envía un mensaje o ejecuta un comando que debe acceder a un sistema remoto. El protocolo de aplicación da formato al paquete para que el protocolo de capa de transporte adecuado (TCP o UDP) pueda manejar el paquete.

Supongamos que el usuario ejecuta un comando `rlogin` para iniciar sesión en el sistema remoto, tal como se muestra en la [Figura 1-1](#). El comando `rlogin` utiliza el protocolo de capa de transporte TCP. TCP espera recibir los datos con el formato de un flujo de bytes que contiene la información del comando. Por tanto, `rlogin` envía estos datos como flujo TCP.

Capa de transporte: el inicio del encapsulado de datos

Cuando los datos llegan a la capa de transporte, los protocolos de la capa inician el proceso de encapsulado de datos. La capa de transporte encapsula los datos de aplicación en unidades de datos de protocolo de transporte.

El protocolo de capa de transporte crea un flujo virtual de datos entre la aplicación de envío y la de recepción, que se identifica con un número de puerto de transporte. El número de puerto identifica un *puerto*, una ubicación dedicada de la memoria par recibir o enviar datos. Además, la capa de protocolo de transporte puede proporcionar otros servicios, como la entrega de datos ordenada y fiable. El resultado final depende de si la información se maneja con los protocolos TCP, SCTP o UDP.

Segmentación TCP

TCP se denomina a menudo protocolo "orientado a la conexión" porque TCP garantiza la entrega correcta de los datos al host de recepción. La [Figura 1-1](#) muestra cómo el protocolo TCP recibe el flujo del comando `rlogin`. A continuación, TCP divide los datos que se reciben de la capa de aplicación en segmentos y adjunta un encabezado a cada segmento.

Los encabezados de segmento contienen puertos de envío y recepción, información de orden de los segmentos y un campo de datos conocido como *suma de comprobación*. Los protocolos TCP de ambos hosts utilizan los datos de suma de comprobación para determinar si los datos se transfieren sin errores.

Establecimiento de una conexión TCP

TCP utiliza segmentos para determinar si el sistema de recepción está listo para recibir los datos. Cuando el protocolo TCP de envío desea establecer conexiones, envía un segmento denominado *SYN* al protocolo TCP del host de recepción. El protocolo TCP de recepción devuelve un segmento denominado *ACK* para confirmar que el segmento se ha recibido correctamente. El protocolo TCP de envío emite otro segmento *ACK* y luego procede al envío de los datos. Este intercambio de información de control se denomina *protocolo de tres vías*.

Paquetes UDP

UDP es un protocolo "sin conexiones". A diferencia de TCP, UDP no comprueba los datos que llegan al host de recepción. En lugar de ello, UDP da formato al mensaje que se recibe desde la capa de la aplicación en los *paquetes UDP*. UDP adjunta un encabezado a cada paquete. El encabezado contiene los puertos de envío y recepción, un campo con la longitud del paquete y una suma de comprobación.

El proceso UDP de envío intenta enviar el paquete a su proceso UDP equivalente en el host de recepción. La capa de aplicación determina si el proceso UDP de recepción confirma la recepción del paquete. UDP no requiere ninguna notificación de la recepción. UDP no utiliza el protocolo de tres vías.

Capa de Internet: preparación de los paquetes para la entrega

Los protocolos de transporte TCP, UDP y SCTP transfieren sus segmentos y paquetes a la capa de Internet, en la que el protocolo IP los maneja. El protocolo IP los prepara para la entrega

asignándolos a unidades denominadas *datagramas IP*. A continuación, el protocolo IP determina las direcciones IP para los datagramas, para que se puedan enviar de forma efectiva al host de recepción.

Datagramas IP

IP adjunta un *encabezado IP* al segmento o el encabezado del paquete, además de la información que agregan los protocolos TCP o UDP. La información del encabezado IP incluye las direcciones IP de los hosts de envío y recepción, la longitud del datagrama y el orden de secuencia del datagrama. Esta información se facilita si el datagrama supera el tamaño de bytes permitido para los paquetes de red y debe fragmentarse.

Capa de vínculo de datos: ubicación de la estructuración

Los protocolos de capa de vínculo de datos, como PPP, colocan el datagrama IP en una *estructura*. Estos protocolos adjuntan un tercer encabezado y un pie de página para crear una estructura del datagrama. El encabezado de la estructura incluye un campo de *comprobación de la redundancia cíclica* (CRC) que comprueba si se producen errores al transferir la estructura por el medio de red. A continuación, la capa del vínculo de datos transfiere la estructura a la capa física.

Capa de red física: ubicación de envío y recepción de estructuras

La capa de red física del host de envío recibe las estructuras y convierte las direcciones IP en las direcciones de hardware adecuadas para el medio de red. A continuación, la capa de red física envía la estructura a través del medio de red.

Administración del paquete por parte del host de recepción

Cuando el paquete llega al host de recepción, se transfiere a través de la pila de protocolo TCP/IP en el orden inverso al envío. La [Figura 1–1](#) ilustra esta ruta. Asimismo, cada protocolo del host de recepción filtra la información de encabezado que adjunta al paquete su equivalente en el host de envío. Tiene lugar el siguiente proceso:

1. La capa de red física recibe el paquete con el formato de estructura. La capa de red física procesa la CRC del paquete y luego envía la misma estructura a la capa del vínculo de datos.
2. La capa del vínculo de datos comprueba que la CRC de la estructura sea correcta y filtra el encabezado de la estructura y la CRC. Finalmente, el protocolo del vínculo de datos envía la estructura a la capa de Internet.
3. La capa de Internet lee la información del encabezado para identificar la transmisión. A continuación, la capa de Internet determina si el paquete es un fragmento. Si la transmisión está fragmentada, el protocolo IP reúne los fragmentos en el datagrama original. A continuación, IP filtra el encabezado de IP y transfiere el datagrama a los protocolos de capa de transporte.

4. La capa de transporte (TCP, SCTP y UDP) lee el encabezado para determinar qué protocolo de capa de aplicación debe recibir los datos. A continuación, TCP, SCTP o UDP filtra el encabezado relacionado. TCP, SCTP o UDP envía el mensaje o el flujo a la aplicación de recepción.
5. La capa de aplicación recibe el mensaje. A continuación, la capa de aplicación lleva a cabo la operación que solicita el host de envío.

Admisión de seguimiento interno de TCP/IP

TCP/IP proporciona admisión de seguimiento interno registrando la comunicación TCP cuando un paquete RST finaliza una conexión. Cuando se transmite o recibe un paquete RST, con la información de conexión se registra la información de hasta 10 paquetes que se acaban de transmitir.

Información adicional sobre TCP/IP e Internet

Hay una gran cantidad de información disponible sobre TCP/IP e Internet. Si necesita información específica que no se incluye en este texto, probablemente la encuentre en las fuentes que se citan a continuación.

Manuales sobre TCP/IP

Encontrará múltiples manuales sobre TCP/IP e Internet en bibliotecas o librerías especializadas. Los dos libros siguientes se consideran clásicos sobre TCP/IP:

- Craig Hunt. *TCP/IP Network Administration*: Este manual contiene algo de teoría y mucha información práctica para la administración de una red TCP/IP heterogénea.
- W. Richard Stevens. *TCP/IP Illustrated, Volume I*: Este manual profundiza en los protocolos TCP/IP. Resulta ideal para los administradores de redes que requieren conocimientos técnicos sobre TCP/IP y para los programadores de redes.

Páginas web sobre TCP/IP y redes

En Internet existe una gran cantidad de páginas web y grupos de usuarios dedicados a los protocolos TCP/IP y su administración. Muchos fabricantes, entre ellos Oracle Corporation, ofrecen recursos en línea de información general sobre TCP/IP. A continuación se incluyen algunos recursos web útiles con información sobre TCP/IP y la administración general del sistema. La tabla muestra sitios web relevantes y descripciones de la información sobre redes que contienen.

Sitio web	Descripción
The Internet Engineering Task Force (IETF) web site (http://www.ietf.org/home.html)	IETF es el organismo responsable de la arquitectura y el gobierno de Internet. La página web de IETF contiene información sobre las distintas actividades que lleva a cabo este organismo. Asimismo, incluye vínculos a las principales publicaciones del IETF.
Portal BigAdmin de Oracle Corporation (http://www.oracle.com/technetwork/systems/index.html)	BigAdmin ofrece información sobre la administración de equipos Sun. En esta página, encontrará preguntas frecuentes, recursos, foros, vínculos a documentación y otros materiales relativos a la administración de Oracle Solaris 10, incluidas las redes.

Peticiones de comentarios y borradores de Internet

Los grupos de trabajo de Internet Engineering Task Force (IETF) publican documentos sobre estándares conocidos como *Requests for Comments* (RFC o peticiones de comentarios). Los estándares que se están desarrollando se publican como borradores de Internet en *Internet Drafts*. El Comité de Arquitectura de Internet (Internet Architecture Board o IAB) debe aprobar todas las RFC antes de colocarlas en un dominio público. Normalmente, las RFC y los borradores de Internet se dirigen a los desarrolladores y otros usuarios con gran experiencia técnica. Sin embargo, hay una serie de RFC que abordan temas de TCP/IP e incluyen información valiosa para los administradores de sistemas. Estas RFC se citan en varios lugares de este manual.

Generalmente, las RFC incluyen un subconjunto de documentos For Your Information (FYI o para su información). Los FYI contienen información que no es relativa a los estándares de Internet. Contienen información de Internet más general. Por ejemplo, los documentos FYI incluyen una bibliografía con manuales y documentos de introducción a TCP/IP. Los documentos FYI constituyen un compendio exhaustivo de las herramientas de software relacionadas con Internet. Finalmente, incluyen un glosario de los términos de redes generales y de Internet.

Encontrará referencias a RFC relevantes en esta guía y en otros manuales para los administradores de Oracle Solaris.

P A R T E I I

Administración de TCP/IP

Esta parte contiene tareas e información conceptual para poder configurar, administrar y resolver problemas de redes TCP/IP.

Planificación de la red TCP/IP (tareas)

En este capítulo se describen las cuestiones que debe resolver para poder crear una red de un modo organizado y rentable. Una vez resueltas estas cuestiones, puede establecer una planificación de la red en la que se contemple la configuración y administración de la red en el futuro.

Este capítulo contiene la información siguiente:

- “Determinación del hardware de red” en la página 55
- “Cómo obtener el número de IP de la red” en la página 58
- “Cómo decidir el formato de las direcciones IP para la red” en la página 55
- “Entidades de denominación en la red” en la página 63
- “Planificación de enrutadores en la red” en la página 66

Para conocer las tareas necesarias para configurar una red, consulte el [Capítulo 5](#), “Configuración de servicios de red TCP/IP y direcciones IPv4 (tareas)”.

Planificación de la red (mapa de tareas)

La tabla siguiente muestra diferentes tareas para configurar la red. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener información
1. Planificar los requisitos de hardware y la topología de red.	Determina los tipos de equipo que se necesitan y la distribución de los equipos en el sitio.	<ul style="list-style-type: none"> ■ Para ver cuestiones generales sobre la topología de red, consulte “Determinación del hardware de red” en la página 55. ■ Para conocer la planificación de la topología de IPv6, consulte “Preparación de la topología red para admitir IPv6” en la página 90. ■ Para obtener información sobre un tipo de equipo específico, consulte la documentación del fabricante del equipo.
2. Obtener una dirección IP registrada para la red.	La red debe tener una dirección IP única si tiene previsto comunicarse fuera de su red local, por ejemplo, a través de Internet.	Consulte “Cómo obtener el número de IP de la red” en la página 58.
3. Crear una planificación de las direcciones IP para los sistemas, basándose en su prefijo de red IPv4 o el prefijo de sitio IPv6.	Determine cuántas direcciones se deben instalar en el sitio.	Consulte “Cómo diseñar un esquema de direcciones IPv4” en la página 58 o “Preparación de un plan de direcciones IPv6” en la página 94.
4. Crear una lista que contenga las direcciones IP y los nombres de host de todos los equipos de la red.	Utilice la lista para crear bases de datos de red.	Consulte “Bases de datos de red” en la página 64.
5. Determinar qué servicio de nombres utilizar en la red.	Permite decidir si utilizar NIS, LDAP, DNS o las bases de datos de red en el directorio /etc local.	Consulte “Selección de un servicio de nombres y de directorios” en la página 64.
6. Establecer subdivisiones administrativas, si la red lo requiere.	Decida si el sitio precisa la división de la red en subdivisiones administrativas.	Consulte “Subdivisiones administrativas” en la página 66.
7. Determinar dónde colocar los enrutadores en el diseño de la red.	Si la red es lo suficientemente grande como para requerir el uso de enrutadores, cree una topología de red que los admita.	Consulte “Planificación de enrutadores en la red” en la página 66.

Tarea	Descripción	Para obtener información
8. Si es preciso, diseñar una estrategia para las subredes.	Es posible que deba crear subredes para la administración del espacio de direcciones IP o para que haya más direcciones IP disponibles para los usuarios.	Para la planificación de subredes IPv4, consulte “¿Qué son las subredes?” en la página 240. Para la planificación de subredes IPv6, consulte “Creación de un esquema de numeración para subredes” en la página 95.

Determinación del hardware de red

Al diseñar la red, debe decidir qué tipo de red se adapta mejor a su organización. Algunas de las decisiones de planificación que debe tomar están relacionadas con el hardware de red siguiente:

- La topología de red, el diseño y las conexiones del hardware de red
- El número de sistemas host que admite la red
- Los tipos de host que admite la red
- Los tipos de servidores que puede necesitar
- El tipo de medio de red que utilizará: Ethernet, Token Ring, FDDI, etc.
- Si necesita puentes o enrutadores que extiendan este medio o conecten la red local a redes externas
- Si algunos sistemas requieren interfaces adquiridas por separado además de sus interfaces integradas

Teniendo en cuenta estos factores, puede determinar el tamaño de la red de área local.

Nota – En este manual no se aborda el tema de la planificación del hardware de red. Para obtener ayuda, consulte los manuales que se proporcionan con el hardware.

Cómo decidir el formato de las direcciones IP para la red

El número de sistemas que desea que sean compatibles determina la configuración de la red. Es posible que su organización requiera una pequeña red de varias docenas de sistemas independientes ubicados en una única planta de un edificio. También es posible que requiera la configuración de una red con más de 1.000 sistemas ubicados en varios edificios. Esta configuración podría hacer necesaria la división de la red en subdivisiones denominadas *subredes*.

Cuando planifique el esquema de direcciones de red, tenga en cuenta los siguientes factores:

- El tipo de dirección IP que desea utilizar: IPv4 o IPv6
- El número de sistemas potenciales de la red
- El número de sistemas que son enrutadores o sistemas de host múltiple, que requieren una dirección IP para cada interfaz
- Si se utilizarán direcciones privadas en la red
- Si habrá un servidor DHCP que administre las agrupaciones de direcciones IPv4

El crecimiento mundial de Internet desde 1990 ha derivado en la escasez de direcciones IP disponibles. Para solucionar esta situación, Internet Engineering Task Force (IETF) ha desarrollado una serie de alternativas a las direcciones IP.

Si se ha asignado a su organización más de una dirección IP para la red o si utiliza subredes, designe una autoridad centralizada en su organización para asignar las direcciones IP. Dicha autoridad debe controlar una agrupación de direcciones IP de red asignadas, y asignar las direcciones de red, subred y host según sea necesario. Para evitar problemas, asegúrese de que no haya números de red duplicados ni aleatorios en su organización. Los tipos de direcciones IP que se utilizan actualmente son:

Direcciones IPv4

Estas direcciones de 32 bits son el formato original de direcciones IP diseñado para TCP/IP. Originalmente, existen tres clases de direcciones IP: A, B y C. El *número de red* que se asigna a una red refleja esta designación de clase más 8 o más bits para representar un host. Las direcciones IPv4 basadas en clases requieren la configuración de una máscara de red para el número de red. Asimismo, para que hayan más direcciones disponibles para los sistemas de la red local, estas direcciones a menudo se dividen en subredes.

Actualmente, se hace referencia a las direcciones IP como *direcciones IPv4*. Aunque los ISP ya no proporcionan números de red IPv4 basados en clases, muchas redes existentes siguen teniéndolos. Si desea más información sobre la administración de direcciones IPv4, consulte [“Cómo diseñar un esquema de direcciones IPv4” en la página 60](#).

Direcciones IPv4 en formato CIDR

IETF ha desarrollado las direcciones CIDR (Classless Inter-Domain Routing) como solución a corto y medio plazo para la escasez de direcciones IPv4. Asimismo, el formato CIDR se ha diseñado como solución para la falta de capacidad de las tablas de enrutamiento de Internet globales. Una dirección IPv4 con notación CIDR tiene una longitud de 32 bits y el mismo formato decimal con punto. Sin embargo, CIDR agrega una designación de prefijo después del byte de la derecha para definir la parte de red de la dirección IPv4. Para más información, consulte [“Cómo diseñar un esquema de direcciones IPv4 CIDR” en la página 61](#).

Direcciones DHCP

El protocolo DHCP (Dynamic Host Configuration Protocol o protocolo dinámico de configuración de host) permite a un sistema recibir información de configuración de un servidor DHCP, incluida una dirección IP, como parte del proceso de inicio. Los servidores DHCP cuentan con agrupaciones de direcciones IP desde las que se asignan direcciones a los clientes DHCP. Un sitio que utilice DHCP puede utilizar una agrupación de direcciones IP menor que la que se necesitaría si todos los clientes tuvieran asignada una dirección IP permanente. Puede configurar el servicio DHCP para administrar las direcciones IP del sitio, o parte de ellas. Para más información, consulte el [Capítulo 12, “Acerca de DHCP \(descripción general\)”](#).

Direcciones IPv6

IETF ha creado las direcciones IPv6 de 128 bits como solución a largo plazo para la escasez de direcciones IPv4 disponibles. Las direcciones IPv6 proporcionan un espacio de direcciones mayor que el que hay disponible con las direcciones IPv4. Oracle Solaris admite direcciones IPv4 e IPv6 en el mismo host, gracias al uso de la pila doble de TCP/IP. Al igual que las direcciones IPv4 en formato CIDR, las direcciones IPv6 no tienen nociones de clases o máscaras de red. Al igual que en el formato CIDR, las direcciones IPv6 utilizan prefijos para designar la parte de la dirección que define la red del sitio. Para ver una introducción a IPv6, consulte [“Descripción general de las direcciones IPv6” en la página 76](#).

Direcciones privadas y prefijos de documentación

La IANA ha reservado un bloque de direcciones IPv4 y un prefijo de sitio IPv6 para utilizar en redes privadas. Puede implementar estas direcciones en sistemas de una red de empresa, pero teniendo en cuenta que los paquetes con direcciones privadas no se pueden enrutar a través de Internet. Si desea más información sobre las direcciones privadas, consulte [“Uso de direcciones IPv4 privadas” en la página 62](#).

Nota – Las direcciones IPv4 privadas también se reservan para fines de documentación. Los ejemplos de este manual utilizan direcciones IPv4 privadas y el prefijo de documentación de IPv6 reservado.

Cómo obtener el número de IP de la red

Una red IPv4 se define con una combinación de un número de red IPv4 más una *máscara de red*. Una red IPv6 se define mediante el *prefijo de sitio* y si cuenta con subredes mediante el *prefijo de subred*.

A menos que la red vaya a ser siempre privada, los usuarios locales seguramente necesitarán comunicarse más allá de la red local. Por tanto, es preciso obtener un número de IP registrado para la red de la organización pertinente antes de que la red se pueda comunicar con el exterior. Esta dirección pasará a ser el número de red para el esquema de direcciones IPv4 o el prefijo de sitio para el esquema de direcciones IPv6.

Los proveedores de servicios de Internet proporcionan direcciones IP para las redes cuyos precios se basan en los distintos niveles de servicio. Compare los diferentes ISP para determinar cuál de ellos proporciona el mejor servicio para su red. Los ISP normalmente ofrecen a las empresas direcciones asignadas dinámicamente o direcciones IP estáticas. Algunos ISP ofrecen direcciones tanto IPv4 como IPv6.

Si su sitio es un ISP, obtiene bloques de direcciones IP para los clientes a través de un registro de Internet (IR) para su configuración regional. La Autoridad de números asignados de Internet (IANA o Internet Assigned Numbers Authority) es la principal responsable de la delegación de direcciones IP registradas a los registros de Internet de todo el mundo. Cada IR cuenta con información de registro y plantillas para la configuración regional en la que el IR ofrece el servicio. Para obtener información sobre la IANA y sus IR, consulte la [página de servicio de direcciones IP de IANA \(http://www.iana.org/ipaddress/ip-addresses.htm\)](http://www.iana.org/ipaddress/ip-addresses.htm).

Nota – No asigne direcciones IP de forma arbitraria a la red, aunque no esté conectando la red a redes TCP/IP externas. En lugar de ello, utilice direcciones privadas tal como se describe en “Uso de direcciones IPv4 privadas” en la página 62.

Cómo diseñar un esquema de direcciones IPv4

Nota – Para obtener información sobre la planificación de direcciones IPv6, consulte “Preparación de un plan de direcciones IPv6” en la página 94.

En esta sección se ofrece una descripción general de las direcciones IPv4 para ayudarle a diseñar un plan de direcciones IPv4. Para obtener información sobre las direcciones IPv6, consulte “Descripción general de las direcciones IPv6” en la página 76. Para obtener información sobre las direcciones DHCP, consulte el [Capítulo 12, “Acerca de DHCP \(descripción general\)”](#).

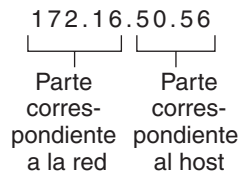
Cada red basada en IPv4 debe contar con:

- Un número de red exclusivo asignado por un ISP, un IR o, para las redes más antiguas, registrado por la IANA. Si tiene previsto utilizar direcciones privadas, los números de red que cree deben ser exclusivos en su organización.
- Direcciones IPv4 exclusivas para las interfaces de cada sistema en la red.
- Una máscara de red.

La dirección IPv4 es un número de 32 bits que identifica de forma exclusiva una interfaz de red en un sistema, tal como se explica en [“Aplicación de las direcciones IP a las interfaces de red” en la página 63](#). Una dirección IPv4 se escribe en dígitos decimales, y se divide en cuatro campos de 8 bits separados por puntos. Cada campo de 8 bits representa un byte de la dirección IPv4. Este modo de representar los bytes de una dirección IPv4 se denomina normalmente *formato de decimales con puntos*.

La figura siguiente muestra los componentes de una dirección IPv4, 172.16.50.56.

FIGURA 2-1 Formato de direcciones IPv4

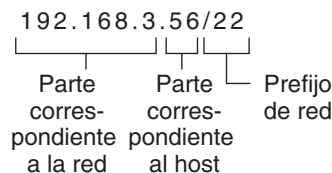


- 172.16 Número de red IPv4 registrada. En la notación IPv4 basada en clases, este número también define la clase de red IP (la clase B en este ejemplo), que registra la IANA.
- 50.56 Parte del host de la dirección IPv4. La parte del host identifica de forma exclusiva una interfaz en un sistema de una red. Para cada interfaz de una red local, la parte de la red de la dirección es la misma, pero la parte del host debe ser diferente.

Si tiene previsto crear una subred de una red IPv4 basada en clases, debe definir una máscara de subred o *máscara de red*, tal como se describe en [“Base de datos netmasks” en la página 240](#).

El ejemplo siguiente muestra la dirección de formato CIDR 192.168.3.56/22

FIGURA 2-2 Dirección IPv4 de formato CIDR



- 192 . 168 . 3
- Parte de la red, que se compone del número de red IPv4 que se recibe de un ISP o un IR.
- 56
- Parte del host, que se asigna a una interfaz de un sistema.
- /22
- Prefijo de la red, que define cuántos bits de la dirección componen el número de red. El prefijo de la red también proporciona la máscara de subred para la dirección IP. Los prefijos de red también los asigna el ISP o el IR.

Una red basada en Oracle Solaris puede combinar direcciones IPv4 estándar, direcciones IPv4 con formato CIDR, direcciones DHCP, direcciones IPv6 y direcciones IPv4 privadas.

Cómo diseñar un esquema de direcciones IPv4

Esta sección describe las clases en las que se organizan las direcciones IPv4 estándar. Aunque la IANA ya no proporciona números de red basados en clases, estos números siguen utilizándose en muchas redes. Es posible que necesite administrar el espacio de dirección de un sitio con números de red basados en clases. Para obtener una explicación completa de las clases de red IPv4, consulte [“Clases de red” en la página 254](#).

La tabla siguiente muestra la división de la dirección IPv4 estándar en espacios de direcciones de red y de host. Para cada clase, el rango especifica el intervalo de valores decimales del primer byte del número de red. La dirección de red indica el número de bytes de la dirección IPv4 que se dedican a la parte de red de la dirección. Cada byte se representa con xxx. La dirección de host indica el número de bytes que se dedican a la parte del host de la dirección. Por ejemplo, en una dirección de red de clase A, el primer byte está dedicado a la red y los tres últimos bytes al host. Para las redes de clase C se aplica la designación opuesta.

TABLA 2-1 División de las clases IPv4

Clase	Intervalo de bytes	Número de red	Dirección de host
A	0–127	xxx	xxx.xxx. xxx
B	128–191	xxx.xxx	xxx.xxx
C	192–223	xxx.xxx. xxx	xxx

Los números del primer byte de la dirección IPv4 definen si la red es de clase A, B o C. Los tres bytes restantes comprenden el intervalo 0–255. Los números 0 y 255 están reservados. Puede asignar los números del 1 al 254 a cada byte, dependiendo de la clase de red que la IANA asignó a su red.

La tabla siguiente muestra qué bytes de la dirección IPv4 tiene asignados. La tabla también muestra el intervalo de números de cada byte que tiene a su disposición para asignarlos a los hosts.

TABLA 2-2 Intervalo de clases IPv4 disponibles

Clase de red	Intervalo de bytes 1	Intervalo de bytes 2	Intervalo de bytes 3	Intervalo de bytes 4
A	0–127	1–254	1–254	1–254
B	128–191	Preasignado por la IANA	1–254	1–254
C	192–223	Preasignado por la IANA	Preasignado por la IANA	1–254

Número de subred IPv4

Las redes locales con grandes cantidades de hosts a veces se dividen en subredes. Si divide el número de red IPv4 en subredes, debe asignar un identificador de red a cada subred. Puede alcanzar la máxima eficacia del espacio de dirección IPv4 utilizando algunos de los bits de la parte de host de la dirección IPv4 como identificador de red. Cuando se utiliza como identificador de red, la parte especificada de la dirección pasa a ser el número de subred. Un número de subred se crea utilizando una máscara de red, que es una máscara de bits que selecciona las partes de red y subred de una dirección IPv4. Consulte [“Creación de la máscara de red para las direcciones IPv4” en la página 241](#) para más información.

Cómo diseñar un esquema de direcciones IPv4 CIDR

Las clases de red que originalmente constituían IPv4 ya no se utilizan en Internet. Actualmente, la IANA distribuye direcciones e formato CIDR sin clase a sus registros de todo el mundo. Cualquier dirección IPv4 que obtenga de un ISP tendrá el formato CIDR, tal como se muestra en la [Figura 2-2](#).

El prefijo de red de la dirección CIDR indica cuántas direcciones IPv4 hay disponibles para los hosts de su red. Tenga en cuenta que estas direcciones de host se asignan a las interfaces de un host. Si un host tiene más de una interfaz física, debe asignar una dirección de host para cada interfaz física que se utilice.

El prefijo de red de una dirección CIDR también define la longitud de la máscara de subred. La mayoría de los comandos de Oracle Solaris 10 reconocen la designación del prefijo CIDR de una máscara de subred de una red. No obstante, el programa de instalación de Oracle Solaris y `/etc/netmask file` hacen necesaria la configuración de la máscara de subred utilizando la notación decimal con punto. En ambos casos, utilice la representación decimal con punto del prefijo de red CIDR, tal como se muestra en la tabla.

TABLA 2-3 Prefijos CIDR y su equivalente decimal

Prefijo de red CIDR	Direcciones IP disponibles	Equivalente de subred decimal con punto
/19	8,192	255.255.224.0
/20	4,096	255.255.240.0
/21	2,048	255.255.248.0
/22	1024	255.255.252.0
/23	512	255.255.254.0
/24	256	255.255.255.0
/25	128	255.255.255.128
/26	64	255.255.255.192
/27	32	255.255.255.224

Para obtener más información sobre las direcciones CIDR, consulte estas fuentes:

- Para obtener información técnica sobre CIDR, consulte [RFC 1519, Classless Inter-Domain Routing \(CIDR\): una estrategia de agregación y asignación de direcciones](http://www.ietf.org/rfc/rfc1519.txt?number=1519) (<http://www.ietf.org/rfc/rfc1519.txt?number=1519>).
- Si desea más información general sobre CIDR, consulte la página de Pacific Bell Internet en [Classless Inter-Domain Routing \(CIDR\) Overview](http://www.wirelesstek.com/cidr.htm) (<http://www.wirelesstek.com/cidr.htm>).
- Puede encontrar otra descripción general de CIDR en el artículo de la Wikipedia "CIDR (Classless inter-domain routing)" (http://en.wikipedia.org/wiki/Classless_inter-domain_routing).

Uso de direcciones IPv4 privadas

La IANA ha reservado tres bloques de direcciones IPv4 para que las compañías las utilicen en sus redes privadas. Estas direcciones aparecen definidas en [RFC 1918, Address Allocation for Private Internets](http://www.ietf.org/rfc/rfc1918.txt?number=1918) (<http://www.ietf.org/rfc/rfc1918.txt?number=1918>). Puede utilizar estas *direcciones privadas*, conocidas también como direcciones 1918, para los sistemas de las redes locales de una intranet corporativa. Sin embargo, las direcciones privadas no son válidas en Internet. No las utilice en sistemas que deban comunicarse fuera de la red local.

La tabla siguiente muestra los intervalos de direcciones IPv4 privadas y sus correspondientes máscaras de red.

Intervalo de direcciones IPv4	Máscara de red
10.0.0.0 - 10.255.255.255	10.0.0.0
172.16.0.0 - 172.31.255.255	172.16.0.0
192.168.0.0 - 192.168.255.255	192.168.0.0

Aplicación de las direcciones IP a las interfaces de red

Para conectarse a la red, un sistema debe tener como mínimo una *interfaz de red física*. Cada interfaz de red debe tener su propia dirección IP exclusiva. Durante la instalación de Oracle Solaris, debe proporcionar la dirección IP para la primera interfaz que encuentre el programa de instalación. Normalmente dicha interfaz se denomina *nombre_dispositivo0*, por ejemplo *eri0* o *hme0*. Esta interfaz se considera la *interfaz de red principal*.

Si añade una segunda interfaz de red a un host, dicha interfaz también debe tener su propia dirección IP exclusiva. Al agregar la segunda interfaz de red, el host pasa a ser un *host múltiple*. En cambio, al agregar una segunda interfaz de red a un host y activar el reenvío de IP, dicho host pasa a ser un enrutador. Consulte [“Configuración de un enrutador IPv4” en la página 121](#) para obtener una explicación.

Cada interfaz de red tiene un nombre de dispositivo, un controlador de dispositivo y un archivo de dispositivo asociado en el directorio `/devices`. La interfaz de red puede tener un nombre de dispositivo como *eri* o *smc0*, que son nombres de dispositivo para dos interfaces Ethernet de uso común.

Si desea información sobre las tareas relacionadas con las interfaces, consulte [Capítulo 6, “Administración de interfaces de red \(tareas\)”](#).

Nota – En este manual se presupone que se está trabajando con sistemas que tengan interfaces de red Ethernet. Si tiene previsto utilizar diferentes medios de red, consulte los manuales que se incluyen con la interfaz de red para obtener información sobre la configuración.

Entidades de denominación en la red

Después de recibir su dirección IP de red asignada y de asignar las direcciones IP a los sistemas, debe asignar los nombres a los hosts. A continuación, debe determinar cómo administrar los servicios de nombres de la red. Estos nombres se utilizan inicialmente al configurar la red y después al expandirla por enrutadores, puentes y PPP.

Los protocolos TCP/IP localizan un sistema en una red utilizando su dirección IP. Sin embargo, si utiliza un nombre reconocible, puede identificar fácilmente el sistema. En consecuencia, los protocolos TCP/IP (y Oracle Solaris) requieren tanto la dirección IP como el nombre de host para identificar un sistema de modo exclusivo.

Desde el punto de vista del protocolo TCP/IP, una red es un conjunto de entidades con nombre. Un host es una entidad con un nombre. Un enrutador es una entidad con un nombre. La red es una entidad con un nombre. Del mismo modo, se puede asignar un nombre a un grupo o departamento en el que esté instalada la red, así como a una división, región o compañía. En teoría, la jerarquía de nombres que se pueden utilizar para identificar una red prácticamente no tiene límites. El nombre de dominio identifica un *dominio*.

Administración de nombres de host

Muchos sitios permiten a los usuarios elegir los nombres de host para sus equipos. Los servidores también requieren como mínimo un nombre de host, asociado a la dirección IP de su interfaz de red principal.

Como administrador del sistema, debe asegurarse de que cada nombre de host de su dominio sea exclusivo. En otros términos, no puede haber dos equipos en la red que tengan el nombre de "fred". Sin embargo, el equipo "fred" puede tener múltiples direcciones IP.

Cuando planifique su red, realice una lista de las direcciones IP y sus nombres de host asociados para poder acceder a ellos fácilmente durante el proceso de configuración. Dicha lista le ayudará a verificar que todos los nombres de host sean exclusivos.

Selección de un servicio de nombres y de directorios

Oracle Solaris permite utilizar tres tipos de servicios de nombres: archivos locales, NIS y DNS. Los servicios de nombres contienen información crítica sobre los equipos de una red, como los nombres de host, las direcciones IP, las direcciones Ethernet, etc. Oracle Solaris también permite utilizar el servicio de directorios LDAP además de un servicio de nombres, o en lugar de él. Para ver una introducción a los servicios de nombres de Oracle Solaris, consulte la [Parte I, “Acerca de los servicios de nombres y directorios” de Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

Bases de datos de red

Al instalar el sistema operativo, facilita el nombre de host y la dirección IP del servidor, los clientes o el sistema independiente como parte del procedimiento. El programa de instalación de Oracle Solaris incluye esta información en `hosts` y, en el caso de Solaris 10 11/06 y versiones anteriores de Solaris 10, la base de datos de red `ipnodes`. Esta base de datos forma parte de un conjunto de bases de datos de red que contienen la información necesaria para el funcionamiento de TCP/IP en la red. El servicio de nombres que seleccione para la red leerá estas bases de datos.

La configuración de las bases de datos de red es imprescindible. Debe decidir qué servicio de nombres utilizará como parte del proceso de planificación de la red. Asimismo, la decisión de

utilizar servicios de nombres también determina si organizará la red en un dominio administrativo. “[Bases de datos de red y el archivo `nsswitch.conf`](#)” en la [página 244](#) incluye información detallada sobre el conjunto de bases de datos de red.

Uso de NIS o DNS como servicio de nombres

Los servicios de nombres NIS y DNS crean bases de datos de red en varios servidores de la red. [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#) describe estos servicios de nombres y explica cómo configurar las bases de datos. Asimismo, la guía explica de forma pormenorizada los conceptos de "espacio de nombres" y "dominio administrativo".

Uso de archivos locales como servicio de nombres

Si no implementa NIS, LDAP o DNS, la red utiliza *archivos locales* para proporcionar el servicio de nombres. El término "archivos locales" hace referencia a la serie de archivos del directorio /etc que utilizan las bases de datos de red. En los procedimientos de este manual se presupone que está utilizando archivos locales para el servicio de nombres, a menos que se especifique lo contrario.

Nota – Si decide utilizar archivos locales como servicio de nombres para la red, puede configurar otro servicio de nombres posteriormente.

Nombres de dominio

Muchas redes organizan sus hosts y enrutadores en una jerarquía de dominios administrativos. Si utiliza el servicio de nombres NIS o DNS, debe seleccionar un nombre de dominio para la organización que sea exclusivo en todo el mundo. Para asegurarse de que su nombre de dominio sea exclusivo, debe registrarlo con InterNIC. Si tiene previsto utilizar DNS, también debe registrar su propio nombre de dominio con InterNIC.

La estructura del nombre de dominio es jerárquica. Un nuevo dominio normalmente se ubica debajo de un dominio relacionado que ya existe. Por ejemplo, el nombre de dominio para una compañía subsidiaria puede ubicarse debajo el dominio de su compañía principal. Si el nombre de dominio no tiene otra relación, una organización puede colocar su nombre de dominio directamente debajo de uno de los dominios que hay en el nivel superior.

A continuación se incluyen algunos ejemplos de dominios de nivel superior:

- .com: compañías comerciales (de ámbito internacional)
- .edu: instituciones educativas (de ámbito internacional)
- .gov: organismos gubernamentales estadounidenses
- .fr: Francia

Seleccione el nombre que identifique a su organización, teniendo en cuenta que debe ser exclusivo.

Subdivisiones administrativas

Las subdivisiones administrativas están relacionadas con el tamaño y el control. Cuantos mas hosts y servidores haya en una red, más compleja será la tarea de administración. Puede configurar divisiones administrativas adicionales si es preciso. Agregue redes de una clase específica. Divida las redes existentes en subredes. La decisión de configurar subdivisiones administrativas para su red la determinan los factores siguientes:

- **¿Qué tamaño tiene la red?**

Una única división administrativa puede controlar una única red de varios cientos de hosts, todo en la misma ubicación física y con los mismos servicios administrativos. Sin embargo, en ocasiones es preciso establecer varias subdivisiones administrativas. Las subdivisiones resultan especialmente útiles si tiene una red reducida con subredes y está repartida por un área geográfica extensa.

- **¿Los usuarios de la red tienen necesidades similares?**

Por ejemplo, puede tener una red confinada a un único edificio que admita un número de equipos relativamente reducido. Estos equipos se reparten en una serie de subredes. Cada subred admite grupos de usuarios con diferentes necesidades. En este ejemplo, puede utilizar una subdivisión administrativa para cada subred.

Planificación de enrutadores en la red

Tenga en cuenta que en el protocolo TCP/IP existen dos tipos de entidades en una red: hosts y enrutadores. Mientras que todas las redes requieren un host, no es necesario que tengan un enrutador. La topología física de la red determina la necesidad de enrutadores. En esta sección se introducen los conceptos de topología de red y enrutamiento. Estos conceptos son importantes cuando decide agregar otra red a su entorno de red.

Nota – Para ver las tareas y detalles completos para la configuración de los enrutadores en las redes IPv4, consulte [“Reenvío de paquetes y rutas en redes IPv4” en la página 114](#). Para ver las tareas y detalles completos para la configuración de los enrutadores en las redes IPv6, consulte [“Configuración de un enrutador IPv6” en la página 177](#).

Descripción general de la topología de red

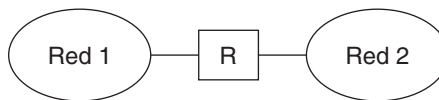
La topología de red describe cómo encajan las redes. Los enrutadores son las entidades que conectan las redes entre sí. Un enrutador es un equipo que tiene dos o más interfaces de red e implementa el reenvío de IP. Sin embargo, el sistema no puede funcionar como enrutador hasta que esté configurado tal como se describe en [“Configuración de un enrutador IPv4” en la página 121](#).

Los enrutadores conectan dos o más redes para formar interredes mayores. Los enrutadores deben configurarse para transferir paquetes entre dos redes adyacentes. Los enrutadores también deben poder transferir paquetes a redes que se encuentran fuera de las redes adyacentes.

La figura siguiente muestra las partes básicas de una topología de red. La primera ilustración muestra una configuración sencilla de dos redes conectadas por un único enrutador. La segunda ilustración muestra una configuración de tres redes, interconectadas por dos enrutadores. En el primer ejemplo, el enrutador R une la red 1 y la red 2 en una interred mayor. En el segundo ejemplo, el enrutador 1 conecta las redes 1 y 2. El enrutador R2 conecta las redes 2 y 3. Las conexiones de una red que incluye las redes 1, 2 y 3.

FIGURA 2-3 Topología de red básica

Dos redes conectadas mediante un encaminador



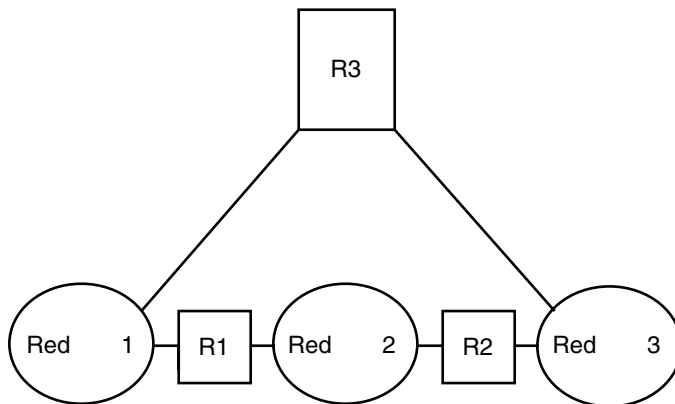
Tres redes conectadas mediante dos encaminadores



Además de unir las redes en interredes, los enrutadores transfieren los paquetes entre las redes que se basan en las direcciones de la red de destino. A medida que las interredes se hacen más complejas, cada enrutador debe tomar más decisiones sobre los destinos de los paquetes.

La figura siguiente muestra un caso más complejo. El enrutador R3 conecta las redes 1 y 3. La redundancia aumenta la fiabilidad. Si la red 2 no funciona, el enrutador R3 continúa proporcionando una ruta entre las redes 1 y 3. Se pueden interconectar muchas redes. No obstante, las redes deben utilizar los mismos protocolos de red.

FIGURA 2-4 Topología de red que proporciona una ruta adicional entre las redes



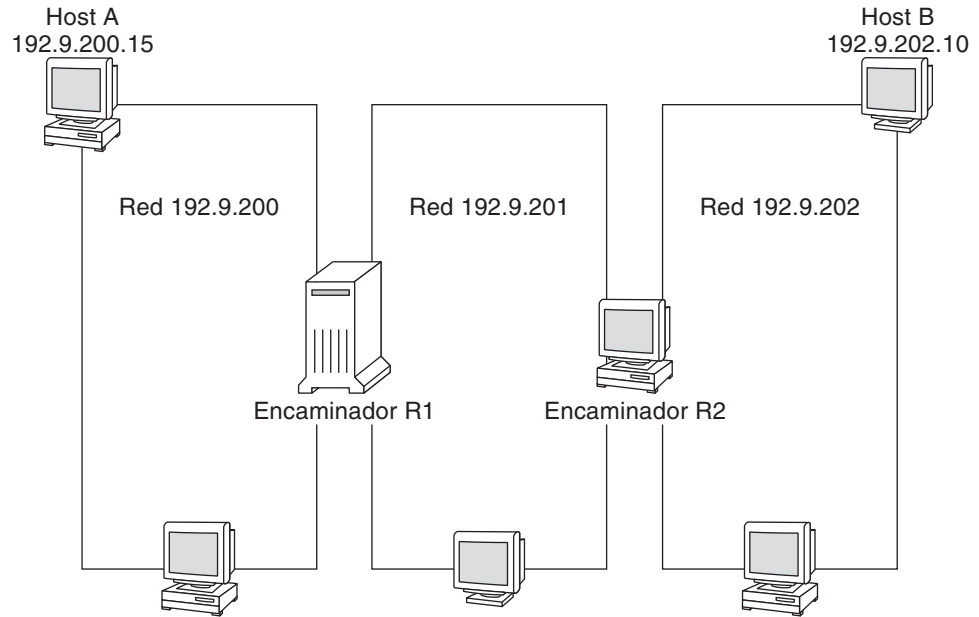
Cómo transfieren los paquetes los enrutadores

La dirección IP del receptor, que forma parte del encabezado del paquete, determina el modo en que se enruta el paquete. Si esta dirección incluye el número de red de la red local, el paquete va directamente al host con esa dirección IP. Si el número de red no es la red local, el paquete va al enrutador de la red local.

Los enrutadores contienen información de enrutamiento en las *tablas de enrutamiento*. Estas tablas contienen la dirección IP de los hosts y enrutadores de las redes a las que está conectado el enrutador. Las tablas también contienen punteros a esas redes. Cuando un enrutador recibe un paquete, comprueba su tabla de enrutamiento para determinar si la tabla incluye la dirección de destino en el encabezado. Si la tabla no contiene la dirección de destino, el enrutador envía el paquete a otro enrutador que aparezca en la tabla de enrutamiento. Si desea más información sobre los enrutadores, consulte [“Configuración de un enrutador IPv4” en la página 121](#).

La figura siguiente muestra una topología de red con tres redes que están conectadas con dos enrutadores.

FIGURA 2-5 Topología de red con tres redes interconectadas



El enrutador R1 conecta las redes 192.9.200 y 192.9.201. El enrutador R2 conecta las redes 192.9.201 y 192.9.202. Si el host A de la red 192.9.200 envía un mensaje al host B de la red 192.9.202, tienen lugar los siguientes eventos:

1. El host A envía un paquete a través de la red 192.9.200. El encabezado del paquete contiene la dirección IPv4 del host B receptor, 192.9.202.10.
2. Ninguno de los equipos de la red 192.9.200 tiene la dirección IPv4 192.9.202.10. Por tanto, el enrutador R1 acepta el paquete.
3. El enrutador R1 examina sus tablas de enrutamiento. Ningún equipo de la red 192.9.201 tiene la dirección 192.9.202.10. Sin embargo, las tablas de enrutamiento incluyen el enrutador R2.
4. A continuación, R1 selecciona R2 como enrutador para el "siguiente salto". R1 envía el paquete a R2.
5. Dado que R2 conecta la red 192.9.201 con 192.9.202, R2 tiene la información de enrutamiento para el host B. A continuación, el enrutador R2 envía el paquete a la red 192.9.202, en la que el host B acepta el paquete.

Introducción a IPv6 (descripción general)

Este capítulo presenta una descripción general de la implementación de Oracle Solaris IPv6 (Internet Protocol versión 6). Dicha implementación se compone del daemon asociado y utilidades compatibles con el espacio de direcciones IPv6.

Las direcciones IPv6 e IPv4 coexisten en el entorno de redes de Oracle Solaris. Los sistemas que se configuran con direcciones IPv6 mantienen sus direcciones IPv4, en caso de que tales direcciones ya existan. Las operaciones en que intervienen direcciones IPv6 no repercuten negativamente en operaciones de IPv4 y viceversa.

Se abordan los siguientes temas principales:

- “Características principales de IPv6” en la página 72
- “Descripción general de las redes IPv6” en la página 74
- “Descripción general de las direcciones IPv6” en la página 76
- “Descripción general del protocolo ND de IPv6” en la página 82
- “Configuración automática de direcciones IPv6” en la página 83
- “Descripción general sobre los túneles de IPv6” en la página 85

Para obtener más información relativa a IPv6, consulte los capítulos siguientes.

- Planificación de redes IPv6: Capítulo 4, “Planificación de una red IPv6 (tareas)”
- Tareas relacionadas con IPv6: Capítulo 7, “Configuración de una red IPv6 (tareas).” y Capítulo 8, “Administración de redes TCP/IP (tareas).”
- Información detallada de IPv6: Capítulo 11, “IPv6 en profundidad (referencia)”

Características principales de IPv6

La característica que distingue a IPv6 es un mayor espacio de dirección comparado con IPv4. Asimismo, IPv6 mejora la capacidad en Internet en numerosos aspectos, como se explica brevemente en esta sección.

Direcciones ampliadas

El tamaño de direcciones IP pasa de 32 bits en IPv4 a 128 bits en IPv6, para permitir más niveles en la jerarquía de direcciones. Aparte, IPv6 proporciona muchos más sistemas IPv6 con direcciones. Para obtener más información, consulte [“Descripción general de las direcciones IPv6” en la página 76](#).

Configuración automática de direcciones y descubrimiento de vecinos

El protocolo *ND* (*Neighbor Discovery, descubrimiento de vecinos*) de IPv6 facilita la configuración automática de direcciones IPv6. La *configuración automática* consiste en la capacidad de un host de IPv6 de generar automáticamente sus propias direcciones IPv6, cosa que facilita la administración de direcciones y supone un ahorro de tiempo. Para obtener más información, consulte [“Configuración automática de direcciones IPv6” en la página 83](#).

El protocolo ND se corresponde con una combinación de los siguientes protocolos IPv4: Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), Router Discovery (RDISC), e ICMP Redirect. Los enrutadores de IPv6 utilizan el protocolo ND para anunciar el prefijo de sitio de IPv6. Los hosts de IPv6 utilizan el descubrimiento de vecinos con varias finalidades, entre las cuales está solicitar el prefijo de un enrutador de IPv6. Para obtener más información, consulte [“Descripción general del protocolo ND de IPv6” en la página 82](#).

Simplificación del formato del encabezado

El formato del encabezado de IPv6 prescinde o convierte en opcionales determinados campos de encabezado de IPv4. Pese al mayor tamaño de las direcciones, este cambio hace que el encabezado de IPv6 consuma el mínimo ancho de banda posible. Aunque las direcciones IPv6 son cuatro veces mayores que las direcciones IPv4, el encabezado de IPv6 sólo tiene el doble de tamaño que el encabezado de IPv4.

Más posibilidades en las opciones de encabezado de IP

Los cambios en la forma de codificar las opciones de encabezado de IP permiten un reenvío más eficaz. Asimismo, las opciones de IPv6 presentan unos límites de longitud menos estrictos. Los cambios aportan una mayor flexibilidad a la hora de incorporar opciones nuevas en el futuro.

Compatibilidad de aplicaciones con direcciones IPv6

Muchos de los principales servicios de red de Oracle Solaris reconocen y admiten direcciones IPv6; por ejemplo:

- Servicios de nombres como DNS, LDAP y NIS. Para obtener más información sobre la compatibilidad de IPv6 con estos servicios de nombres, consulte *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*.
- Aplicaciones de autenticación y protección de la privacidad, por ejemplo IP Security Architecture (IPsec) e Internet Key Exchange (IKE). Para obtener más información, consulte la *Parte IV*.
- Servicios diferenciados, como los que proporciona IP Quality of Service (IPQoS). Para obtener más información, consulte la *Parte VII*.
- Detección de fallos y funcionamiento a prueba de fallos, como se proporciona mediante IP multirruta de redes (IPMP). Para obtener más información, consulte la *Parte VI*.

Otros recursos de IPv6

Además de esta parte, hay información adicional sobre IPv6 en las fuentes que se citan en las secciones siguientes.

Petición de comentarios IPv6 y borradores de Internet

Hay disponibles numerosas RFC referidas a IPv6. En la tabla siguiente aparecen los principales artículos y sus ubicaciones web de Internet Engineering Task Force (IETF) a partir de su escritura.

TABLA 3–1 Borradores de Internet y RFC relativos a IPv6

RFC o borrador de Internet	Tema	Ubicación
RFC 2461, <i>Neighbor Discovery for IP Version 6 (IPv6)</i>	Describe las características y funciones del protocolo ND (descubrimiento de vecinos) de IPv6	http://www.ietf.org/rfc/rfc2461.txt\$number=2461 (http://www.ietf.org/rfc/rfc2461.txt?number=2461)

TABLA 3-1 Borradores de Internet y RFC relativos a IPv6 (Continuación)

RFC o borrador de Internet	Tema	Ubicación
RFC 3306, <i>Unicast-Prefix-Based IPv6 Multicast Addresses</i>	Describe el formato y los tipos de direcciones IPv6 multidifusión	ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt (ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt)
RFC 3484: <i>Default Address Selection for Internet Protocol version 6 (IPv6)</i>	Describe los algoritmos que se usan en la selección de direcciones predeterminadas de IPv6	http://www.ietf.org/rfc/rfc3484?number=3484 (http://www.ietf.org/rfc/rfc3484.txt?number=3484)
RFC 3513, <i>Internet Protocol version 6 (IPv6) Addressing Architecture</i>	Contiene información exhaustiva sobre los tipos de direcciones IPv6 con abundantes ejemplos	http://www.ietf.org/rfc/rfc3513.txt?number=3513 (http://www.ietf.org/rfc/rfc3513.txt?number=3513)
RFC 3587, <i>IPv6 Global Unicast Address Format</i>	Define el formato estándar de las direcciones IPv6 unidifusión	http://www.ietf.org/rfc/rfc3587.txt?number=3587 (http://www.ietf.org/rfc/rfc3587.txt?number=3587)

Sitios web

Los sitios web siguientes aportan información útil sobre IPv6.

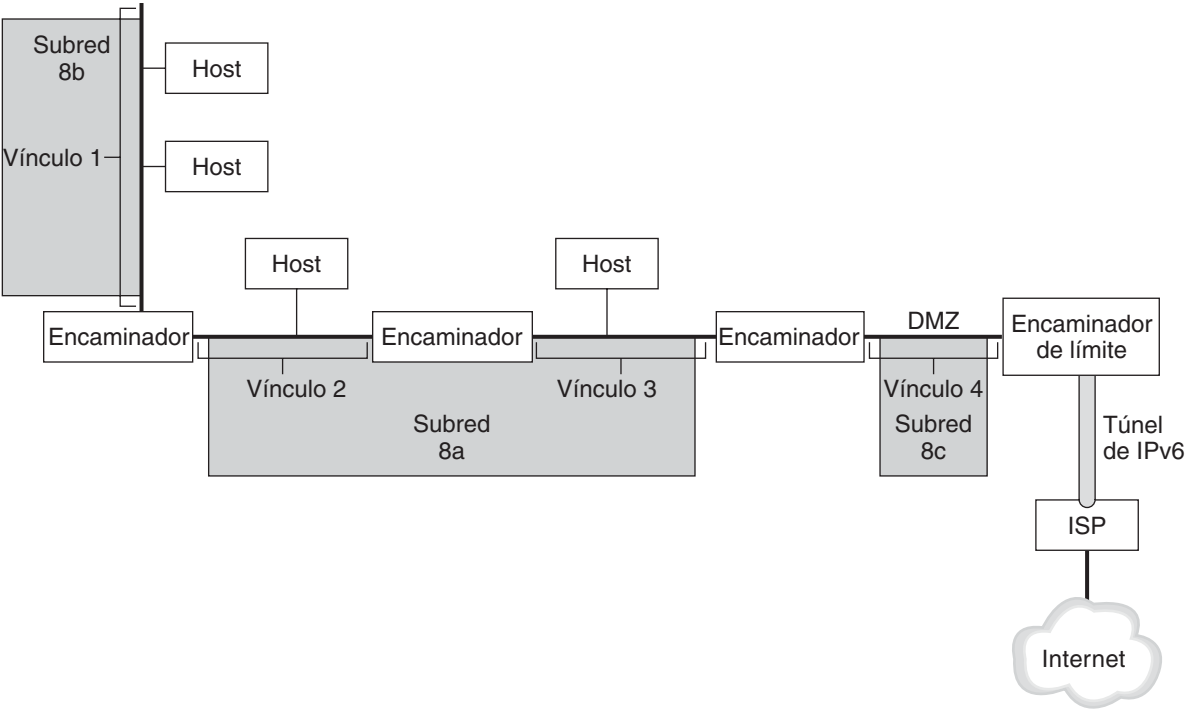
TABLA 3-2 Sitios web relacionados con IPv6

Sitio web	Descripción	Ubicación
Foro de IPv6	En este sitio web hay vínculos a presentaciones, eventos, clases e implementaciones sobre IPv6 en todo el mundo	http://www.ipv6forum.com
Grupo de trabajo de IPv6 de Internet Educational Task Force	La página inicial de este grupo de trabajo de IETF proporciona vínculos a todos los borradores de Internet y RFC importantes relacionados con IPv6	http://www.ietf.org/html.charters/ipv6-charter.html

Descripción general de las redes IPv6

En esta sección se presentan términos básicos en la topología de redes IPv6. En la figura siguiente se muestran los componentes básicos de una red IPv6.

FIGURA 3-1 Componentes básicos de una red IPv6



La figura ilustra una red IPv6 y sus conexiones con un ISP. La red interna consta de los vínculos 1, 2, 3 y 4. Los hosts rellenan los vínculos y un enrutador los termina. El vínculo 4, considerado la DMZ de la red, queda terminado en un extremo por el enrutador de límite. El enrutador de límite ejecuta un túnel IPv6 a un ISP, que ofrece conexión a Internet para la red. Los vínculos 2 y 3 se administran como subred 8a. La subred 8b tan sólo consta de sistemas en el vínculo 1. La subred 8c es contigua a la DMZ del vínculo 4.

Como se muestra en la [Figura 3-1](#), una red IPv6 tiene prácticamente los mismos componentes que una red IPv4. No obstante, la terminología de IPv6 presenta ligeras diferencias respecto a la de IPv4. A continuación se presenta una serie de términos sobre componentes de red empleados en un contexto de IPv6.

- nodo** Sistema con una dirección IPv6 y una interfaz configurada para admitir IPv6. Término genérico que se aplica a hosts y enrutadores.
- enrutador de IPv6** Nodo que reenvía paquetes de IPv6. Para admitir IPv6, debe configurarse como mínimo una de las interfaces del enrutador. Un enrutador de IPv6 también puede anunciar el prefijo de sitio IPv6 registrado para la empresa en la red interna.

host de IPv6	Nodo con una dirección IPv6. Un host IPv6 puede tener configurada más de una interfaz para que sea compatible con IPv6. Al igual que en IPv4, los hosts de IPv6 no reenvían paquetes.
vínculo	Un solo soporte contiguo de red conectado por un enrutador en cualquiera de sus extremos.
vecino	Nodo de IPv6 que se encuentra en el mismo vínculo que el nodo local.
subred IPv6	Segmento administrativo de una red IPv6. Los componentes de una subred IPv6 se pueden corresponder directamente con todos los nodos de un vínculo, igual que en IPv4. Si es preciso, los nodos de un vínculo se pueden administrar en subredes independientes. Además, IPv6 no permite subredes multivínculo, en las cuales los nodos de vínculos distintos pueden ser componentes de una sola subred. Los vínculos 2 y 2 de la Figura 3–1 son componentes de la subred 8a multivínculo.
túnel de IPv6	Túnel que proporciona una ruta de extremo a extremo virtual entre un nodo de IPv6 y otro punto final de nodo de IPv6. IPv6 permite la configuración manual de túneles y automática de túneles de 6to4.
enrutador de límite	Enrutador en el límite de una red que proporciona un extremo del túnel de IPv6 a un punto final fuera de la red local. Este enrutador debe tener como mínimo una interfaz de IPv6 a la red interna. En cuanto a la red externa, el enrutador puede tener una interfaz de IPv6 o IPv4.

Descripción general de las direcciones IPv6

Las direcciones IPv6 se asignan a interfaces en lugar de a nodos, teniendo en cuenta que en un nodo puede haber más de una interfaz. Asimismo, se puede asignar más de una dirección IPv6 a una interfaz.

Nota – Para obtener información referente a aspectos técnicos sobre el formato de dirección IPv6, consulte RFC 2374, [IPv6 Global Unicast Address Format \(http://www.ietf.org/rfc/rfc2374.txt?number=2374\)](http://www.ietf.org/rfc/rfc2374.txt?number=2374)

IPv6 abarca tres clases de direcciones:

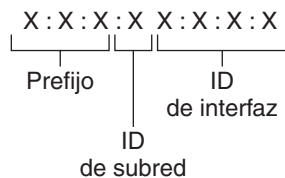
unidifusión	Identifica una interfaz de un solo nodo.
multidifusión	Identifica un grupo de interfaces, en general en nodos distintos. Los paquetes que se envían a una dirección multidifusión se dirigen a todos los miembros del <i>grupo de multidifusión</i> .

difusión por proximidad Identifica un grupo de interfaces, en general en nodos distintos. Los paquetes que se envían a una dirección de difusión por proximidad se dirigen al nodo de miembros del *grupo de difusión por proximidad* que se encuentre más cerca del remitente.

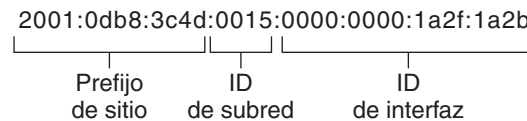
Partes de una dirección IPv6

Una dirección IPv6 tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits, cada uno de ellos unido por dos puntos. Cada campo debe contener un número hexadecimal, a diferencia de la notación decimal con puntos de las direcciones IPv4. En la figura siguiente, las *equis* representan números hexadecimales.

FIGURA 3-2 Formato básico de las direcciones IPv6



Ejemplo:



Los tres campos que están más a la izquierda (48 bits) contienen el *prefijo de sitio*. El prefijo describe la *topología pública* que el ISP o el RIR (Regional Internet Registry, Registro Regional de Internet) suelen asignar al sitio.

El campo siguiente lo ocupa el *ID de subred* de 16 bits que usted (u otro administrador) asigna al sitio. El ID de subred describe la *topología privada*, denominada también *topología del sitio*, porque es interna del sitio.

Los cuatro campos situados más a la derecha (64 bits) contienen el *ID de interfaz*, también denominado *token*. El ID de interfaz se configura automáticamente desde la dirección MAC de interfaz o manualmente en formato EUI-64.

Examine de nuevo la dirección de la figura [Figura 3-2](#):

2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

En este ejemplo se muestran los 128 bits completos de una dirección IPv6. Los primeros 48 bits, `2001:0db8:3c4d`, contienen el prefijo de sitio y representan la topología pública. Los siguientes 16 bits, `0015`, contienen el ID de subred y representan la topología privada del sitio. Los 64 bits que están más a la derecha, `0000:0000:1a2f:1a2b`, contienen el ID de interfaz.

Abreviación de direcciones IPv6

La mayoría de las direcciones IPv6 no llegan a alcanzar su tamaño máximo de 128 bits. Eso comporta la aparición de campos rellenos con ceros o que sólo contienen ceros.

La arquitectura de direcciones IPv6 permite utilizar la notación de dos puntos consecutivos (`::`) para representar campos contiguos de 16 bits de ceros. Por ejemplo, la dirección IPv6 de la [Figura 3–2](#) se puede abreviar reemplazando los dos campos contiguos de ceros del ID de interfaz por dos puntos. La dirección resultante es `2001:0db8:3c4d:0015::1a2f:1a2b`. Otros campos de ceros pueden representarse como un único 0. Asimismo, puede omitir los ceros que aparezcan al inicio de un campo, como por ejemplo cambiar `0db8` por `db8`.

Así pues, la dirección `2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b` se puede abreviar en `2001:db8:3c4d:15::1a2f:1a2b`.

La notación de los dos puntos consecutivos se puede emplear para reemplazar cualquier campo contiguo de ceros de la dirección IPv6. Por ejemplo, la dirección IPv6 `2001:0db8:3c4d:0015:0000:d234::3eee:0000` se puede contraer en `2001:db8:3c4d:15:0:d234:3eee::`.

Prefijos de IPv6

Los campos que están más a la izquierda de una dirección IPv6 contienen el prefijo, que se emplea para enrutar paquetes de IPv6. Los prefijos de IPv6 tienen el formato siguiente:

prefijo/tamaño en bits

El tamaño del prefijo se expresa en notación CIDR (enrutamiento entre dominios sin clase). La notación CIDR consiste en una barra inclinada al final de la dirección, seguida por el tamaño del prefijo en bits. Para obtener información sobre direcciones IP en formato CIDR, consulte [“Cómo diseñar un esquema de direcciones IPv4 CIDR” en la página 61](#).

El *prefijo de sitio* de una dirección IPv6 ocupa como máximo los 48 bits de la parte más a la izquierda de la dirección IPv6. Por ejemplo, el prefijo de sitio de la dirección IPv6 `2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48` se ubica en los 48 bits que hay más a la izquierda, `2001:db8:3c4d`. Utilice la representación siguiente, con ceros comprimidos, para representar este prefijo:

2001:db8:3c4d::/48

Nota – 2001:db8::/32 es un prefijo especial de IPv6 que se emplea específicamente en ejemplos de documentación.

También se puede especificar un *prefijo de subred*, que define la topología interna de la red respecto a un enrutador. La dirección IPv6 de ejemplo tiene el siguiente prefijo de subred:

2001:db8:3c4d:15::/64

El prefijo de subred siempre contiene 64 bits. Estos bits incluyen 48 del prefijo de sitio, además de 16 bits para el ID de subred.

Los prefijos siguientes se han reservado para usos especiales:

- | | |
|-----------|--|
| 2002::/16 | Indica que sigue un prefijo de enrutamiento de 6to4. |
| fe80::/10 | Indica que sigue una dirección local de vínculo. |
| ff00::/8 | Indica que sigue una dirección multidifusión. |

Direcciones unidifusión

IPv6 incluye dos clases de asignaciones de direcciones unidifusión:

- Dirección unidifusión global
- Dirección local de vínculo

El tipo de dirección unidifusión viene determinado por los bits contiguos que están más a la izquierda (orden superior) de la dirección, los cuales contienen el prefijo.

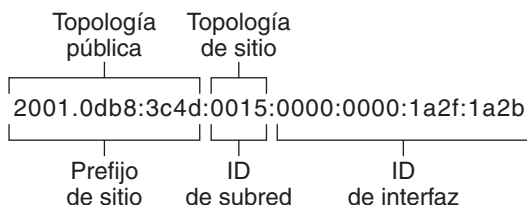
El formato de direcciones unidifusión se organiza conforme a la jerarquía siguiente:

- Topología pública
- Topología de sitio (privada)
- ID de interfaz

Dirección unidifusión global

La dirección unidifusión global es globalmente exclusiva de Internet. La dirección IPv6 de ejemplo que hay en “[Prefijos de IPv6](#)” en la [página 78](#) es de unidifusión global. En la figura siguiente se muestra el ámbito de la dirección unidifusión global, en comparación con las partes que componen la dirección IPv6.

FIGURA 3-3 Partes de la dirección unidifusión global



Topología pública

El prefijo de sitio define la *topología pública* de la red respecto a un enrutador. El ISP o el RIR proporcionan el prefijo de sitio a las empresas.

Topología de sitio y subredes IPv6

En IPv6, el *ID de subred* define una subred administrativa de la red y tiene un tamaño máximo de 16 bits. Un ID de subred se asigna como parte de la configuración de redes IPv6. El *prefijo de subred* define la topología de sitio respecto a un enrutador especificando el vínculo al que se ha asignado la subred.

Desde un punto de vista conceptual, las subredes IPv6 y las IPv4 son iguales en el sentido de que cada subred suele asociarse con solo vínculo de hardware. Sin embargo, los ID de subredes IPv6 se expresan en notación hexadecimal, en lugar de decimal con puntos.

ID de interfaz

El *ID de interfaz* identifica una interfaz de un determinado nodo. Un ID de interfaz debe ser exclusivo en la subred. Los hosts de IPv6 pueden aplicar el protocolo ND para generar automáticamente sus propios ID de interfaz. El protocolo ND genera de forma automática el ID de interfaz, a partir de la dirección MAC o la dirección EUI-64 de la interfaz del host. Los ID de interfaz también se pueden asignar manualmente, lo cual es preferible en el caso de enrutadores de IPv6 y servidores habilitados para IPv6. Si desea obtener instrucciones sobre cómo crear manualmente direcciones EUI-64, consulte RFC 3513 [Internet Protocol Version 6 \(IPv6\) Addressing Architecture](#).

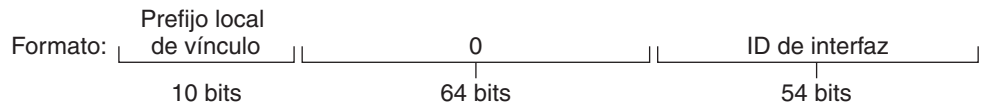
Direcciones unidifusión globales de transición

Por motivos de transición, el protocolo IPv6 incluye la posibilidad de incrustar una dirección IPv4 en una dirección IPv6. Esta clase de dirección IPv4 facilita la colocación en túneles de paquetes IPv6 en redes IPv4 ya configuradas. La dirección 6to4 es un ejemplo de dirección unidifusión global de transición. Para obtener más información sobre direcciones 6to4, consulte [“Túneles automáticos 6to4” en la página 290](#).

Dirección unidifusión local de vínculo

La dirección unidifusión local de vínculo sólo se puede utilizar en el vínculo de red local. Las direcciones locales de vínculo no son válidas ni se reconocen fuera del ámbito corporativo u organizativo. A continuación se muestra un ejemplo del formato que tienen las direcciones locales de vínculo.

EJEMPLO 3-1 Partes de la dirección unidifusión local de vínculo



Ejemplo: fe80::123e:456d

Un *prefijo local de vínculo* presenta el formato siguiente:

fe80::ID_interfaz/10

A continuación se muestra una dirección local de vínculo:

fe80::23a1:b152

fe80 Representación hexadecimal del prefijo binario de 10 bits 111111010. Este prefijo identifica el tipo de dirección IPv6 como dirección local de vínculo.

ID_interfaz Dirección hexadecimal de la interfaz, que en general se deriva de la dirección MAC de 48 bits.

Al habilitar IPv6 durante la instalación de Oracle Solaris, la interfaz con el número más bajo del equipo local se configura con una dirección local de vínculo. Cada interfaz necesita por lo menos una dirección local de vínculo para identificar el nodo en los demás nodos del vínculo local. Así pues, las direcciones locales de vínculo deben configurarse manualmente para las interfaces adicionales de un nodo. Tras la configuración, el nodo utiliza sus direcciones locales de vínculo para la configuración automática de direcciones y el descubrimiento de vecinos.

Direcciones multidifusión

IPv6 permite el uso de direcciones multidifusión. La dirección multidifusión identifica un *grupo de multidifusión*, que es un grupo de interfaces, en general en nodos distintos. Una interfaz puede pertenecer a cualquier cantidad de grupos de multidifusión. Si los primeros 16 bits de una dirección IPv6 son ff00 n, la dirección es del tipo multidifusión.

Las direcciones multidifusión se usan para el envío de información o servicios a todas las interfaces que se definen como miembros del grupo de multidifusión. Por ejemplo, uno de los usos de las direcciones multidifusión es comunicarse con todos los nodos de IPv6 del vínculo local.

Al crearse la dirección unidifusión IPv6 de una interfaz, el núcleo convierte automáticamente la interfaz en miembro de determinados grupos de multidifusión. Por ejemplo, el núcleo convierte cada nodo en un miembro del grupo de multidifusión del nodo solicitado, que utiliza el protocolo ND para detectar la accesibilidad. El núcleo convierte automáticamente también un nodo en miembro de los grupos de multidifusión de todos los nodos o todos los enrutadores.

Para obtener información exhaustiva sobre direcciones multidifusión, consulte “[Direcciones multidifusión IPv6 en profundidad](#)” en la página 260. Para obtener información sobre aspectos técnicos, consulte RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses* (<ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt>), donde se explica el formato de direcciones multidifusión. Para obtener más información sobre el uso adecuado de grupos y direcciones multidifusión, consulte RFC 3307, *Allocation Guidelines for IPv6 Multicast Addresses* (<ftp://ftp.rfc-editor.org/in-notes/rfc3307.txt>).

Grupos y direcciones de difusión por proximidad

Las direcciones de difusión por proximidad IPv6 identifican un grupo de interfaces en distintos nodos de IPv6. Cada grupo de interfaces se denomina *grupo de difusión por proximidad*. Cuando se envía un paquete al grupo de difusión por proximidad, recibe el paquete el miembro del grupo que esté más próximo al remitente.

Nota – La implementación de IPv6 en Oracle Solaris no permite crear direcciones ni grupos de difusión por proximidad. Ahora bien, los nodos de IPv6 de Oracle Solaris pueden enviar paquetes a direcciones de difusión por proximidad. Para obtener más información, consulte “[Consideraciones para túneles hasta un enrutador de reenvío 6to4](#)” en la página 293.

Descripción general del protocolo ND de IPv6

IPv6 aporta el protocolo ND (Neighbor Discovery, descubrimiento de vecinos), que emplea la mensajería como medio para controlar la interacción entre nodos vecinos. Por *nodos vecinos* se entienden los nodos de IPv6 que están en el mismo vínculo. Por ejemplo, al emitir mensajes relativos al descubrimiento de vecinos, un nodo puede aprender la dirección local de vínculo de un vecino. El protocolo ND controla las principales actividades siguientes del vínculo local de IPv6:

- **Descubrimiento de enrutadores:** ayuda a los hosts a detectar enrutadores en el vínculo local.
- **Configuración automática de direcciones:** permite que un nodo configure de manera automática direcciones IPv6 para sus interfaces.
- **Descubrimiento de prefijos:** posibilita que los nodos detecten los prefijos de subred conocidos que se han asignado a un vínculo. Los nodos utilizan prefijos para distinguir los destinos que se encuentran en el vínculo local de los asequibles únicamente a través de un enrutador.
- **Resolución de direcciones:** permite que los nodos puedan determinar la dirección local de vínculo de un vecino solamente a partir de la dirección IP de los destinos.
- **Determinación de salto siguiente:** utiliza un algoritmo para establecer la dirección IP de un salto de destinatario de paquetes que está más allá del vínculo local. El salto siguiente puede ser un enrutador o el nodo de destino.
- **Detección de inasequibilidad de vecinos:** ayuda a los nodos a establecer si un nodo ya no es asequible. La resolución de direcciones puede repetirse tanto en enrutadores como hosts.
- **Detección de direcciones duplicadas:** permite que un nodo pueda determinar si está en uso o no una dirección que el nodo tenga la intención de utilizar.
- **Redirección:** un enrutador indica a un host el mejor nodo de primer salto que se puede usar para acceder a un determinado destino.

El protocolo ND emplea los tipos de mensajes ICMP siguientes para la comunicación entre los nodos de un vínculo:

- Solicitud de enrutador
- Anuncio de enrutador
- Solicitud de vecino
- Anuncio de vecino
- Redirección

Para obtener información exhaustiva sobre mensajes de protocolo ND y otros temas relativos a dicho protocolo, consulte “[Protocolo ND de IPv6](#)” en la página 278. Para obtener información sobre aspectos técnicos sobre Neighbor Discovery (ND), consulte [RFC 2461, Neighbor Discovery for IP Version 6 \(IPv6\)](#) (<http://www.ietf.org/rfc/rfc2461.txt?number=2461>).

Configuración automática de direcciones IPv6

Una de las características principales de IPv6 es la capacidad que tiene un host de configurar automáticamente una interfaz. Mediante el protocolo ND, el host busca un enrutador de IPv6 en el vínculo local y solicita un prefijo de sitio. Como parte del proceso de configuración automática, el host lleva a cabo los pasos siguientes:

- Crea una dirección local de vínculo para cada interfaz, lo cual no precisa un enrutador en el vínculo.
- Verifica la exclusividad de una dirección en un vínculo, lo cual no precisa un enrutador en el vínculo.
- Determina si las direcciones globales deben obtenerse a partir del mecanismo con estado, sin estado o ambos. (Precisa un enrutador en el vínculo).

Descripción general de configuración automática sin estado

La configuración automática no necesita la configuración manual de hosts, una configuración mínima de enrutadores (si los hay) ni servidores adicionales. El mecanismo sin estado permite que un host genere sus propias direcciones. Para generar las direcciones, el mecanismo sin estado utiliza la información local y la no local anunciada por los enrutadores.

Pueden implementarse direcciones temporales en una interfaz, configuradas también de manera automática. Se puede habilitar un token de direcciones temporales para una o varias interfaces en un host. Sin embargo, a diferencia de las direcciones IPv6 estándar configuradas automáticamente, una dirección temporal consta del prefijo de sitio y un número de 64 bits generado aleatoriamente. Ese número aleatorio constituye la parte del ID de interfaz de la dirección IPv6. Una dirección local de vínculo no se genera con la dirección temporal como ID de interfaz.

Los enrutadores anuncian todos los prefijos que se han asignado al vínculo. Los hosts de IPv6 emplean el protocolo ND para obtener un prefijo de subred a partir de un enrutador local. Los hosts crean direcciones IPv6 automáticamente combinando el prefijo de subred con un ID de interfaz que se genera a partir de la dirección MAC de una interfaz. Si no hay enrutadores, un host puede generar únicamente direcciones locales de vínculo. Las direcciones locales de vínculo sólo son aptas para comunicaciones con nodos del mismo vínculo.

Nota – La configuración automática de direcciones sin estado no debe usarse para crear las direcciones IPv6 de servidores. Los hosts generan automáticamente unos ID de interfaz que se basan en información específica del hardware durante la configuración automática. El ID de interfaz actual puede llegar a invalidarse si la interfaz vigente se intercambia con una interfaz nueva.

Descripción general sobre los túneles de IPv6

En la mayoría de las empresas, la implantación de IPv6 en una red IPv4 ya configurada debe realizarse de manera gradual y por fases. El entorno de redes de pila doble de Oracle Solaris permite el funcionamiento compatible de IPv4 e IPv6. Debido a que casi todas las redes emplean el protocolo IPv4, en la actualidad las redes IPv6 necesitan una forma de comunicarse más allá de sus límites. Para ello, las redes IPv6 se sirven de los túneles.

En buena parte de las situaciones hipotéticas para túneles de IPv6, el paquete de IPv6 saliente se encapsula en un paquete de IPv4. El enrutador de límite de la red IPv6 configura un túnel de extremo a extremo a través de varias redes IPv4 hasta el enrutador de límite de la red IPv6 de destino. El paquete se desplaza por el túnel en dirección al enrutador de límite de la red de destino, que se encarga de desencapsular el paquete. A continuación, el enrutador reenvía el paquete IPv6 desencapsulado al nodo de destino.

La implementación de IPv6 en Oracle Solaris permite las siguientes situaciones hipotéticas de configuración de túneles:

- Túnel configurado manualmente entre dos redes IPv6, a través de una red IPv4. La red IPv4 puede ser Internet o una red local dentro de una empresa.
- Túnel configurado manualmente entre dos redes IPv4, a través de una red IPv6, en general dentro de una empresa.
- Túnel de 6to4 configurado dinámicamente entre dos redes IPv6, a través de una red IPv4 de una empresa o por Internet.

Para obtener más información sobre los túneles de IPv6, consulte [“Túneles de IPv6” en la página 286](#). Para obtener más información relativa a túneles de IPv4 a IPv4 y redes privadas virtuales, consulte [“Redes privadas virtuales e IPsec” en la página 502](#).

Planificación de una red IPv6 (tareas)

Implementar IPv6 en una red nueva o ya configurada supone un importante esfuerzo de planificación. En este capítulo se presentan las tareas principales imprescindibles para poder configurar IPv6. En el caso de redes ya configuradas, la implementación de IPv6 se debe establecer por fases. Los temas de este capítulo ayudan a implantar IPv6 en fases en una red que, por otro lado, es de sólo IPv4.

En este capítulo se tratan los temas siguientes:

- “Planificación de IPv6 (mapas de tareas)” en la página 87
- “Situación hipotética de topología de red IPv6” en la página 88
- “Preparación de la red ya configurada para admitir IPv6” en la página 90
- “Preparación de un plan de direcciones IPv6” en la página 94

Para obtener una introducción a los conceptos relativos a IPv6, consulte el [Capítulo 3](#), “Introducción a IPv6 (descripción general)”. Para obtener información detallada, consulte el [Capítulo 11](#), “IPv6 en profundidad (referencia)”.

Planificación de IPv6 (mapas de tareas)

Efectúe en el orden que se indica las tareas del mapa de tareas siguiente para realizar las tareas de planificación relativas la implementación de IPv6.

La tabla siguiente muestra diferentes tareas para la configuración de la red IPv6. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

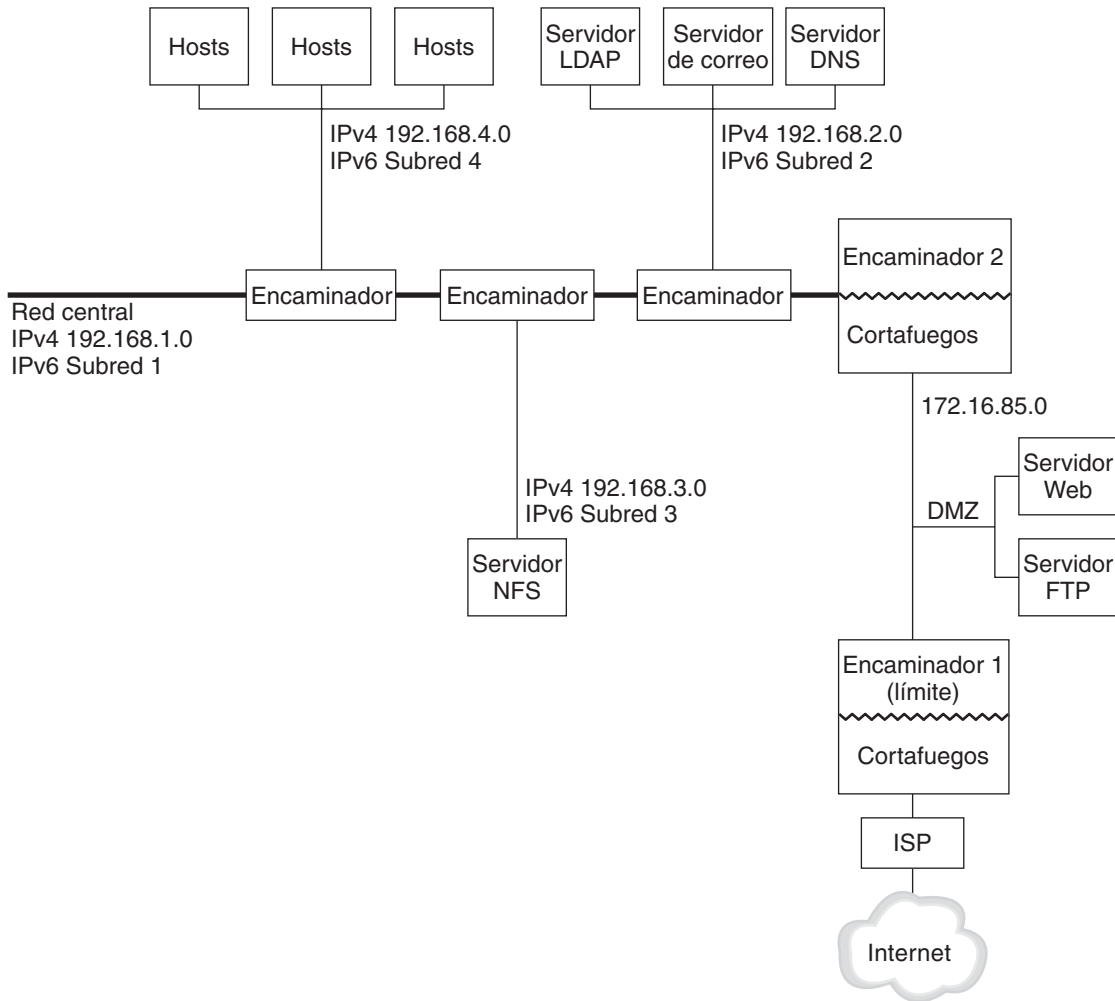
Tarea	Descripción	Para obtener instrucciones
1. Preparar el hardware para admitir IPv6.	Compruebe que el hardware se pueda actualizar a IPv6.	“Preparación de la topología red para admitir IPv6” en la página 90

Tarea	Descripción	Para obtener instrucciones
2. Disponer de un ISP que admita IPv6.	Compruebe que el ISP que utiliza admita IPv6. De no ser así, busque uno que sea compatible con IPv6. Puede utilizar dos ISP, uno para IPv6 y otro para comunicaciones de IPv4.	
3. Comprobar que las aplicaciones estén preparadas para funcionar con IPv6.	Verifique que las aplicaciones puedan funcionar en un entorno IPv6.	“Cómo preparar servicios de red para admitir IPv6” en la página 92
4. Disponer de prefijo de sitio.	Solicite al ISP o al RIR más próximo un prefijo de sitio de 48 bits.	“Obtención de un prefijo de sitio” en la página 94
5. Crear un plan de direcciones de subredes.	Se debe planificar la topología de red IPv6 global y el esquema de direcciones para poder configurar IPv6 en los distintos nodos de la red.	“Creación de un esquema de numeración para subredes” en la página 95
6. Diseñar un plan para el uso de túneles.	Establezca los enrutadores que deben ejecutar túneles a otras subredes o redes externas.	“Planificación de túneles en la topología de red” en la página 93
7. Crear un plan de direcciones para entidades de la red.	Se debe planificar la dirección de servidores, enrutadores y hosts antes de configurar IPv6.	“Creación de un plan de direcciones IPv6 para nodos” en la página 95
8. Desarrollar directrices de seguridad de IPv6.	A la hora de desarrollar directrices de seguridad de IPv6, consulte las funciones de filtro IP, arquitectura de seguridad IP (IPsec), Internet Key Exchange (IKE) y otras funciones de seguridad de Oracle Solaris.	Parte IV
9. (Opcional) Configurar una DMZ.	Por motivos de seguridad, se precisa un plan de direcciones para la DMZ y sus entidades antes de configurar IPv6.	“Aspectos relacionados con la seguridad en la implementación de IPv6” en la página 94
10. Habilitar los nodos para que admitan IPv6.	Configure IPv6 en todos los hosts y enrutadores.	“Configuración de IPv6 en enrutadores (mapa de tareas)” en la página 177
11. Activar servicios de red.	Compruebe que los servidores puedan admitir IPv6.	“Tareas de administración principales de TCP/IP (mapa de tareas)” en la página 204
12. Actualizar nombres de servidor para la compatibilidad con IPv6.	Compruebe que los servidores DNS, NIS y LDAP se actualicen con las nuevas direcciones IPv6.	“Configuración de la compatibilidad con el servicio de nombres para IPv6” en la página 198

Situación hipotética de topología de red IPv6

Las tareas de todo el capítulo explican la forma de planificar servicios de IPv6 en una red empresarial estándar. En la figura siguiente se muestra la red a la que se hace referencia a lo largo del capítulo. La red IPv6 que se propone puede incluir varios o todos los vínculos que aparecen en esta figura.

FIGURA 4-1 Situación hipotética de topología de red IPv6



La situación hipotética de red empresarial se compone de cinco subredes con cuatro direcciones IPv4 ya configuradas. Los vínculos de la red se corresponden directamente con las subredes administrativas. Las cuatro redes internas se muestran con direcciones IPv4 privadas en formato RFC 1918, solución habitual ante la falta de direcciones IPv4. Estas redes internas se basan en el siguiente esquema de direcciones:

- La subred 1 es la red principal interna 192.168.1.
- La subred 2 es la red interna 192.168.2, con LDAP, sendmail y servidores DNS.
- La subred 3 es la red interna 192.168.3, con los servidores NFS de la empresa.

- La subred 4 es la red interna 192 . 168 . 4, que contiene hosts para los empleados de la empresa.

La red pública externa 172 . 16 . 85 funciona como DMZ de la corporación. Esta red contiene servidores web, servidores FTP anónimos y demás recursos que la empresa ofrece al entorno exterior. El enrutador 2 ejecuta un cortafuegos y separa la red pública 172 . 16 . 85 de la red principal interna. En el otro extremo de la DMZ, el enrutador 1 ejecuta un cortafuegos y actúa como enrutador de límite de la empresa.

En la [Figura 4-1](#), la DMZ pública presenta la dirección privada RFC 1918 172 . 16 . 85. En un entorno real, la DMZ pública debe tener registrada una dirección IPv4. La mayoría de los sitios de IPv4 emplean una combinación de direcciones públicas y direcciones privadas RFC 1918. Sin embargo, en el ámbito de IPv6 el concepto de direcciones públicas y privadas es distinto. Debido a que IPv6 dispone de mucho más espacio de direcciones, las direcciones públicas IPv6 se utilizan en redes públicas y privadas.

Preparación de la red ya configurada para admitir IPv6

Nota – La pila doble de protocolos de Oracle Solaris permite operaciones simultáneas de IPv4 e IPv6. Puede ejecutar sin ningún problema operaciones relacionadas con IPv4 en la red, durante la implementación de IPv6 y tras ésta.

IPv6 incorpora funciones adicionales a una red ya configurada. Así pues, la primera vez que implemente IPv6, compruebe que no se interrumpen las operaciones que funcionan con IPv4. Los temas que se tratan en esta sección muestran detalladamente un procedimiento para incorporar IPv6 en una red ya configurada.

Preparación de la topología red para admitir IPv6

El primer paso al implementar IPv6 consiste en detectar las entidades de la red que sean compatibles con IPv6. La mayoría de las veces, la implementación de IPv6 no modifica la topología de red (cables, enrutadores y hosts). Ahora bien, antes de configurar direcciones IPv6 en interfaces de red, quizá deba preparar para IPv6 el hardware y las aplicaciones.

Verifique que el hardware de la red se pueda actualizar a IPv6. Por ejemplo, consulte la documentación de los fabricantes sobre la compatibilidad con IPv6 respecto a los siguientes tipos de hardware:

- Enrutadores
- Servidores de seguridad
- Servidores

- Conmutadores

Nota – Todos los procedimientos de esta parte dan por sentado que el equipo, en especial los enrutadores, se pueden actualizar a IPv6.

Algunos modelos de enrutador no se pueden actualizar a IPv6. Para obtener más información y una solución alternativa, consulte [“El enrutador IPv4 no puede actualizarse a IPv6” en la página 231.](#)

Preparación de servicios de red para admitir IPv6

Los siguientes servicios de red IPv4 típicos de la versión actual de Oracle Solaris admiten IPv6:

- `sendmail`
- NFS
- HTTP (Apache 2.x u Orion)
- DNS
- LDAP

El servicio de correo IMAP sólo es apto para IPv4.

Los nodos configurados para IPv6 pueden ejecutar servicios de IPv4. Al activar IPv6, no todos los servicios aceptan conexiones IPv6. Los servicios conectados a IPv6 aceptarán una conexión. Los servicios que no estén conectados a IPv6 seguirán funcionando con la mitad de IPv4 de la pila de protocolos.

Al actualizar los servicios a IPv6 pueden surgir algunos problemas. Para obtener más información, consulte [“Problemas tras la actualización de servicios a IPv6” en la página 231.](#)

Preparación de servidores para admitir IPv6

Debido a que los servidores se consideran hosts de IPv6, el protocolo ND configura automáticamente sus direcciones IPv6. No obstante, muchos servidores tienen varias tarjetas de interfaz de red que quizá tenga la intención de extraer para mantener o reemplazar. Si se reemplaza una tarjeta de interfaz de red, el protocolo ND genera automáticamente un ID de interfaz nuevo para dicha tarjeta. Algún servidor en concreto podría no aceptar este comportamiento.

Por lo tanto, no descarte la configuración manual de la parte correspondiente al ID de interfaz de las direcciones IPv6 en cada interfaz del servidor. Para obtener instrucciones, consulte [“Cómo configurar un token IPv6 especificado por el usuario” en la página 186.](#) Más adelante, cuando deba reemplazar una tarjeta de interfaz de red, se aplica la dirección IPv6 que ya estaba configurada a la tarjeta nueva.

▼ Cómo preparar servicios de red para admitir IPv6

1 Actualice los servicios de red siguientes para que admitan IPv6:

- Servidores de correo
- Servidores NIS
- NFS

Nota – LDAP admite IPv6 sin tener que realizar tareas de configuración propias de IPv6.

2 Verifique que el hardware del cortafuegos ya esté preparado para IPv6.

Para obtener instrucciones, consulte la documentación pertinente sobre servidores de seguridad.

3 Verifique que otros servicios de la red se hayan conectado a IPv6.

Para obtener más información, consulte la publicidad adicional y la documentación relativa al software.

4 Si el sitio implementa los servicios siguientes, asegúrese de haber tomado las medidas apropiadas:

- Servidores de seguridad

Para poder admitir IPv6, quizá deba incrementar la severidad de las directrices ya establecidas para IPv4. Para otros aspectos sobre seguridad, consulte [“Aspectos relacionados con la seguridad en la implementación de IPv6” en la página 94.](#)

- Correo

En los registros MX para DNS, quizá deba agregar la dirección IPv6 del servidor de correo.

- DNS

Para cuestiones específicas de DNS, consulte [“Cómo preparar DNS para admitir IPv6” en la página 92.](#)

- IPQoS

En un host, emplee las mismas directrices DiffServ que se usaban en IPv4. Para obtener más información, consulte [“Módulo Classifier” en la página 871.](#)

5 Audite los servicios de red que ofrezca un nodo antes de convertir a IPv6 dicho nodo.

▼ Cómo preparar DNS para admitir IPv6

La versión actual de Oracle Solaris admite resolución de DNS desde el lado del cliente y del servidor. Efectúe el procedimiento siguiente con el fin de preparar IPv6 para servicios de DNS.

Para obtener más información relativa a la compatibilidad de DNS con IPv6, consulte la [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

- 1 **Compruebe que el servidor DNS que ejecuta la resolución de nombres recursivos esté en una pila doble (IPv4 e IPv6) o sólo en IPv4.**
- 2 **En el servidor DNS, rellene la base de datos de DNS con los pertinentes registros AAAA de base de datos de IPv6 en la zona de reenvío.**

Nota – Los servidores que ejecutan varios servicios fundamentales necesitan atención especial. Verifique que la red funcione correctamente. Compruebe también que todos los servicios fundamentales tengan conexión con IPv6. A continuación, agregue la dirección IPv6 del servidor a la base de datos de DNS.

- 3 **Incorpore los registros PTR relativos a los registros AAAA en la zona inversa.**
- 4 **Agregue datos sólo de IPv4, o de IPv6 e IPv4, en el registro NS que describe zonas.**

Planificación de túneles en la topología de red

La implementación de IPv6 permite varias configuraciones de túneles para actuar como mecanismos de transición cuando la red migra a una combinación de IPv4 e IPv6. Los túneles posibilitan la comunicación entre redes IPv6 aisladas. Como en Internet se ejecuta mayoritariamente IPv4, los paquetes de IPv6 del sitio deben desplazarse por Internet a través de túneles hacia las redes IPv6 de destino.

A continuación se presentan varias de las situaciones hipotéticas más destacadas sobre el uso de túneles en la topología de red IPv6:

- El ISP del que adquiere servicios IPv6 permite crear un túnel desde el enrutador de límite del sitio hasta la red del ISP. La [Figura 4–1](#) muestra un túnel de esta clase. En tal caso, se debe ejecutar IPv6 manual a través de un túnel de IPv4.
- Se administra una red distribuida de gran tamaño con conectividad IPv4. Para conectar los sitios distribuidos que utilizan IPv6, puede ejecutar un túnel de 6to4 desde el enrutador de límite de cada subred.
- En ocasiones, un enrutador de la infraestructura no se puede actualizar a IPv6. En tal caso, la alternativa es crear un túnel manual en el enrutador de IPv4 con dos enrutadores de IPv6 como puntos finales.

Para obtener información sobre configuración de túneles, consulte “[Tareas de configuración de túneles para compatibilidad con IPv6 \(mapa de tareas\)](#)” en la página 189. Para obtener información conceptual relativa a túneles, consulte “[Túneles de IPv6](#)” en la página 286.

Aspectos relacionados con la seguridad en la implementación de IPv6

Al implementar IPv6 en una red ya configurada, debe tener la precaución de no poner en riesgo la seguridad del sitio. Durante la sucesivas fases en la implementación de IPv6, tenga en cuenta los siguientes aspectos relacionados con la seguridad:

- Los paquetes de IPv6 e IPv4 necesitan la misma cantidad de filtrado.
- A menudo, los paquetes de IPv6 pasan por un túnel a través de un cortafuegos. Por lo tanto, debe aplicar cualquiera de las siguientes situaciones hipotéticas:
 - Haga que el cortafuegos inspeccione el contenido en el túnel.
 - Coloque un cortafuegos de IPv6 con reglas parecidas en el punto final del túnel del extremo opuesto.
- Determinados mecanismos de transición utilizan IPv6 en UDP a través de túneles de IPv4. Dichos mecanismos pueden resultar peligrosos al cortocircuitarse el cortafuegos.
- Los nodos de IPv6 son globalmente asequibles desde fuera de la red empresarial. Si la directiva de seguridad prohíbe el acceso público, debe establecer reglas más estrictas con relación al cortafuegos. Por ejemplo, podría configurar un cortafuegos con estado.

Este manual proporciona funciones de seguridad válidas en una implementación de IPv6.

- La función de IPsec (IP architecture security, arquitectura de seguridad IP) posibilita la protección criptográfica de paquetes IPv6. Para obtener más información, consulte el [Capítulo 19, “Arquitectura de seguridad IP \(descripción general\)”](#).
- La función IKE (Internet Key Exchange, intercambio de claves en Internet) permite el uso de autenticación de claves públicas para paquetes de IPv6. Para obtener más información, consulte el [Capítulo 22, “Intercambio de claves de Internet \(descripción general\)”](#).

Preparación de un plan de direcciones IPv6

Desarrollar un plan de direcciones es importante en la transición de IPv4 a IPv6. Para esta tarea se necesitan los siguientes requisitos previos:

- [“Obtención de un prefijo de sitio” en la página 94](#)
- [“Creación del esquema de numeración de IPv6” en la página 95](#)

Obtención de un prefijo de sitio

Debe obtenerse un prefijo de sitio antes de configurar IPv6. El prefijo de sitio se emplea en la derivación de direcciones IPv6 para todos los nodos de la implementación de IPv6. En [“Prefijos de IPv6” en la página 78](#) se proporciona una introducción a los prefijos de sitio.

Un ISP que admita IPv6 puede brindar a las empresas prefijos de sitio de IPv6 de 48 bits. Si el ISP sólo admite IPv4, se puede buscar otro que sea compatible con IPv6 y mantener el ISP actual para IPv4. En tal caso, existen las siguientes soluciones alternativas. Para obtener más información, consulte “El ISP actual no admite IPv6” en la página 231.

Si su organización es un ISP, los prefijos de sitio de sus clientes se obtienen del pertinente registro de Internet. Para obtener más información, consulte la página de [IANA \(Internet Assigned Numbers Authority\)](http://www.iana.org) (<http://www.iana.org>).

Creación del esquema de numeración de IPv6

A menos que la red IPv6 que se proponga sea totalmente nueva, la topología de IPv4 ya configurada sirve de base para el esquema de numeración de IPv6.

Creación de un esquema de numeración para subredes

Inicie el esquema de numeración asignando las subredes IPv4 ya configuradas a subredes IPv6 equivalentes. Por ejemplo, fíjese en las subredes de la [Figura 4-1](#). Las subredes 1–4 utilizan la designación de redes privadas IPv4 de RFC 1918 para los primeros 16 bits de sus direcciones, además de los dígitos 1–4 para indicar la subred. A modo de ejemplo, suponga que el prefijo de IPv6 `2001:db8:3c4d/48` se ha asignado al sitio.

La tabla siguiente muestra la asignación de prefijos de IPv4 privados a prefijos de IPv6.

Prefijo de subred IPv4	Prefijo de subred IPv6 equivalente
192.168.1.0/24	2001:db8:3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

Creación de un plan de direcciones IPv6 para nodos

En la mayoría de los hosts, la configuración automática sin estado de direcciones IPv6 para sus interfaces constituye una estrategia válida y eficaz. Cuando el host recibe el prefijo de sitio del enrutador más próximo, el protocolo ND genera de forma automática direcciones IPv6 para cada interfaz del host.

Los servidores necesitan direcciones IPv6 estables. Si no configura manualmente las direcciones IPv6 de un servidor, siempre que se reemplaza una tarjeta NIC del servidor se configura automáticamente una dirección IPv6. Al crear direcciones para servidores debe tenerse en cuenta lo siguiente:

- Proporcione a los servidores unos ID de interfaz descriptivos y estables. Un método consiste en aplicar un sistema de numeración consecutiva a los ID de interfaz. Por ejemplo, la interfaz interna del servidor LDAP que aparece en la [Figura 4-1](#) podría ser `2001:db8:3c4d:2::2`.
- Si habitualmente no cambia la numeración de la red IPv4, es buena idea utilizar como ID de interfaz las direcciones IPv4 ya creadas de los enrutadores y servidores. En la [Figura 4-1](#), suponga que la interfaz del enrutador 1 con la DMZ tiene la dirección IPv4 `123.456.789.111`. La dirección IPv4 puede convertirse a hexadecimal y aplicar el resultado como ID de interfaz. El nuevo ID de interfaz será `::7bc8:156f`.

Este planteamiento se utiliza sólo si se es el propietario de la dirección IPv4 registrada, en lugar de haber obtenido la dirección de un ISP. Si utiliza una dirección IPv4 proporcionada por un ISP, se crea una dependencia que puede causar problemas en caso de cambiar los ISP.

Debido al número limitado de direcciones IPv4, antes un diseñador de redes debía tener en cuenta si iba a utilizar direcciones registradas globales y direcciones RFC 1918 privadas. No obstante, el concepto de direcciones IPv4 globales y privadas no es aplicable a las direcciones IPv6. Puede utilizar direcciones unidifusión globales, que incluyen el prefijo de sitio, en todos los vínculos de la red, incluida la DMZ pública.

Configuración de servicios de red TCP/IP y direcciones IPv4 (tareas)

La administración de redes TCP/IP se compone de dos fases. La primera consiste en ensamblar el hardware. A continuación, se configuran los daemon, archivos y servicios que implementan el protocolo TCP/IP.

En este capítulo se explica cómo configurar el protocolo TCP/IP en una red que implementa servicios y direcciones IPv4.

Nota – Muchas de las tareas de este capítulo se aplican a redes habilitadas tanto para IPv4 como para IPv6. Cuando las tareas de configuración son distintas en los dos formatos de direcciones, es preciso seguir los pasos de configuración de IPv4 que se indican en este capítulo. Las tareas de este capítulo establecen referencias cruzadas con las tareas IPv6 equivalentes del [Capítulo 7](#), “Configuración de una red IPv6 (tareas)”.

Este capítulo contiene la información siguiente:

- “Antes de configurar una red IPv4 (mapa de tareas)” en la página 98
- “Cómo determinar los modos de configuración de host” en la página 99
- “Cómo agregar una subred a una red (mapa de tareas)” en la página 102
- “Configuración de sistemas en la red local” en la página 104
- “Mapa de tareas de configuración de red” en la página 103
- “Reenvío de paquetes y rutas en redes IPv4” en la página 114
- “Supervisión y modificación de los servicios de capa de transporte” en la página 137

Novedades de este capítulo

En Solaris 10 8/07, se realizan los siguientes cambios:

- Puede configurar y administrar las rutas a través de la Utilidad de gestión de servicios (SMF) como alternativa al uso del comando `routeadm`. Para ver las instrucciones, consulte los procedimientos y ejemplos de [“Reenvío de paquetes y rutas en redes IPv4” en la página 114](#) y la página del comando `man routeadm(1M)`.
- El archivo `/etc/inet/ipnodes` pasa a estar obsoleto. Utilice `/etc/inet/ipnodes` únicamente para las versiones anteriores de Oracle Solaris 10, tal como se explica en los procedimientos individuales.

Antes de configurar una red IPv4 (mapa de tareas)

Antes de configurar el protocolo TCP/IP, complete las tareas que se enumeran en la tabla siguiente. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener instrucciones
1. Diseñar la topología de red.	Determina la distribución física de la red.	“Descripción general de la topología de red” en la página 66 y “Topología de sistemas autónomos IPv4” en la página 118
2. Obtener un número de red del proveedor de servicios de Internet (ISP) o el Registro Regional de Internet (RIR).	Obtiene un número de red registrado, que permite a los sistemas del sitio comunicarse externamente.	“Cómo diseñar un esquema de direcciones IPv4” en la página 60.
3. Planificar el esquema de direcciones IPv4 para la red. Si es preciso, incluir las direcciones de subred.	Utiliza el número de red como base para el plan de direcciones.	“Cómo diseñar un esquema de direcciones IPv4” en la página 60.
4. Ensamblar el hardware de red en función de la topología de red. Verificar que el hardware funcione correctamente.	Configura sistemas, medios de red, enrutadores, conmutadores, concentradores y puentes destacados en el diseño de la topología de red.	Los manuales del hardware y “Descripción general de la topología de red” en la página 66.
5. Asignar direcciones IPv4 y nombres de host a todos los sistemas de la red.	Asigna las direcciones IPv4 durante la instalación de Oracle Solaris o la fase posterior a la instalación, en los archivos apropiados.	“Cómo diseñar un esquema de direcciones IPv4” en la página 60 y “Cómo cambiar la dirección IPv4 y otros parámetros de configuración de red” en la página 110

Tarea	Descripción	Para obtener instrucciones
6. Ejecutar el software de configuración que necesitan los enrutadores e interfaces de red, si es preciso.	Configura los hosts múltiples y enrutadores.	“Planificación de enrutadores en la red” en la página 66 y “Configuración de un enrutador IPv4” en la página 121 for information on routers.
7. Determinar qué servicio de nombres o directorios utiliza la red: NIS, LDAP, DNS o archivos locales.	Configura el servicio de nombres o de directorios seleccionado.	Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP).
8. Seleccionar nombres de dominio para la red, si es preciso.	Elige un nombre de dominio para la red y lo registra con InterNIC.	Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP).

Cómo determinar los modos de configuración de host

Como administrador de red, configure el protocolo TCP/IP para ejecutarse en hosts y enrutadores (si es preciso). Puede configurar estos sistemas para obtener información de la configuración de los archivos del sistema local o de archivos que se encuentran en otros sistemas de la red. Necesita la siguiente información de configuración:

- Nombre de host de cada sistema
- Dirección IP de cada sistema
- Nombre de dominio al que pertenece cada sistema
- Enrutador predeterminado
- Máscara de red IPv4 en uso en cada red del sistema

Un sistema que obtiene la información de configuración de TCP/IP de los archivos locales funciona en *modo de archivos locales*. Un sistema que obtiene la información de configuración de TCP/IP de un servidor de red remoto funciona en *modo de cliente de red*.

Sistemas que deben ejecutarse en modo de archivos locales

Para ejecutarse en modo de archivos locales, un sistema debe tener copias locales de los archivos de configuración de TCP/IP. Estos archivos se describen en [“Archivos de configuración TCP/IP” en la página 233](#). Se recomienda que el sistema tenga su propio disco, aunque no es imprescindible.

La mayoría de los servidores deben ejecutarse en el modo de archivos locales. Este requisito afecta a los siguientes servidores:

- Servidores de configuración de red

- Servidores NFS
- Servidores de nombres que proporcionan servicios NIS, LDAP o DNS
- Servidores de correo

Asimismo, los enrutadores deben ejecutarse en el modo de archivos locales.

Los sistemas que funcionan exclusivamente como servidores de impresión no necesitan ejecutarse en el modo de archivos locales. El tamaño de la red determina si los hosts individuales deben ejecutarse en el modo de archivos locales.

Si está ejecutando una red de tamaño reducido, la cantidad de trabajo que implica el mantenimiento de dichos archivos en los hosts individuales es manejable. Si la red sirve a cientos de hosts, la tarea resulta más difícil, incluso aunque se divida la red en una serie de subdominios administrativos. Por consiguiente, en el caso de las redes de gran tamaño, el uso del modo de archivos locales suele ser menos eficaz. Sin embargo, dado que los enrutadores y servidores deben ser autosuficientes, deben configurarse en el modo de archivos locales.

Servidores de configuración de red

Los *servidores de configuración de red* son los servidores que facilitan la información de configuración de TCP/IP a los hosts que están configurados en el modo de clientes de red. Estos servidores admiten tres protocolos de inicio:

- RARP: el protocolo RARP (Reverse Address Resolution Protocol) asigna direcciones Ethernet addresses (48 bits) a direcciones IPv4 (32 bits), al contrario que ARP. Al ejecutar RARP en un servidor de configuración de red, los hosts que se ejecutan en el modo de cliente de red obtienen sus direcciones IP y archivos de configuración de TCP/IP del servidor. El daemon `in.rarpd` permite los servicios de RARP. Consulte la página del comando `man in.rarpd(1M)` para obtener más información.
- TFTP: el protocolo TFTP (Trivial File Transfer Protocol) es una aplicación que transfiere archivos entre sistemas remotos. El daemon `in.tftpd` ejecuta los servicios TFTP, lo cual permite la transferencia de archivos entre los servidores de configuración de red y sus clientes de red. Consulte la página del comando `man in.tftpd(1M)` para obtener más información.
- Bootparams: el protocolo Bootparams proporciona los parámetros para el inicio que necesitan los clientes que inician la red. El daemon `rpc.bootparamd` ejecuta estos servicios. Consulte la página del comando `man bootparamd(1M)` para obtener más información.

Los servidores de configuración de red también pueden funcionar como servidores de archivos NFS.

Si está configurando host como clientes de red, también debe configurar, como mínimo, un sistema en la red como servidor de configuración de red. Si la red cuenta con subredes, debe tener como mínimo un servidor de configuración de red para cada subred con clientes de red.

Sistemas que son clientes de red

Cualquier host que obtenga su información de configuración de un servidor de configuración de red funciona en modo de cliente de red. Los sistemas que están configurados como clientes de red no requieren copias locales de los archivos de configuración de TCP/IP.

El *modo de cliente de red* simplifica la administración de grandes redes. El modo de cliente de red minimiza el número de tareas de configuración que se llevan a cabo en hosts individuales. El modo de cliente de red garantiza que todos los sistemas de la red se adhieran a los mismos estándares de configuración.

Puede configurar el modo de cliente de red en todo tipo de equipos. Por ejemplo, puede configurar el modo de cliente de red en sistemas autónomos.

Configuraciones mixtas

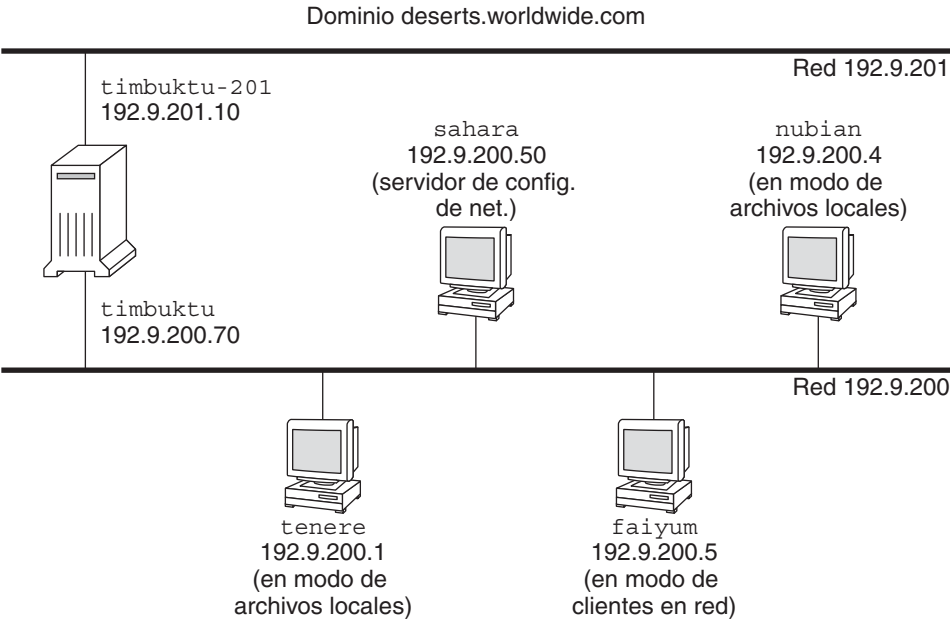
Las configuraciones no se limitan al modo de todos los archivos locales o al modo de todos los clientes de red. Los enrutadores y servidores siempre deben configurarse en modo local. Para los hosts, puede utilizar cualquier combinación de modos de clientes de red y de archivos locales.

Situación hipotética de topología de red IPv4

La [Figura 5-1](#) muestra los hosts de una red ficticia con el número de red 192.9.200. La red tiene un servidor de configuración de red, denominado sahara. Los hosts tenere y nubian tienen sus propios discos y se ejecutan en modo de archivos locales. El host faiyum también tiene un disco, pero este sistema funciona en modo de cliente de red.

Finalmente, el sistema timbuktú está configurado como enrutador. El sistema incluye dos interfaces de red. La primera se denomina timbuktú. Esta interfaz pertenece a la red 192.9.200. La segunda interfaz se denomina timbuktú-201. Esta interfaz pertenece a la red 192.9.201. Ambas redes están en el dominio organizativo deserts.worldwide.com. El dominio utiliza archivos locales como servicio de nombres.

FIGURA 5-1 Hosts en un ejemplo de topología de red IPv4



Cómo agregar una subred a una red (mapa de tareas)

Si pasa de una red que no utiliza una subred a una red que sí la utiliza, lleve a cabo las tareas del siguiente mapa de tareas.

Nota – La información de esta sección se aplica únicamente a las subredes IPv4. Para obtener información sobre la planificación de subredes IPv6, consulte [“Preparación de la topología red para admitir IPv6” en la página 90](#) y [“Creación de un esquema de numeración para subredes” en la página 95](#).

La tabla siguiente muestra diferentes tareas para agregar una subred a la red actual. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener instrucciones
1. Determinar si la topología de red requiere subredes.	Determina la nueva topología de subred, incluida la ubicación de los enrutadores y los hosts de las subredes.	“Planificación de enrutadores en la red” en la página 66 , “¿Qué son las subredes?” en la página 240 y “Clases de red” en la página 254

Tarea	Descripción	Para obtener instrucciones
2. Asignar las direcciones IP con el nuevo número de subred para que los sistemas pasen a ser miembros de la subred.	Configura las direcciones IP que utilizan el nuevo número de subred, ya sea durante la instalación de Oracle Solaris o posteriormente, en el archivo <code>/etc/hostname.interfaz</code> .	“Cómo decidir el formato de las direcciones IP para la red” en la página 55
3. Configurar la máscara de red de la subred en todos los sistemas previstos en la subred.	Modifica el archivo <code>/etc/inet/netmasks</code> , si está configurando manualmente los clientes de red. También proporciona la máscara de red al programa de instalación de Oracle Solaris.	“Base de datos netmasks” en la página 240 y “Creación de la máscara de red para las direcciones IPv4” en la página 241
4. Editar las bases de datos de red con las nuevas direcciones IP de todos los sistemas de la subred.	Modificar <code>/etc/inet/hosts</code> y, para Solaris 10 11/06 y las versiones anteriores, <code>/etc/inet/ipnodes</code> en todos los hosts para que se reflejen las nuevas direcciones de host.	“Base de datos hosts” en la página 235
5. Reiniciar todos los sistemas.		

Mapa de tareas de configuración de red

La tabla siguiente muestra las tareas adicionales requeridas después de cambiar de una configuración de red sin subredes a una red que utiliza subredes. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener instrucciones
Configurar un host para el modo de archivos locales	Implica editar los archivos <code>nodename</code> , <code>hostname</code> , <code>hosts</code> , <code>defaultdomain</code> , <code>defaultrouter</code> y <code>netmasks</code>	“Cómo configurar un host para el modo de archivos locales” en la página 105
Configurar un servidor de configuración de red	Implica activar el daemon <code>in.tftpd</code> y editar los archivos <code>hosts</code> , <code>ethers</code> y <code>bootparams</code>	“Cómo instalar un servidor de configuración de red” en la página 107
Configurar un host para el modo de cliente de red	Implica crear el archivo <code>hostname</code> , editar el archivo <code>hosts</code> y eliminar los archivos <code>nodename</code> y <code>defaultdomain</code> , si existen	“Cómo configurar hosts para el modo de cliente de red” en la página 109

Tarea	Descripción	Para obtener instrucciones
Especificar una estrategia de enrutamiento para el cliente de red	Implica determinar si se utilizará el enrutamiento estático o dinámico en el host	“Cómo activar el enrutamiento estático en un host de interfaz única” en la página 132 y “Cómo activar el enrutamiento dinámico en un host de interfaz única” en la página 135.
Modificar la configuración de red existente	Implica cambiar el nombre de host, la dirección IP y otros parámetros configurados durante la instalación o posteriormente	“Cómo cambiar la dirección IPv4 y otros parámetros de configuración de red” en la página 110

Configuración de sistemas en la red local

La instalación del software de red tiene lugar durante la instalación del software del sistema operativo. En ese momento, deben guardarse determinados parámetros de configuración de IP en los archivos adecuados para que puedan leerse al iniciar.

El proceso de configuración de red implica crear o editar los archivos de configuración de red. El modo en que la información de configuración está disponible para el kernel de un sistema puede variar. La disponibilidad depende de si estos archivos se guardan localmente (modo de archivos locales) o se obtienen del servidor de configuración de red (modo de cliente de red).

Los parámetros que se proporcionan durante la configuración de red son:

- La dirección IP de cada interfaz de red en cada sistema.
- Los nombres de host de cada sistema de la red. Puede escribir el nombre de host en un archivo local o en una base de datos de servicios de nombres.
- El nombre de dominio DNS, NIS o LDAP en el que reside la base de datos, si es pertinente.
- Las direcciones de enrutador predeterminadas. Esta información se facilita en caso de tener una topología de red simple con un único enrutador conectado a cada red. También se facilita esta información si los enrutadores no ejecutan protocolos de enrutamiento como RDISC (Router Discovery Server Protocol) o RIP (Router Information Protocol). Para más información sobre los enrutadores predeterminados, consulte [“Reenvío de paquetes y rutas en redes IPv4” en la página 114](#). Consulte la [Tabla 5–1](#) para ver una lista de los protocolos de enrutamiento que admite Oracle Solaris.
- Máscara de subred (sólo se necesita para las redes con subredes).

Si el programa de instalación de Oracle Solaris detecta más de una interfaz en el sistema, tiene la opción de configurar las interfaces adicionales durante la instalación. Para obtener más información, consulte la [Guía de instalación de Oracle Solaris 10 9/10: instalaciones básicas](#).

Este capítulo contiene información sobre cómo crear y editar archivos de configuración locales. Consulte [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#) para obtener información sobre cómo trabajar con bases de datos de servicios de nombres.

▼ **Cómo configurar un host para el modo de archivos locales**

Siga este procedimiento para configurar el protocolo TCP/IP en un host que se ejecute en modo de archivos locales.

Para conocer los pasos para configurar manualmente las interfaces en Solaris 10 11/06 y versiones posteriores, consulte “[Cómo configurar una interfaz física tras la instalación del sistema](#)” en la página 148.

1 Asuma el rol de administrador principal, o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de [Guía de administración del sistema: administración básica](#).

2 Cambie al directorio /etc.

3 Compruebe que se haya configurado el nombre de host correcto en el archivo /etc/nodename.

Al especificar el nombre de host de un sistema durante la instalación de Oracle Solaris, dicho nombre se especifica en el archivo /etc/nodename. Asegúrese de que la entrada del nombre de nodo sea el nombre de host correcto para el sistema.

4 Compruebe que exista un archivo /etc/hostname.interfaz para cada interfaz de red del sistema.

Para obtener la sintaxis del archivo e información básica sobre el archivo /etc/hostname.interfaz, consulte “[Aspectos básicos sobre la administración de interfaces físicas](#)” en la página 145.

El programa de instalación de Oracle Solaris requiere la configuración de al menos una interfaz durante la instalación. La primera interfaz que se configura automáticamente se convierte en la *interfaz de red principal*. El programa de instalación crea un archivo /etc/hostname.interfaz para la interfaz de red principal y otras interfaces que configure de modo opcional durante la instalación.

Si ha configurado interfaces adicionales durante la instalación, compruebe que cada interfaz tenga un archivo /etc/hostname.interfaz correspondiente. No es necesario configurar más de una interfaz durante la instalación de Oracle Solaris. Sin embargo, si más adelante desea agregar más interfaces al sistema, debe configurarlas manualmente.

Para conocer los pasos para configurar manualmente las interfaces en Solaris 10 11/06 y versiones posteriores, consulte [“Cómo configurar una interfaz física tras la instalación del sistema” en la página 148](#).

5 Para Solaris 10 11/06 y las versiones anteriores, compruebe que las entradas del archivo `/etc/inet/ipnodes` sean actuales.

El programa de instalación de Oracle Solaris 10 crea el archivo `/etc/inet/ipnodes`. Este archivo contiene el nombre de nodo y las direcciones IPv4, así como la dirección IPv6, si es pertinente, de cada interfaz que se configure durante la instalación.

Utilice el formato siguiente para las entradas del archivo `/etc/inet/ipnodes`:

IP-address node-name nicknames...

Los *apodos* son nombres adicionales por los que se conoce una interfaz.

6 Compruebe que las entradas del archivo `/etc/inet/hosts` sean actuales.

El programa de instalación de Oracle Solaris crea entradas para la interfaz de red principal, la dirección en bucle y, si es preciso, cualquier interfaz adicional configurada durante la instalación.

a. Asegúrese de que las entradas de `/etc/inet/hosts` sean actuales.

b. (Opcional) Agregue las direcciones IP y los nombres correspondientes para las interfaces de red que se hayan agregado al host local tras la instalación.

c. (Opcional) Agregue la dirección o las direcciones IP del servidor de archivos, si el sistema de archivos `/usr` está montado con NFS.

7 Escriba el nombre de dominio completo de host en el archivo `/etc/defaultdomain`.

Por ejemplo, supongamos que el host `tenere` es parte del dominio `deserts.worldwide.com`. Por tanto, debería escribir `deserts.worldwide.com` en `/etc/defaultdomain`. Consulte [“Archivo `/etc/defaultdomain`” en la página 235](#) para obtener información adicional.

8 Escriba el nombre de enrutador en el archivo `/etc/defaultrouter`.

Consulte [“Archivo `/etc/defaultrouter`” en la página 235](#) para obtener información sobre este archivo.

9 Escriba el nombre del enrutador predeterminado y sus direcciones IP en el archivo `/etc/inet/hosts`.

Hay disponibles opciones de enrutamiento adicionales, tal como se describe en [“Cómo configurar hosts para el modo de cliente de red” en la página 109](#). Puede aplicar dichas opciones a una configuración de modo de archivos locales.

10 Agregue la máscara de red para su red, si es preciso:

- Si el host obtiene la dirección IP de un servidor DHCP, no es necesario especificar la máscara de red.
- Si ha configurado un servidor NIS en la misma red que este cliente, puede agregar información de netmask en la base de datos adecuada del servidor.
- Para las demás condiciones, haga lo siguiente:

a. Escriba el número de red y la máscara de red en el archivo `/etc/inet/netmasks`.

Use el siguiente formato:

```
network-number netmask
```

Por ejemplo, para el número de red de clase C 192.168.83, escribiría:

```
192.168.83.0 255.255.255.0
```

Para las direcciones CIDR, convierta el prefijo de red en la representación decimal con punto equivalente. Los prefijos de red y sus equivalentes decimales con punto se incluyen en la [Tabla 2-3](#). Por ejemplo, utilice lo siguiente para expresar el prefijo de red CIDR 192.168.3.0/22.

```
192.168.3.0 255.255.252.0
```

b. Cambie el orden de búsqueda de las máscaras de red en `/etc/nsswitch.conf`, para que se busquen los archivos locales en primer lugar:

```
netmasks: files nis
```

11 Reinicio el sistema.

▼ Cómo instalar un servidor de configuración de red

Puede encontrar información sobre cómo configurar servidores de instalación y servidores de arranque en [Guía de instalación de Oracle Solaris 10 9/10: instalaciones básicas](#)

1 Asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Cambie al directorio raíz (/) del servidor de configuración de red.

3 Active el daemon `in.tftpd` creando el directorio `/tftpboot`:

```
# mkdir /tftpboot
```

Este comando configura el sistema como servidor TFTP, bootparams y RARP.

4 Cree un vínculo simbólico al directorio.

```
# ln -s /tftpboot/. /tftpboot/tftpboot
```

5 Active la línea `tftp` en el archivo `/etc/inetd.conf`.

Compruebe que la entrada sea como la siguiente:

```
tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

Esta línea impide que `in.tftpd` recupere archivos que no sean los que se encuentran en `/tftpboot`.

6 Edite la base de datos `hosts`.

Agregue los nombres de host y direcciones IP para cada cliente de la red.

7 Edite la base de datos `ethers`.

Cree entradas para cada host en la red que se ejecute en modo de cliente de red.

8 Edite la base de datos `bootparams`.

Consulte “[Base de datos `bootparams`](#)” en la [página 249](#). Utilice la entrada de comodín o cree una entrada para cada host que se ejecute en modo de cliente de red.

9 Convierta la entrada `/etc/inetd.conf` en un manifiesto de servicio de la Utilidad de gestión de servicios (SMF), y active el servicio resultante:

```
# /usr/sbin/inetconv
```

10 Compruebe que `in.tftpd` funcione correctamente.

```
# svcs network/tftp/udp6
```

Obtendrá un resultado similar al siguiente:

```
STATE      STIME      FMRI
online     18:22:21   svc:/network/tftp/udp6:default
```

Más información **Administración del daemon `in.tftpd`**

La Utilidad de gestión de servicios administra el daemon `in.tftpd`. Las acciones administrativas de `in.tftpd`, como la activación, la desactivación o la solicitud de reinicio, pueden llevarse a cabo utilizando el comando `svcadm`. La responsabilidad de iniciar y reiniciar este servicio se delega al comando `inetd`. Utilice el comando `inetadm` para realizar cambios de configuración y ver la información de configuración para `in.tftpd`. Puede consultar el estado del servicio con el comando `svcs`. Para ver una descripción general de la Utilidad de gestión de servicios, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)” de *Guía de administración del sistema: administración básica*](#).

Configuración de clientes de red

Los clientes de red reciben la información de configuración de los servidores de configuración de red. En consecuencia, antes de configurar un host como cliente de red, debe asegurarse de que haya como mínimo un servidor de configuración de red para la red.

▼ Cómo configurar hosts para el modo de cliente de red

Siga este procedimiento en cada host que deba configurar en modo de cliente de red.

1 Asuma el rol de administrador principal, o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Busque el directorio `/etc` para el archivo `nodename`.

Si existe, elimínelo.

La eliminación de `/etc/nodename` hace que el sistema utilice el programa `hostconfig` para obtener el nombre de host, el nombre de dominio y las direcciones de enrutador del servidor de configuración de red. Consulte [“Configuración de sistemas en la red local”](#) en la [página 104](#).

3 Cree el archivo `/etc/hostname.interface`, si no existe.

Asegúrese de que el archivo esté vacío. Un archivo `/etc/hostname.interface` vacío hace que el sistema obtenga la dirección IPv4 del servidor de configuración de red.

4 Asegúrese de que el archivo `/etc/inet/hosts` contenga únicamente el nombre y la dirección IP de `localhost` de la interfaz de red en bucle.

```
# cat /etc/inet/hosts
# Internet host table
#
127.0.0.1      localhost
```

La interfaz en bucle IPv4 tiene la dirección IP `127.0.0.1`

Para más información, consulte [“Dirección en bucle”](#) en la [página 236](#). El archivo no debe contener la dirección IP ni el nombre de host para el host local (interfaz de red principal).

5 Compruebe que exista un archivo `/etc/defaultdomain`.

Si existe, elimínelo.

El programa `hostconfig` configura automáticamente el nombre de dominio. Para modificar el nombre de dominio que establece `hostconfig`, escriba el nombre de dominio que desee en el archivo `/etc/defaultdomain`.

- 6 **Asegúrese de que las rutas de búsqueda del archivo `/etc/nsswitch.conf` del cliente reflejen los requisitos del servicio de nombres para la red.**

▼ **Cómo cambiar la dirección IPv4 y otros parámetros de configuración de red**

Este procedimiento explica cómo modificar la dirección IPv4, el nombre de host y otros parámetros de red en un sistema instalado previamente. Siga el procedimiento para modificar la dirección IP de un servidor o sistema autónomo en red. El procedimiento no se aplica a los clientes o dispositivos en red. Estos pasos crean una configuración que persiste a pesar de los reinicios.

Nota – Las instrucciones tienen la finalidad de cambiar la dirección IPv4 de la interfaz de red principal. Para agregar otra interfaz al sistema, consulte [“Cómo configurar una interfaz física tras la instalación del sistema” en la página 148](#).

En la mayoría de los casos, los pasos siguientes utilizan la notación decimal con punto de IPv4 tradicional para especificar la dirección IPv4 y la máscara de subred. También puede utilizar la notación CIDR para especificar la dirección IPv4 en todos los archivos aplicables de este procedimiento. Para ver una introducción a la notación CIDR, consulte [“Direcciones IPv4 en formato CIDR” en la página 56](#).

- 1 **Asuma el rol de administrador principal, o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

- 2 **Sólo para Solaris 10 11/06 y las versiones anteriores, modifique la dirección IP del archivo `/etc/inet/ipnodes` o la base de datos `ipnodes` equivalente.**

Utilice la siguiente sintaxis para cada dirección IP que agregue al sistema:

IP-address host-name, nicknames

IP-address interface-name, nicknames

La primera entrada debe contener la dirección IP de la interfaz de red principal y el nombre de host del sistema. De modo opcional, puede agregar apodos para el nombre de host. Al agregar interfaces físicas adicionales a un sistema, cree entradas en `/etc/inet/ipnodes` para las direcciones IP y los nombres asociados de dichas interfaces.

- 3 **Si necesita cambiar el nombre de host del sistema, modifique la entrada de nombre de host en el archivo `/etc/nodename`.**

- 4 **Modifique la dirección IP y, si es preciso, el nombre de host en el archivo `/etc/inet/hosts` o la base de datos `hosts` equivalente.**

- 5 **Modifique la dirección IP con el comando `ipadm`.**

Con el comando `ipadm`, no puede modificar una dirección de IP directamente. Primero suprime el objeto de dirección que representa la dirección IP que desea modificar. A continuación, asigne una nueva dirección mediante la misma dirección nombre de objeto.

```
# ipadm delete-addr addrobj
# ipadm create-addr -T static IP-address addrobj
```

- 6 **Modifique la dirección IP del archivo `/etc/hostname.interface` para la interfaz de red principal.**

Puede utilizar cualquiera de las siguientes entradas como entrada para la interfaz de red principal en el archivo `/etc/hostname.interface`:

- Dirección IPv4, expresada en el formato decimal con punto tradicional

Use la sintaxis siguiente:

IPv4 address subnet mask

La entrada de máscara de red es opcional. Si no la especifica, se utiliza la máscara de red predeterminada.

A continuación le mostramos un ejemplo:

```
# vi hostname.eri0
10.0.2.5 netmask 255.0.0.0
```

- Direcciones IPv4, expresadas en la notación CIDR, si son adecuadas para la configuración de la red.

IPv4 address/network prefix

A continuación le mostramos un ejemplo:

```
# vi hostname.eri0
10.0.2.5/8
```

El prefijo CIDR indica la máscara de red adecuada para la dirección IPv4. Por ejemplo, el `/8` indica la máscara de red `255.0.0.0`.

- Nombre de host.

Para utilizar el nombre de host del sistema en el archivo `/etc/hostname.interface`, asegúrese de que el nombre de host y la dirección IPv4 asociada también estén en la base de datos `hosts`.

- 7 **Si la máscara de subred ha cambiado, modifique las entradas de subred en los archivos siguientes:**

- `/etc/netmasks`
- (Opcional) `/etc/hostname.interface`

8 Si la dirección de subred ha cambiado, cambie la dirección IP del enrutador predeterminado en `/etc/defaultrouter` a la dirección del nuevo enrutador predeterminado de la subred.

9 Reinicie el sistema.

```
# reboot -- -r
```

Ejemplo 5-1 Cómo modificar las direcciones IPv4 y otros parámetros de red para que persistan en los reinicios

Este ejemplo muestra cómo cambiar los siguientes parámetros de red de un sistema que se pasa a otra subred:

- La dirección IP de la interfaz de red principal `eri0` cambia de `10.0.0.14` a `192.168.55.14`.
- El nombre de host cambia de `myhost` a `mynewhostname`.
- La máscara de red cambia de `255.0.0.0` a `255.255.255.0`.
- La dirección del enrutador predeterminado cambia a `192.168.55.200`.

Compruebe el estado actual del sistema:

```
# hostname
myhost
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.14 netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:c1:8b:c3
```

A continuación, cambie el nombre de host del sistema y la dirección IP de `eri0` en los archivos adecuados:

```
# vi /etc/nodename
mynewhostname
```

En Oracle Solaris 10 11/06 y versiones anteriores de Oracle Solaris 10 únicamente, realice las siguientes acciones:

```
# vi /etc/inet/ipnodes
192.168.55.14    mynewhostname        #moved system to 192.168.55 net

# vi /etc/inet/hosts
#
# Internet host table
#
127.0.0.1        localhost
192.168.55.14    mynewhostname        loghost
# vi /etc/hostname.eri0
192.168.55.14    netmask    255.255.255.0
```

Finalmente, cambie la máscara de red y la dirección IP del enrutador predeterminado.


```
# vi /etc/netmasks
...
192.168.55.0    255.255.255.0

# vi /etc/defaultrouter
192.168.55.200    #moved system to 192.168.55 net
#
```

Una vez realizados los cambios, reinicie el sistema.

```
# reboot -- -r
```

Compruebe que la configuración que acaba de establecer persista tras el reinicio:

```
# hostname
mynewhostname
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.55.14 netmask fffffff0 broadcast 10.255.255.255
    ether 8:0:20:c1:8b:c3
```

Ejemplo 5-2 Cómo cambiar la dirección IP y el nombre de host para la sesión actual

Este ejemplo muestra cómo cambiar el nombre de un host, la dirección IP de la interfaz de red principal y la máscara de subred sólo para la sesión actual. Si reinicia, el sistema vuelve a tener la máscara de subred y la dirección IP anteriores. La dirección IP de la interfaz de red principal eri0 cambia de 10.0.0.14 a 192.168.34.100 .

```
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.14 netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:c1:8b:c3
# ifconfig eri0 192.168.34.100 netmask 255.255.255.0 broadcast + up
# vi /etc/nodename
mynewhostname

# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.34.100 netmask fffffff0 broadcast 10.255.255.255
    ether 8:0:20:c1:8b:c3

# hostname
mynewhostname
```

Ejemplo 5–3 Cómo cambiar la dirección IPv4 para la sesión actual, utilizando la notación CIDR

Este ejemplo muestra cómo cambiar un nombre de host y la dirección IP sólo para la sesión actual, utilizando la notación CIDR. Si reinicia, el sistema vuelve a tener la máscara de subred y la dirección IP anteriores. La dirección IP de la interfaz de red principal, `eri0`, cambia de `10.0.0.14` a `192.168.6.25/27`.

```
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.14 netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:c1:8b:c3
# ifconfig eri0 192.168.6.25/27 broadcast + up
# vi /etc/nodename
mynewhostname
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.06.25 netmask fffffffe0 broadcast 10.255.255.255
    ether 8:0:20:c1:8b:c3
# hostname
mynewhostname
```

Cuando utiliza la notación CIDR para la dirección IPv4, no es preciso especificar la máscara de red. `ifconfig` utiliza la designación de prefijo de red para determinar la máscara de red. Por ejemplo, para la red `192.168.6.0/27`, `ifconfig` configura la máscara de red `ffffffe0`. Si ha utilizado la designación de prefijo `/24` más común, la máscara de red resultante es `ffffff00`. El uso de la designación de prefijo `/24` equivale a especificar la máscara de red `255.255.255.0` como `ifconfig` al configurar una nueva dirección IP.

Véase también Para cambiar la dirección IP de una interfaz que no sea la interfaz de red principal, consulte [Guía de administración del sistema: administración básica](#) y “[Cómo configurar una interfaz física tras la instalación del sistema](#)” en la página 148.

Reenvío de paquetes y rutas en redes IPv4

Esta sección contiene los procedimientos y ejemplos que muestran cómo configurar el reenvío y las rutas de los enrutadores y hosts en las redes IPv4.

El *reenvío de paquetes* es el método básico para compartir información entre los sistemas de una red. Los paquetes se transfieren entre una interfaz de origen y una de destino, que normalmente se encuentran en dos sistemas diferentes. Al enviar un comando o un mensaje a una interfaz que no sea local, el sistema reenvía dichos paquetes a la red local. A continuación, la interfaz con la dirección IP de destino que se especifica en los encabezados del paquete recupera los paquetes

de la red local. Si la dirección de destino no se encuentra en la red local, los paquetes se reenvían a la siguiente red adyacente, o *salto*. De manera predeterminada, el reenvío de paquetes se configura de manera automática al instalar Oracle Solaris.

El *enrutamiento* es el proceso por el cual los sistemas deciden adónde enviar un paquete. Los protocolos de enrutamiento de un sistema "descubren" los otros sistemas de la red local. Cuando el sistema de origen y el de destino se encuentran en la misma red local, la ruta que recorren los paquetes entre ellos se denomina *ruta directa*. Si un paquete debe dar como mínimo un salto desde su sistema de origen, la ruta entre el sistema de origen y el de destino se denomina *ruta indirecta*. Los protocolos de enrutamiento recuerdan la ruta a una interfaz de destino y conservan los datos sobre las rutas conocidas en la *tabla de enrutamiento* del sistema.

Los *enrutadores* son sistemas configurados especialmente con varias interfaces físicas que conectan el enrutador a más de una red local. Por tanto, el enrutador puede reenviar paquetes más allá de la LAN de inicio, al margen de si el enrutador ejecuta un protocolo de enrutamiento. Para más información sobre el modo en que los enrutadores reenvían paquetes, consulte [“Planificación de enrutadores en la red” en la página 66](#).

Los *protocolos de enrutamiento* administran la actividad de enrutamiento de un sistema y, al intercambiar la información de rutas con otros hosts, mantienen las rutas conocidas para las redes remotas. Tanto los enrutadores como los hosts pueden ejecutar protocolos de enrutamiento. Los protocolos de enrutamiento del host se comunican con los daemons de enrutamiento de otros enrutadores y hosts. Estos protocolos ayudan al host a determinar a donde reenviar los paquetes. Cuando las interfaces de red están activas, el sistema automáticamente se comunica con los daemons de enrutamiento. Estos daemons supervisan los enrutadores de la red y publican las direcciones de los enrutadores para los hosts de la red local. Algunos protocolos de enrutamiento, aunque no todos, también guardan estadísticas que puede utilizar para medir el rendimiento del enrutamiento. A diferencia del reenvío de paquetes, debe configurar explícitamente el enrutamiento en un sistema Oracle Solaris.

Esta sección contiene las tareas necesarias para administrar el reenvío de paquetes y el enrutamiento en hosts y enrutadores habilitados para IPv4. Para obtener información sobre el enrutamiento en una red habilitada para IPv6, consulte [“Configuración de un enrutador IPv6” en la página 177](#).

Protocolos de enrutamiento admitidos por Oracle Solaris

Los protocolos de enrutamiento pueden ser de portal interior (IGP), de portal exterior (EGPs) o una combinación de ambos. Los *protocolos de portal interior* intercambian la información de enrutamiento entre los enrutadores de las redes bajo un control administrativo común. En la topología de red de la [Figura 5–3](#), los encaminadores ejecutan un IGP para intercambiar información de encaminamiento. Los *protocolos de portal exterior* permiten que el enrutador que conecta la interred local a una red externa intercambie información con otro enrutador de

la red externa. Por ejemplo, el enrutador que conecta una red corporativa a un ISP ejecuta un EGP para intercambiar información de enrutamiento con su enrutador equivalente del ISP. El protocolo de portal de límite (BGP) es un conocido protocolo EGP que se utiliza para transferir información de enrutamiento entre diferentes organizaciones e IGP.

La tabla siguiente proporciona información sobre los protocolos de enrutamiento de Oracle Solaris y la ubicación de la documentación asociada a cada protocolo.

TABLA 5-1 Protocolos de enrutamiento de Oracle Solaris

Protocolo	Daemon asociado	Descripción	Para obtener instrucciones
Protocolo Routing Information Protocol (RIP)	in.routed	IGP que enruta paquetes IPv4 y mantiene una tabla de enrutamiento	“Configuración de un enrutador IPv4” en la página 121
Descubrimiento de enrutador de protocolo de mensajes de control de Internet (ICMP)	in.routed	Lo utilizan los hosts para descubrir la presencia de un enrutador en la red	“Cómo activar el enrutamiento estático en un host de interfaz única” en la página 132 y “Cómo activar el enrutamiento dinámico en un host de interfaz única” en la página 135
Protocolo de información de enrutamiento, nueva generación (RIPng)	in.ripngd	IGP que enruta paquetes IPv6 y mantiene una tabla de enrutamiento	“Cómo configurar un enrutador habilitado para IPv6” en la página 178
Protocolo de descubrimiento de vecinos (ND)	in.ndpd	Advierte la presencia de un enrutador IPv6 y descubre la presencia de hosts IPv6 en una red	“Configuración de una interfaz de IPv6” en la página 171

Oracle Solaris también admite los protocolos de enrutamiento de código abierto Quagga. Estos protocolos están disponibles en el disco de consolidación de SFW, aunque no forman parte de la distribución principal de Oracle Solaris. La tabla siguiente enumera los protocolos Quagga.

TABLA 5-2 Protocolos OpenSolaris Quagga

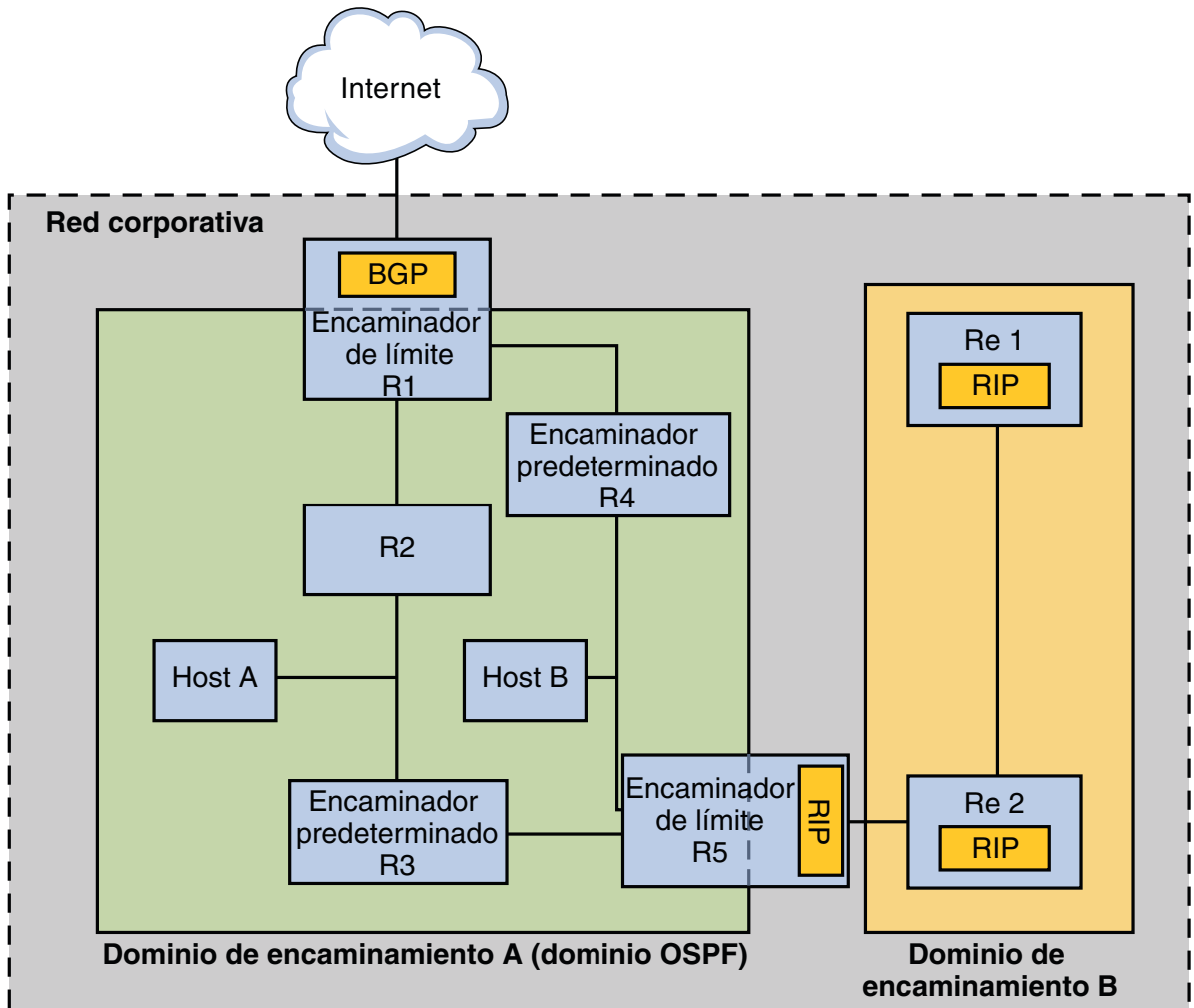
Protocolo	Daemon	Descripción
Protocolo RIP	ripd	Protocolo IGP vector-distancia para IPv4 que enruta paquetes IPv4 y muestra su tabla de enrutamiento a los vecinos.
RIPng	ripngd	Protocolo IGP vector-distancia para IPv6. Enruta paquetes IPv6 y mantiene una tabla de enrutamiento.
Protocolo Abrir primero la ruta más corta (OSPF)	ospfd	Protocolo IGP de estado de vínculo IPv4 para el enrutamiento de paquetes y las redes de gran disponibilidad.

TABLA 5-2 Protocolos OpenSolaris Quagga (Continuación)

Protocolo	Daemon	Descripción
Protocolo de portal de límite (BGP)	bgpd	Protocolo EGP para IPv4 y IPv6 para el enrutamiento en dominios administrativos.

La figura siguiente muestra un sistema autónomo que utiliza los protocolos de enrutamiento Quagga.

FIGURA 5-2 Red corporativa que ejecuta protocolos Quagga



La figura muestra un sistema autónomo de red corporativa subdividido en dos dominios de enrutamiento: A y B. Un *dominio de enrutamiento* es una interred con una directiva de enrutamiento cohesiva, para fines administrativos o porque el dominio utiliza un único protocolo de enrutamiento. Ambos dominios de la figura ejecutan protocolos de enrutamiento desde el conjunto de protocolos Quagga.

El dominio de enrutamiento A es un dominio OSPF, que se administra con un único ID de dominio OSPF. Todos los sistemas de este dominio ejecutan OSPF como protocolo de portal interior. Además de los hosts y enrutadores internos, el dominio A incluye dos enrutadores de límite.

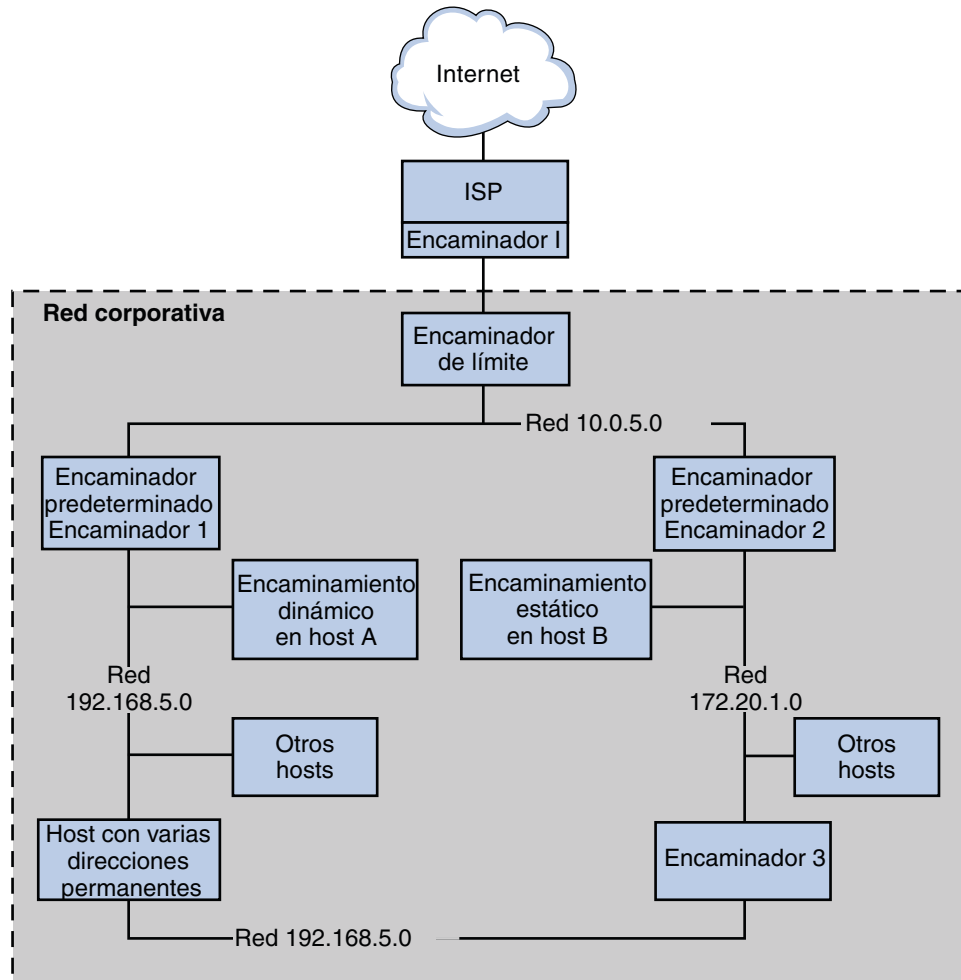
El enrutador R1 conecta la red corporativa a un ISP y finalmente a Internet. Para facilitar las comunicaciones entre la red corporativa y el exterior, R1 ejecuta BGP en su interfaz de red dirigida al exterior. El enrutador de límite R5 conecta el dominio A con el dominio B. Todos los sistemas del dominio B se administran con RIP como protocolo de portal interior. Por tanto, el enrutador de límite R5 debe ejecutar OSPF en la interfaz dirigida al dominio A y RIP en la interfaz dirigida al dominio B.

Para obtener más información acerca de los protocolos Quagga, consulte [Open Solaris Quagga](http://hub.opensolaris.org/bin/view/Project+quagga/) (<http://hub.opensolaris.org/bin/view/Project+quagga/>). Para obtener información acerca de los procedimientos de configuración de estos protocolos, visite [documentación de Quagga](http://quagga.net/docs/docs-info.php) (<http://quagga.net/docs/docs-info.php>).

Topología de sistemas autónomos IPv4

Los sitios con varios enrutadores y redes normalmente administran su topología de red como dominio de enrutamiento único, o *sistema autónomo* (SA). La figura siguiente muestra una topología de red típica que podría considerarse un pequeño SA. En los ejemplos de esta sección se hace referencia a esta topología.

FIGURA 5-3 Sistema autónomo con varios enrutadores IPv4



La figura muestra un SA dividido en tres redes locales: 10.0.5.0, 172.20.1.0 y 192.168.5.0. Cuatro enrutadores comparten las responsabilidades de reenvío de paquetes y enrutamiento. El SA incluye los siguientes tipos de sistemas:

- Los *enrutadores de límite* conectan un SA con una red externa, como Internet. Los enrutadores de límite se interconectan con redes externas al IGP que se ejecuta en el SA local. Un enrutador de límite puede ejecutar un EGP, como BGP, para intercambiar información con enrutadores externos, por ejemplo los enrutadores del ISP. En la [Figura 5-3](#), las interfaces del encaminador de límite se conectan a la red interna 10.0.5.0 y a un encaminador de alta velocidad de un proveedor de servicios.

Para obtener información sobre cómo configurar un enrutador de límite, consulte la [documentación de Open Source Quagga \(http://www.quagga.net/docs/docs-info.php#SEC72\)](http://www.quagga.net/docs/docs-info.php#SEC72) para BGP.

Si tiene previsto utilizar BGP para conectar el SA con Internet, debe obtener un número de sistema autónomo (ASN) del registro de Internet para su configuración regional. Los registros regionales, como ARIN (American Registry for Internet Numbers), incluyen las pautas para obtener un ASN. Por ejemplo, [ARIN Number Resource Policy Manual \(http://www.arin.net/policy/nrpm.html#five\)](http://www.arin.net/policy/nrpm.html#five) contiene instrucciones para obtener un ASN para sistemas autónomos en Estados Unidos y Canadá. Su ISP también puede facilitarle un ASN.

- Los *enrutadores predeterminados* guardan la información de enrutamiento en la red local. Estos enrutadores normalmente ejecutan IGP como RIP. En la [Figura 5-3](#), las interfaces del enrutador 1 están conectadas a las redes internas 10.0.5.0 y 192.168.5. El enrutador 1 también sirve como enrutador predeterminado para 192.168.5. El enrutador 1 guarda la información de enrutamiento para todos los sistemas en 192.168.5 y la dirige a otros enrutadores, como el enrutador de límite. Las interfaces del enrutador 2 se conectan a las redes internas 10.0.5.0 y 172.20.1.

Para ver un ejemplo de configuración de un encaminador predeterminado, consulte el [Ejemplo 5-4](#).

- Los *enrutadores de reenvío de paquetes* reenvían paquetes pero no ejecutan protocolos de enrutamiento. Este tipo de enrutador recibe paquetes de una de sus interfaces que está conectada a una única red. A continuación, estos paquetes se reenvían mediante otra interfaz del enrutador a otra red local. En la [Figura 5-3](#), el enrutador 3 es un enrutador de reenvío de paquetes con conexiones a las redes 172.20.1 y 192.168.5.
- Los *hosts múltiples* tienen dos o más interfaces conectadas al mismo segmento de red. Un host múltiple puede reenviar paquetes, que es la acción predeterminada para todos los sistemas que ejecutan Oracle Solaris. La [Figura 5-3](#) muestra un host múltiple con ambas interfaces conectadas a la red 192.168.5. El [Ejemplo 5-6](#) muestra cómo configurar un host múltiple.
- Los *hosts de interfaz única* dependen de los encaminadores locales, no sólo para reenviar paquetes, sino también para recibir información de configuración de gran valor. La [Figura 5-3](#) incluye el host A en la red 192.168.5, que implementa un encaminamiento dinámico, y el host B en la red 172.20.1, que implementa un encaminamiento estático. Para configurar un host para ejecutar encaminamiento dinámico, consulte “[Cómo activar el enrutamiento dinámico en un host de interfaz única](#)” en la página 135. Para configurar un host para ejecutar enrutamiento estático, consulte “[Cómo activar el enrutamiento estático en un host de interfaz única](#)” en la página 132.

Configuración de un enrutador IPv4

Esta sección contiene un procedimiento y un ejemplo para configurar un enrutador IPv4. Para configurar un enrutador habilitado para IPv6, consulte [“Cómo configurar un enrutador habilitado para IPv6” en la página 178](#).

Dado que un enrutador proporciona la interfaz entre dos o más redes, debe asignar un nombre exclusivo y una dirección IP a cada interfaz de red física del enrutador. Por tanto, cada enrutador tiene un nombre de host y una dirección IP asociados con su interfaz de red principal, además de otro nombre exclusivo y dirección IP, como mínimo, para cada interfaz de red adicional.

También puede utilizar el siguiente procedimiento para configurar un sistema sólo con una interfaz física (de modo predeterminado, un host) como enrutador. Puede configurar un sistema con una sola interfaz si el sistema actúa como punto final en un vínculo PPP, tal como se describe en [“Planificación de un enlace de PPP por marcación telefónica” de Guía de administración del sistema: servicios de red](#).

Nota – Puede configurar todas las interfaces de un enrutador durante la instalación de Oracle Solaris. Para obtener más información, consulte [Guía de instalación de Oracle Solaris 10 9/10: instalaciones básicas](#).

▼ Configuración de un enrutador IPv4

Las instrucciones siguientes presuponen que está configurando interfaces para el enrutador tras la instalación.

Antes de empezar

Una vez el enrutador está instalado físicamente en la red, configúrelo para que funcione en modo de archivos locales, tal como se describe en [“Cómo configurar un host para el modo de archivos locales” en la página 105](#). Con esta configuración, los enrutadores se reiniciarán si el servidor de configuración de red no funciona.

- 1 **En el sistema que va a configurar como enrutador, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

- 2 **A partir de Solaris 10 1/06, utilice el comando `dladm show-link` para determinar qué interfaces están instaladas físicamente en el enrutador.**

```
# dladm show-link
```

El siguiente ejemplo de resultado de `dladm show-link` indica que en el sistema hay disponibles una tarjeta NIC `qfe` con cuatro interfaces y dos interfaces `bge`.

```
qfe0          type: legacy    mtu: 1500    device: qfe0
qfe1          type: legacy    mtu: 1500    device: qfe1
qfe2          type: legacy    mtu: 1500    device: qfe0
qfe3          type: legacy    mtu: 1500    device: qfe1
bge0          type: non-vlan  mtu: 1500    device: bge0
bge1          type: non-vlan  mtu: 1500    device: bge1
```

3 Revise las interfaces del enrutador que se han configurado y sondeado durante la instalación.

```
# ifconfig -a
```

El resultado siguiente de `ifconfig -a` muestra que se ha configurado la interfaz `qfe0` durante la instalación. Esta interfaz se encuentra en la red `172.16.0.0`. Las interfaces restantes de NIC `qfe`, `qfe1` - `qfe3` y las interfaces `bge` no se han configurado.

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
      inet 127.0.0.1 netmask ff000000
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 172.16.26.232 netmask ffff0000 broadcast 172.16.26.255
      ether 0:3:ba:11:b1:15
```

4 Configure y sondee otro comando interfaz.

```
# ifconfig interface plumb up
```

Por ejemplo, para `qfe1`, escribiría:

```
# ifconfig qfe1 plumb up
```

Nota – Las interfaces que se configuran explícitamente con el comando `ifconfig` no persisten tras un reinicio.

5 Asigne una dirección IPv4 y una máscara de red a la interfaz.



Precaución – Puede configurar un enrutador IPv4 para que reciba su dirección IP a través de DHCP, pero sólo se recomienda hacerlo a los administradores de sistemas DHCP experimentados.

```
# ifconfig interface IPv4-address netmask+netmask
```

Por ejemplo, para asignar la dirección IP `192.168.84.3` a `qfe1`, haga lo siguiente:

- Utilizando la notación IPv4 tradicional, escriba:

```
# ifconfig qfe1 192.168.84.3 netmask + 255.255.255.0
```
- Utilizando la notación CIDR, escriba:

```
# ifconfig qfe1 192.168.84.3/24
```

El prefijo /24 asigna automáticamente la máscara de red 255.255.255.0 a qfe1. Consulte la tabla de prefijos CIDR y sus equivalentes de máscara de red de decimal con punto en la [Figura 2-2](#).

- 6 (Opcional) Para asegurarse de que la configuración de la interfaz se conserve tras los rearranques, cree un archivo /etc/hostname.interfaz para cada interfaz física adicional.**

Por ejemplo, cree los archivos /etc/hostname.qfe1 y /etc/hostname.qfe2. A continuación, escriba el nombre de host timbuktú en el archivo /etc/hostname.qfe1 y el nombre de host timbuktú-201 en /etc/hostname.qfe1. Para obtener más información sobre cómo configurar interfaces únicas, consulte “[Cómo configurar una interfaz física tras la instalación del sistema](#)” en la [página 148](#).

Asegúrese de reiniciar la configuración tras crear el archivo:

```
# reboot -- -r
```

- 7 Agregue el nombre de host y la dirección IP de cada interfaz al archivo /etc/inet/hosts.**

Por ejemplo:

```
172.16.26.232    deadsea        #interface for network 172.16.0.0
192.168.200.20  timbuktú       #interface for network 192.168.200
192.168.201.20  timbuktú-201   #interface for network 192.168.201
192.168.200.9   gobi          #
192.168.200.10  mojave         #
192.168.200.110 saltlake       #
192.168.200.12  chilean        #
```

Las interfaces timbuktú y timbuktú-201 se encuentran en el mismo sistema. Observe que la dirección de red para timbuktú-201 es diferente de la interfaz de red para timbuktú. Esa diferencia existe porque el medio de red físico de la red 192.168.201 está conectado a la interfaz de red timbuktú-201, mientras que el medio de la red 192.168.200 está conectado a la interfaz timbuktú.

- 8 Sólo para Solaris 10 11/06 y las versiones anteriores de Solaris 10, agregue la dirección IP y el nombre de host de cada interfaz nueva en el archivo /etc/inet/ipnodes o la base de datos ipnodes equivalente.**

Por ejemplo:

```
vi /etc/inet/ipnodes
172.16.26.232    deadsea        #interface for network 172.16.0.0
192.168.200.20  timbuktú       #interface for network 192.168.200
192.168.201.20  timbuktú-201   #interface for network 192.168.201
```

- 9 Si el enrutador está conectado a una red con subredes, agregue el número de red y la máscara de red al archivo /etc/inet/netmasks.**

- Para la notación de direcciones IPv4 tradicional, como 192.168.83.0, debería escribir:

```
192.168.83.0    255.255.255.0
```

- Para las direcciones CIDR, utilice la versión de decimal con punto del prefijo en la entrada del archivo `/etc/inet/netmask`. Los prefijos de red y sus equivalentes decimales con punto se pueden encontrar en la [Figura 2-2](#). Por ejemplo, debe utilizar la entrada siguiente de `/etc/netmasks` para expresar el prefijo de red CIDR `192.168.3.0/22`:

```
192.168.3.0 255.255.252.0
```

10 Habilite el reenvío de paquetes IPv4 en el enrutador.

Utilice uno de los siguientes comandos para habilitar el reenvío de paquetes:

- Utilice el comando `routeadm`, del modo siguiente:

```
# routeadm -e ipv4-forwarding -u
```
- Utilice el siguiente comando de la Utilidad de gestión de servicios (SMF):

```
# svcadm enable ipv4-forwarding
```

En este punto, el enrutador puede reenviar paquetes más allá de la red local. El enrutador también admite el *enrutamiento estático*, un proceso que permite agregar manualmente rutas a la tabla de enrutamiento. Si tiene previsto utilizar enrutamiento estático en este sistema, habrá finalizado la configuración del enrutador. Sin embargo, debe guardar las rutas en la tabla de enrutamiento del sistema. Para obtener información sobre cómo agregar rutas, consulte “[Configuración de rutas](#)” en la [página 127](#) y la página del comando `man route(1M)`.

11 (Opcional) Inicie un protocolo de enrutamiento.

El daemon de enrutamiento `/usr/sbin/in.routed` actualiza automáticamente la tabla de enrutamiento. Este proceso se conoce como *enrutamiento dinámico*. Active los protocolos de enrutamiento IPv4 predeterminados de uno de los modos siguientes:

- Utilice el comando `routeadm`, del modo siguiente:

```
# routeadm -e ipv4-routing -u
```
- Utilice el siguiente comando de SMF para iniciar un protocolo de enrutamiento como RIP.

```
# svcadm enable route:default
```

El FMRI SMF asociado con el daemon `in.routed` es `svc:/network/routing/route`.

Para obtener información sobre el comando `routeadm`, consulte la página del comando `man routeadm(1M)`.

Ejemplo 5-4 Configuración del enrutador predeterminado para una red

Este ejemplo muestra cómo actualizar un sistema con más de una interfaz para convertirlo en un encaminador predeterminado. El objetivo es convertir el enrutador 2, que se muestra en la [Figura 5-3](#), en el enrutador predeterminado de la red `172.20.1.0`. El encaminador 2 contiene dos conexiones de red cableadas, una conexión a la red `172.20.1.0` y otra a la red `10.0.5.0`. El ejemplo presupone que el enrutador funciona en el modo de archivos locales, tal como se describe en “[Cómo configurar un host para el modo de archivos locales](#)” en la [página 105](#).

Una vez se haya convertido en superusuario o haya asumido un rol equivalente, debe determinar el estado de las interfaces del sistema. A partir de Solaris 10 1/06, puede utilizar el comando `dladm` del modo siguiente:

```
# dladm show-link
ce0          type: legacy      mtu: 1500      device: ce0
bge0         type: non-vlan   mtu: 1500      device: bge0
bge1         type: non-vlan   mtu: 1500      device: bge1

# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 172.20.1.10 netmask ffff0000 broadcast 172.20.10.100
    ether 8:0:20:c1:1b:c6
```

El resultado de `dladm show-link` indica que hay tres vínculos disponibles en el sistema. Sólo la interfaz `ce0` ha sido configurada con una dirección IP. Para iniciar la configuración de enrutador predeterminada, debe sondear físicamente la interfaz `bge0` a la red `10.0.5.0`. A continuación, debe sondear la interfaz y configurarla para que persista tras los reinicios.

```
# ifconfig bge0 plumb up
# ifconfig bge0 10.0.5.10
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 172.20.1.10 netmask ffff0000 broadcast 172.255.255.255
    ether 8:0:20:c1:1b:c6
bge0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.5.10 netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:e5:95:c4

# vi /etc/hostname.bge0
10.0.5.10
255.0.0.0
```

Reinicie el sistema utilizando el comando de inicio de reconfiguración:

```
# reboot -- -r
```

Siga configurando las siguientes bases de datos de red con información sobre la interfaz que acaba de sondear y la red a la que está conectada:

```
# vi /etc/inet/hosts
127.0.0.1      localhost
172.20.1.10    router2          #interface for network 172.20.1
10.0.5.10      router2-out     #interface for network 10.0.5
# vi /etc/inet/netmasks
172.20.1.0     255.255.0.0
10.0.5.0       255.0.0.0
```

Finalmente, utilice SMF para activar el reenvío de paquetes y luego active el daemon de enrutamiento `in.routed`.

```
# svcadm enable ipv4-forwarding
# svcadm enable route:default
```

Ahora el reenvío de paquetes IPv4 y el enrutamiento dinámico mediante RIP están activados en el enrutador 2. Sin embargo, la configuración de enrutador predeterminada para la red 172.20.1.0 todavía no se ha completado. Debe hacer lo siguiente:

- Modificar cada host de 172.10.1.10 para que obtenga su información de enrutamiento del nuevo enrutador predeterminado. Para más información, consulte [“Cómo activar el enrutamiento estático en un host de interfaz única” en la página 132](#).
- Defina una ruta estática para el enrutador de límite en la tabla de enrutamiento del enrutador 2. Para obtener más información, consulte [“Tablas y tipos de enrutamiento” en la página 126](#).

Tablas y tipos de enrutamiento

Tanto los enrutadores como los hosts guardan una *tabla de enrutamiento*. El daemon de enrutamiento de cada sistema actualiza la tabla con todas las rutas conocidas. El núcleo del sistema lee la tabla de enrutamiento antes de reenviar paquetes a la red local. La tabla de enrutamiento enumera las direcciones IP de las redes que conoce el sistema, incluida la red local predeterminada del sistema. La tabla también enumera la dirección IP de un sistema de portal para cada red conocida. El *portal* es un sistema que puede recibir paquetes de salida y reenviarlos un salto más allá de la red local. A continuación se incluye una tabla de enrutamiento simple en una red sólo de IPv4:

Routing Table: IPv4					
Destination	Gateway	Flags	Ref	Use	Interface
default	172.20.1.10	UG	1	532	ce0
224.0.0.0	10.0.5.100	U	1	0	bge0
10.0.0.0	10.0.5.100	U	1	0	bge0
127.0.0.1	127.0.0.1	UH	1	57	lo0

En un sistema Oracle Solaris puede configurar dos tipos de enrutamiento: estático y dinámico. Puede configurar uno o ambos tipos de enrutamiento en un único sistema. Un sistema que implementa *enrutamiento dinámico* se basa en los protocolos de enrutamiento, como RIP para redes IPv4 y RIPng para redes IPv6, con el fin de mantener sus tablas de enrutamiento. Un sistema que sólo ejecuta *enrutamiento estático* no se basa en ningún protocolo de enrutamiento para la información de enrutamiento ni para actualizar la tabla de enrutamiento. Es preciso guardar las rutas conocidas del sistema manualmente con el comando `route`. Para obtener más información al respecto, consulte la página del comando `man route(1M)`.

Al configurar el enrutamiento para la red local o el sistema autónomo, considere el tipo de enrutamiento que desea para los hosts y enrutadores específicos.

La tabla siguiente muestra los diversos tipos de enrutamiento y las redes para las que es adecuado cada tipo.

Tipo de enrutamiento	Recomendado para
Estático	Hosts y redes de tamaño reducido que obtienen las rutas de un enrutador predeterminado, y enrutadores predeterminados que sólo necesitan conocer uno o dos enrutadores en los siguientes saltos.
Dinámico	Interredes de mayor tamaño, enrutadores en redes locales con múltiples hosts y hosts de sistemas autónomos de gran tamaño. El enrutamiento dinámico es la mejor opción para los sistemas en la mayoría de las redes.
Estático y dinámico combinados	Enrutadores que conectan una red con enrutamiento estático y una red con enrutamiento dinámico, y enrutadores de límite que conectan un sistema autónomo interior con redes externas. La combinación del enrutamiento estático y dinámico en un sistema es una práctica habitual.

El SA que se muestra en la [Figura 5–3](#) combina el enrutamiento estático y el dinámico.

Configuración de rutas

Para implementar el enrutamiento dinámico para una red IPv4, utilice el comando `routeadm` o `svcadm` para iniciar el daemon de enrutamiento `in.routed`. Para ver las instrucciones, consulte “[Configuración de un enrutador IPv4](#)” en la [página 121](#). El enrutamiento dinámico es la estrategia preferida para la mayoría de las redes y sistemas autónomos. Sin embargo, la topología de red o un sistema específico de la red podrían requerir el enrutamiento estático. En tal caso, debe editar manualmente la tabla de enrutamiento del sistema para que refleje la ruta conocida al portal. El siguiente procedimiento muestra cómo agregar una ruta estática.

Nota – Dos rutas al mismo destino no hacen que el sistema ejecute automáticamente la función de equilibrio de carga o fallos. Si necesita estas funciones, utilice IPMP, tal como se describe en el [Capítulo 30](#), “[Introducción a IPMP \(descripción general\)](#)”.

▼ Cómo agregar una ruta estática a la tabla de enrutamiento

1 Visualice el estado actual de la tabla de enrutamiento.

Utilice su cuenta de usuario habitual para ejecutar el siguiente comando `netstat`:

```
% netstat -rn
```

Obtendrá un resultado similar al siguiente:

```
Routing Table: IPv4
  Destination          Gateway             Flags   Ref    Use  Interface
-----
192.168.5.125         192.168.5.10       U        1   5879   ipge0
224.0.0.0             198.168.5.10       U        1     0   ipge0
default              192.168.5.10       UG       1  91908
127.0.0.1            127.0.0.1          UH       1  811302  lo0
```

2 Asuma el rol de administrador principal, o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

3 (Opcional) Vacíe las entradas existentes en la tabla de enrutamiento.

```
# route flush
```

4 Agregue una ruta que persista tras el reinicio del sistema.

```
# route -p add -net network-address -gateway gateway-address
```

-p Crea una ruta que debe persistir tras el reinicio del sistema. Si desea que la ruta sea válida sólo para la sesión actual, no utilice la opción -p.

add Indica que está a punto de agregar la siguiente ruta.

-net *dirección_red* Especifica que la ruta se dirige a la red con la dirección de *dirección_red*.

-gateway *dirección_portal* Indica que el sistema de portal para la ruta especificada tiene la dirección IP *dirección_portal*.

Ejemplo 5-5 Cómo agregar una ruta estática a la tabla de enrutamiento

El siguiente ejemplo muestra cómo agregar una ruta estática a un sistema. El sistema es el encaminador 2, el encaminador predeterminado para la red 172.20.1.0 que se muestra en la [Figura 5-3](#). En el [Ejemplo 5-4](#), el encaminador 2 está configurado para el encaminamiento dinámico. Para actuar como enrutador predeterminado para los hosts de la red 172.20.1.0, el enrutador 2 necesita además una ruta estática al enrutador de límite del SA, 10.0.5.150.

Para ver la tabla de enrutamiento del enrutador 2, debe configurar lo siguiente:

```
# netstat -rn
Routing Table: IPv4
```

Destination	Gateway	Flags	Ref	Use	Interface
default	172.20.1.10	UG	1	249	ce0
224.0.0.0	172.20.1.10	U	1	0	ce0
10.0.5.0	10.0.5.20	U	1	78	bge0
127.0.0.1	127.0.0.1	UH	1	57	lo0

La tabla de enrutamiento indica las dos rutas que conoce el enrutador 2. La ruta predeterminada utiliza la interfaz 172.20.1.10 del enrutador 2 como portal. La segunda ruta, 10.0.5.0, fue descubierta por el daemon `in.routed` que se ejecuta en el enrutador 2. El portal de esta ruta es el enrutador 1, con la dirección IP 10.0.5.20.

Para agregar una segunda ruta a la red 10.0.5.0, que tiene su portal como enrutador de límite, debe configurar lo siguiente:

```
# route -p add -net 10.0.5.0/24 -gateway 10.0.5.150/24
add net 10.0.5.0: gateway 10.0.5.150
```

Ahora la tabla de enrutamiento cuenta con una ruta para el enrutador de límite, que tiene la dirección IP 10.0.5.150/24.

```
# netstat -rn
Routing Table: IPv4
  Destination      Gateway            Flags  Ref    Use  Interface
-----
default            172.20.1.10        UG          1     249   ce0
224.0.0.0          172.20.1.10        U           1         0   ce0
10.0.5.0           10.0.5.20          U           1         78  bge0
10.0.5.0           10.0.5.150         U           1        375  bge0
127.0.0.1          127.0.0.1          UH          1         57   lo0
```

Configuración de hosts múltiples

En Oracle Solaris, un sistema con más de una interfaz se considera un *host múltiple*. Un host múltiple no reenvía paquetes IP. No obstante, puede configurar un host múltiple para que ejecute protocolos de enrutamiento. Normalmente se configuran los siguientes tipos de sistemas como hosts múltiples:

- Los servidores NFS, especialmente los que funcionan como grandes centros de datos, se pueden conectar a más de una red para que una agrupación de usuarios de gran tamaño pueda compartir archivos. No es necesario que estos servidores mantengan tablas de enrutamiento.
- Los servidores de bases de datos pueden tener varias interfaces de red para proporcionar recursos a una agrupación de usuarios de gran tamaño, como los servidores NFS.
- Los portales de cortafuegos son sistemas que proporcionan conexión entre la red de una compañía y las redes públicas como Internet. Los administradores configuran los cortafuegos como una medida de seguridad. Cuando se configura el host como un cortafuegos, no transfiere paquetes entre las redes conectadas a las interfaces del host. Sin embargo, el host puede seguir ofreciendo los servicios TCP/IP estándar, como ssh, a los usuarios autorizados.

Nota – Cuando los hosts múltiples tienen diferentes tipos de cortafuegos en cualquiera de sus interfaces, procure evitar las interrupciones involuntarias de los paquetes del host. Este problema sucede especialmente con los cortafuegos con estado. Una solución podría ser configurar los cortafuegos sin estado. Para más información sobre los cortafuegos, consulte “Sistemas de cortafuegos” de *Guía de administración del sistema: servicios de seguridad* o la documentación del cortafuegos si es de otro proveedor.

▼ **Cómo crear un host múltiple**

- 1 **En el host múltiple previsto, asuma la función de administrador principal o conviértase en superusuario.**
La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.
- 2 **Configure y conecte cada interfaz de red adicional que no se haya configurado como parte de la instalación de Oracle Solaris.**
Consulte [“Cómo configurar una interfaz física tras la instalación del sistema”](#) en la [página 148](#).

- 3 **Compruebe que el reenvío de IP no esté habilitado en el host múltiple.**
routeadm

El comando routeadm sin opciones informa del estado de los daemon de enrutamiento. El siguiente resultado de routeadm muestra que el reenvío de IPv4 está activo:

Configuration	Current Option	Current Configuration	System State
IPv4 routing		disabled	disabled
IPv6 routing		disabled	disabled
IPv4 forwarding		enabled	disabled
IPv6 forwarding		disabled	disabled
Routing services		"route:default ripng:default"	

- 4 **Desactive el reenvío de paquetes si está habilitado en el sistema.**
Utilice uno de los siguientes comandos:
 - Para el comando routeadm, escriba lo siguiente:
routeadm -d ipv4-forwarding -u
 - Para utilizar SME, escriba:
svcadm disable ipv4-forwarding

5 (Opcional) Active el enrutamiento dinámico para el host múltiple.

Utilice uno de los siguientes comandos para activar el daemon `in.routed`:

- Para el comando `routeadm`, escriba lo siguiente:

```
# routeadm -e ipv4-routing -u
```

- Para utilizar SME, escriba:

```
# svcadm enable route:default
```

Ejemplo 5-6 Configuración de un host múltiple

El ejemplo siguiente muestra cómo configurar el host múltiple que aparece en la [Figura 5-3](#). En el ejemplo, el sistema tiene el nombre de host `hostc`. Este host cuenta con dos interfaces, que están conectadas a la red `192.168.5.0`.

Para empezar, debe mostrar el estado de las interfaces del sistema.

```
# dladm show-link
hme0      type: legacy      mtu: 1500      device: hme0
qfe0      type: legacy      mtu: 1500      device: qfe0
qfe1      type: legacy      mtu: 1500      device: qfe1
qfe2      type: legacy      mtu: 1500      device: qfe2
qfe3      type: legacy      mtu: 1500      device: qfe3
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.5.82 netmask ff000000 broadcast 192.255.255.255
    ether 8:0:20:c1:1b:c6
```

El comando `dladm show-link` muestra que `hostc` tiene dos interfaces con un total de cinco vínculos posibles. Sin embargo, sólo se ha sondeado `hme0`. Para configurar `hostc` como host múltiple, debe agregar `qfe0` u otro vínculo en la tarjeta NIC `qfe`. En primer lugar, debe conectar físicamente la interfaz `qfe0` a la red `192.168.5.0`. A continuación, sondee la interfaz `qfe0` y haga que persista tras los reinicios.

```
# ifconfig qf0 plumb up
# ifconfig qfe0 192.168.5.85
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.5.82 netmask ff000000 broadcast 192.255.255.255
    ether 8:0:20:c1:1b:c6
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.5.85 netmask ff000000 broadcast 192.255.255.255
    ether 8:0:20:e1:3b:c4
# vi /etc/hostname.qfe0
192.168.5.85
255.0.0.0
```

Reinicie el sistema utilizando el comando de reconfiguración:

```
# reboot -- -r
```

A continuación, agregue la interfaz qfe0 a la base de datos hosts:

```
# vi /etc/inet/hosts
127.0.0.1      localhost
192.168.5.82   host3      #primary network interface for host3
192.168.5.85   host3-2    #second interface
```

A continuación, compruebe el estado del reenvío de paquetes y las rutas en host3:

```
# routeadm
Configuration Option      Current Configuration      Current System State
-----
IPv4 routing               enabled                     enabled
IPv6 routing               disabled                    disabled
IPv4 forwarding            enabled                     enabled
IPv6 forwarding            disabled                    disabled

Routing services           "route:default ripng:default"
```

El comando routeadm indica que el enrutamiento dinámico a través del daemon in.routed y el reenvío de paquetes están activos. Sin embargo, necesita deshabilitar el reenvío de paquetes:

```
# svcadm disable ipv4-forwarding
```

También puede utilizar los comandos routeadm como se indica en [“Cómo crear un host múltiple” en la página 130](#) para desactivar el reenvío de paquetes. Cuando el reenvío de paquetes está desactivado, host3 se convierte en un host múltiple.

Configuración del enrutamiento para sistemas de interfaz única

Los hosts de interfaz única deben implementar algún tipo de enrutamiento. Si el host tiene la finalidad de obtener sus rutas de uno o más enrutadores locales predeterminados, debe configurar el host para que utilice el enrutamiento estático. De lo contrario, se recomienda utilizar el enrutamiento dinámico para el host. Los procedimientos siguientes contienen las instrucciones para activar ambos tipos de enrutamiento.

▼ Cómo activar el enrutamiento estático en un host de interfaz única

Este procedimiento activa el enrutamiento estático en un host de interfaz única. Los hosts que utilizan enrutamiento estático no ejecutan un protocolo de enrutamiento dinámico como RIP. En lugar de ello, el host se basa en los servicios de un enrutador predeterminado para la

información de enrutamiento. La figura “[Topología de sistemas autónomos IPv4](#)” en la [página 118](#) muestra varios enrutadores predeterminados y sus hosts cliente. Si ha facilitado el nombre de un enrutador predeterminado al instalar un host específico, dicho host ya estará configurado para utilizar el enrutamiento estático.

Nota – También puede utilizar el procedimiento siguiente para configurar enrutamiento estático en un host múltiple.

Para obtener información sobre el archivo `/etc/defaultrouter`, consulte “[Archivo /etc/defaultrouter](#)” en la [página 235](#). Para obtener información sobre el enrutamiento estático y la tabla de enrutamiento, consulte “[Tablas y tipos de enrutamiento](#)” en la [página 126](#).

1 En el host de interfaz única, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2](#), “[Trabajo con Solaris Management Console \(tareas\)](#)” de *Guía de administración del sistema: administración básica*.

2 Compruebe que el archivo `/etc/defaultrouter` esté presente en el host.

```
# cd /etc
# ls | grep defaultrouter
```

3 Abra un editor de texto para crear o modificar el archivo `/etc/defaultrouter`.

4 Agregue una entrada para el enrutador predeterminado.

```
# vi /etc/defaultrouter
router-IP
```

donde *IP_enrutador* indica la dirección IP del enrutador predeterminado para el host que se debe usar.

5 Compruebe que el enrutamiento y el reenvío de paquetes no se estén ejecutando en el host.

```
# routeadm
Configuration      Current          Current
                   Option      Configuration    System State
-----
                   IPv4 routing    disabled         disabled
                   IPv6 routing    disabled         disabled
                   IPv4 forwarding disabled         disabled
                   IPv6 forwarding disabled         disabled

Routing services    "route:default  ripng:default"
```

6 Agregue una entrada para el enrutador predeterminado en el archivo `/etc/inet/hosts` local.

Para obtener información sobre cómo configurar `/etc/inet/hosts`, consulte [“Cómo cambiar la dirección IPv4 y otros parámetros de configuración de red”](#) en la página 110.

Ejemplo 5-7 Configuración de un enrutador predeterminado y enrutamiento estático para un host de interfaz única

El ejemplo siguiente muestra cómo configurar el encaminamiento estático para `hostb`, un host de interfaz única en la red `172.20.1.0` que aparece en la [Figura 5-3](#). `hostb` debe utilizar el encaminador 2 como predeterminado.

En primer lugar, debe iniciar sesión en `hostb` como superusuario o asumir un rol equivalente. A continuación, determine si el archivo `/etc/defaultrouter` está presente en el host:

```
# cd /etc
# ls | grep defaultrouter
```

Ninguna respuesta de `grep` indica que debe crear el archivo `/etc/defaultrouter`.

```
# vi /etc/defaultrouter
172.20.1.10
```

La entrada en el archivo `/etc/defaultrouter` es la dirección IP de la interfaz en el enrutador 2, que se conecta a la red `172.20.1.0`. A continuación, compruebe si el host permite el reenvío de paquetes o el enrutamiento.

```
# routeadm
Configuration      Current      Current
                   Option      Configuration      System State
-----
                   IPv4 routing disabled         disabled
                   IPv6 routing disabled         disabled
                   IPv4 forwarding enabled         enabled
                   IPv6 forwarding disabled        disabled

Routing services   "route:default ripng:default"
```

El reenvío de paquetes está activado para este host específico. Debe desactivarlo del modo siguiente:

```
# svcadm disable ipv4-forwarding
```

Por último, debe asegurarse de que el archivo `/etc/inet/hosts` del host tenga una entrada para el nuevo enrutador predeterminado.

```
# vi /etc/inet/hosts
127.0.0.1          localhost
172.20.1.18        host2    #primary network interface for host2
172.20.1.10        router2  #default router for host2
```

▼ Cómo activar el enrutamiento dinámico en un host de interfaz única

El enrutamiento dinámico es el modo más sencillo de administrar el enrutamiento en un host. Los hosts que utilizan enrutamiento dinámico ejecutan los protocolos de enrutamiento que proporciona el daemon `in.routed` para IPv4 o el daemon `in.ripngd` para IPv6. Utilice el procedimiento siguiente para activar el enrutamiento dinámico de IPv4 en un host de interfaz única. Para obtener información adicional sobre el enrutamiento dinámico, consulte [“Reenvío de paquetes y rutas en redes IPv4” en la página 114](#).

1 En el host, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Compruebe que exista el archivo `/etc/defaultrouter`.

```
# cd /etc
# ls | grep defaultrouter
```

3 Si `/etc/defaultrouter` existe, elimine cualquier entrada que encuentre.

Un archivo `/etc/defaultrouter` vacío obliga al host a utilizar el enrutamiento dinámico.

4 Compruebe que el reenvío de paquetes y el enrutamiento estén activados en el host.

```
# routeadm
```

Configuration	Current Option	Current Configuration	System State
	IPv4 routing	disabled	disabled
	IPv6 routing	disabled	disabled
	IPv4 forwarding	enabled	enabled
	IPv6 forwarding	disabled	disabled
Routing services		"route:default ripng:default"	

5 Si el reenvío de paquetes está activo, desactívelo.

Utilice uno de los siguientes comandos:

- Para el comando `routeadm`, escriba lo siguiente:

```
# routeadm -d ipv4-forwarding -u
```

- Para utilizar SME, escriba:

```
# svcadm disable ipv4-forwarding
```

6 Active los protocolos de enrutamiento en el host.

Utilice uno de los siguientes comandos:

- Para el comando `routeadm`, escriba lo siguiente:

```
# routeadm -e ipv4-routing -u
■ Para utilizar SME, escriba:
# svcadm enable route:default
```

Ahora el enrutamiento dinámico de IPv4 estará activo. La tabla de enrutamiento del host se guarda de forma dinámica mediante el daemon `in.routed`.

Ejemplo 5-8 Cómo ejecutar el encaminamiento dinámico en un host de interfaz única

El ejemplo siguiente muestra cómo configurar el enrutamiento dinámico para `hosta`, un host de interfaz única en la red `192.168.5.0` que aparece en la [Figura 5-3](#). `hosta` utiliza actualmente el enrutador 1 como predeterminado. Sin embargo, `hosta` ahora debe ejecutar enrutamiento dinámico.

En primer lugar, debe iniciar sesión en `hosta` como superusuario o asumir un rol equivalente. A continuación, determine si el archivo `/etc/defaultrouter` está presente en el host:

```
# cd /etc
# ls | grep defaultrouter
defaultrouter
```

La respuesta de `grep` indica que existe un archivo `/etc/defaultrouter` para `hosta`.

```
# vi /etc/defaultrouter
192.168.5.10
```

El archivo presenta la entrada `192.168.5.10`, que es la dirección IP del enrutador 1. Para activar el enrutamiento estático, deberá eliminar esta entrada. A continuación, debe verificar que el reenvío de paquetes y el enrutamiento estén activados para el host.

# routeadm	Configuration Option	Current Configuration	Current System State
	IPv4 routing	disabled	disabled
	IPv6 routing	disabled	disabled
	IPv4 forwarding	disabled	disabled
	IPv6 forwarding	disabled	disabled
	Routing services	"route:default ripng:default"	

Tanto el enrutamiento como el reenvío de paquetes están desactivados para `hosta`. Active el enrutamiento para completar la configuración del enrutamiento dinámico para `hosta`, del modo siguiente:

```
# svcadm enable route:default
```


Supervisión y modificación de los servicios de capa de transporte

Los protocolos de capa de transporte TCP, SCTP y UDP son parte del paquete Oracle Solaris estándar. Estos protocolos normalmente no requieren ninguna intervención para ejecutarse correctamente. Sin embargo, las circunstancias de su sitio podrían requerir el registro o la modificación de los servicios que ejecutan los protocolos de capa de transporte. En tal caso, debe modificar los perfiles de los servicios con la Utilidad de gestión de servicios (SMF), que se describe en el [Capítulo 18, “Gestión de servicios \(descripción general\)” de Guía de administración del sistema: administración básica](#).

El daemon `inetd` se encarga de iniciar los servicios estándar de Internet cuando se inicia un sistema. Estos servicios incluyen aplicaciones que utilizan TCP, SCTP o UDP como protocolo de capa de transporte. Puede modificar los servicios de Internet existentes o agregar servicios nuevos con los comandos SMF. Para más información sobre `inetd`, consulte [“Daemon de servicios de Internet inetd” en la página 244](#).

Las operaciones que requieren protocolos de capa de transporte incluyen:

- Registrar todas las conexiones TCP entrantes
- Agregar servicios que ejecutan un protocolo de capa de transporte, utilizando SCTP a modo de ejemplo
- Configurar la función de envoltorios TCP para el control de acceso

Para obtener información detallada sobre el daemon `inetd`, consulte la página del comando `man inetd(1M)`.

▼ Cómo registrar las direcciones IP de todas las conexiones TCP entrantes

- 1 En el sistema local, asuma la función de administrador de red o hágase superusuario.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 Active el seguimiento TCP para todos los servicios que administre `inetd`.

```
# inetadm -M tcp_trace=TRUE
```

▼ Cómo agregar servicios que utilicen el protocolo SCTP

El protocolo de transporte SCTP ofrece servicios a los protocolos de capa de modo similar a TCP. Sin embargo, SCTP permite la comunicación entre dos sistemas, que pueden ser (uno o ambos) de host múltiple. La conexión SCTP se denomina *asociación*. En una asociación, una aplicación divide los datos que se transmitirán en uno o más flujos de mensajes, o en *múltiples flujos*. Una conexión SCTP puede realizarse en los puntos finales con varias direcciones IP, lo cual es especialmente importante en las aplicaciones de telefonía. Las posibilidades que ofrece el host múltiple de SCTP constituyen una consideración de seguridad si el sitio utiliza filtro IP o IPsec. En la página del comando `man sctp(7P)` se describen algunas de estas consideraciones.

De modo predeterminado, SCTP se incluye en Oracle Solaris y no requiere ninguna configuración adicional. Sin embargo, es posible que tenga que configurar de modo explícito determinados servicios de capa de la aplicación para que utilicen SCTP. Algunas aplicaciones de ejemplo son `echo` y `discard`. El procedimiento siguiente muestra cómo agregar un servicio `echo` que utilice un socket de estilo uno a uno SCTP.

Nota – También puede utilizar el procedimiento siguiente para agregar servicios para los protocolos de capa de transporte TCP y UDP.

La tarea siguiente muestra cómo agregar un servicio SCTP `inet` que administre el daemon `inetd` al depósito SMF. La tarea muestra cómo utilizar los comandos de la Utilidad de gestión de servicios (SMF) para agregar el servicio.

- Para obtener información sobre los comandos de SMF, consulte [“Utilidades administrativas de la línea de comandos de la SMF” de Guía de administración del sistema: administración básica](#).
- Para obtener información sobre la sintaxis, consulte las páginas del comando `man` para los comandos SMF, como se describe en el procedimiento.
- Para obtener información detallada sobre SMF, consulte la página del comando `man smf(5)`.

Antes de empezar

Antes de llevar a cabo el procedimiento siguiente, cree un archivo manifest para el servicio. El procedimiento utiliza como ejemplo un archivo manifest para el servicio `echo` que se denomina `echo.sctp.xml`.

- 1 Inicie sesión en el sistema local con una cuenta de usuario con privilegios de escritura para los archivos del sistema.**
- 2 Edite el archivo `/etc/services` y agregue una definición para el nuevo servicio.**

Utilice la siguiente sintaxis para la definición del servicio.

`service-name` `[port/protocol]` `aliases`

3 Agregue el nuevo servicio.

Vaya al directorio en el que se encuentra el manifiesto del servicio y escriba lo siguiente:

```
# cd dir-name
# svccfg import service-manifest-name
```

Para ver la sintaxis completa de `svccfg`, consulte la página del comando `man svccfg(1M)`.

Supongamos que desea agregar un nuevo servicio SCTP echo utilizando el manifiesto `echo.sctp.xml` que se encuentra en el directorio `service.dir`. Debe escribir lo siguiente:

```
# cd service.dir
# svccfg import echo.sctp.xml
```

4 Compruebe que se haya agregado el manifiesto del servicio:

```
# svcs FMRI
```

Para el argumento *FMRI*, utilice el Fault Managed Resource Identifier (FMRI) del manifiesto del servicio. Por ejemplo, para el servicio SCTP echo, debe utilizar el comando siguiente:

```
# svcs svc:/network/echo:sctp_stream
```

El resultado que obtendrá será similar al siguiente:

```
STATE      STIME      FMRI
disabled   16:17:00   svc:/network/echo:sctp_stream
```

Si desea obtener información detallada sobre el comando `svcs`, consulte la página del comando `man svcs(1)`.

El resultado indica que el nuevo manifiesto del servicio está desactivado.

5 Enumere las propiedades del servicio para determinar si debe realizar modificaciones.

```
# inetadm -l FMRI
```

Para obtener información detallada sobre el comando `inetadm`, consulte la página del comando `man inetadm(1M)`.

Por ejemplo, para el servicio SCTP echo, debe escribir lo siguiente:

```
# inetadm -l svc:/network/echo:sctp_stream
SCOPE      NAME=VALUE
           name="echo"
           endpoint_type="stream"
           proto="sctp"
           isrpc=FALSE
           wait=FALSE
           exec="/usr/lib/inet/in.echod -s"
           .
           .
           default tcp_trace=FALSE
           default tcp_wrappers=FALSE
```

6 Active el nuevo servicio:

```
# inetadm -e FMRI
```

7 Compruebe que el servicio esté activado:

Por ejemplo, para el nuevo servicio echo, debe escribir:

```
# inetadm | grep sctp_stream
.
.
    enabled    online          svc:/network/echo:sctp_stream
```

Ejemplo 5-9 Cómo agregar un servicio que utilice el protocolo de transporte SCTP

El siguiente ejemplo muestra los comandos para utilizar las entradas de archivo necesarias para que el servicio echo utilice el protocolo de capa de transporte SCTP.

```
$ cat /etc/services
.
.
echo          7/tcp
echo          7/udp
echo          7/sctp

# cd service.dir

# svccfg import echo.sctp.xml

# svcs network/echo*
STATE          STIME          FMRI
disabled       15:46:44      svc:/network/echo:dgram
disabled       15:46:44      svc:/network/echo:stream
disabled       16:17:00      svc:/network/echo:sctp_stream

# inetadm -l svc:/network/echo:sctp_stream
SCOPE          NAME=VALUE
               name="echo"
               endpoint_type="stream"
               proto="sctp"
               isrpc=FALSE
               wait=FALSE
               exec="/usr/lib/inet/in.echod -s"
               user="root"
default bind_addr=""
default bind_fail_max=-1
default bind_fail_interval=-1
default max_con_rate=-1
default max_copies=-1
default con_rate_offline=-1
default failrate_cnt=40
default failrate_interval=60
default inherit_env=TRUE
default tcp_trace=FALSE
default tcp_wrappers=FALSE
```

```
# inetadm -e svc:/network/echo:sctp_stream

# inetadm | grep echo
disabled disabled      svc:/network/echo:stream
disabled disabled      svc:/network/echo:dgram
enabled  online          svc:/network/echo:sctp_stream
```

▼ Cómo utilizar los envoltorios TCP para controlar el acceso a los servicios TCP

El programa `tcpd` implementa *envoltorios TCP*. Los envoltorios TCP incorporan una medida de seguridad para los daemons de servicio como `ftpd` al permanecer entre el daemon y las solicitudes de servicio entrantes. Los envoltorios TCP registran los intentos de conexión correctos e incorrectos. Asimismo, los envoltorios TCP pueden proporcionar control de acceso, y permitir o denegar la conexión en función del lugar donde se origine la solicitud. Puede utilizar los envoltorios TCP para proteger los daemons como SSH, Telnet o FTP. La aplicación `sendmail` también puede utilizar envoltorios TCP, tal como se describe en [“Compatibilidad con envoltorios TCP de la versión 8.12 de sendmail” de Guía de administración del sistema: servicios de red](#).

1 En el sistema local, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Active los envoltorios TCP.

```
# inetadm -M tcp_wrappers=TRUE
```

3 Configure la directiva de control de acceso de los envoltorios TCP tal como se describe en la página del comando `man hosts_access(3)`.

Esta página del comando `man` se encuentra en el directorio `/usr/sfw/man` del CD-ROM de SFW, que se suministra con el CD-ROM de Oracle Solaris.

Administración de interfaces de red (tareas)

Este capítulo contiene tareas e información sobre las interfaces de red:

- “Administración de interfaces (mapa de tareas)” en la página 144
- “Aspectos básicos sobre la administración de interfaces físicas” en la página 145
- “Administración de interfaces de red individuales” en la página 146

Novedades en la administración de interfaces de red

La información de este capítulo describe la configuración de la interfaz a partir de la versión 10 1/06 de Solaris. Para ver una lista completa de las nuevas funciones de Oracle Solaris y una descripción de las versiones de Oracle Solaris, consulte [Novedades de Oracle Solaris 10 8/11](#).

En Solaris 10 1/06, se han introducido las novedades siguientes:

- El nuevo comando `dladm` para ver el estado de la interfaz se ha introducido en “[Cómo configurar una interfaz física tras la instalación del sistema](#)” en la página 148.
- Se ha ampliado la compatibilidad con VLAN a las interfaces GLDv3, tal como se explica en “[Administración de redes de área local virtuales](#)” en la página 154.
- Se ha incorporado la compatibilidad con vínculos en “[Descripción general de agregaciones de vínculos](#)” en la página 160.

En Solaris 10 7/07, `/etc/inet/ipnodes` pasa a estar obsoleto. Utilice `/etc/inet/ipnodes` únicamente para las versiones anteriores de Solaris 10, tal como se explica en los procedimientos individuales.

Administración de interfaces (mapa de tareas)

La tabla siguiente muestra diferentes tareas para configurar las interfaces de red, incluidas configuraciones especiales, como redes de área local virtuales y agregaciones de vínculos. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener instrucciones
Comprobar el estado de las interfaces en un sistema.	Enumera todas las interfaces del sistema y comprueba cuáles de ellas ya están sondeadas.	“Cómo obtener el estado de una interfaz” en la página 147
Agregar una sola interfaz tras la instalación del sistema.	Cambia un sistema a un enrutador o host múltiple configurando otra interfaz.	“Cómo configurar una interfaz física tras la instalación del sistema” en la página 148
SPARC: comprobar que la dirección MAC de una interfaz sea única.	Comprueba que la interfaz esté configurada con su dirección MAC de fábrica, en lugar de la dirección MAC del sistema (sólo SPARC).	“SPARC: Cómo asegurarse de que la dirección MAC de una interfaz sea única” en la página 152
Planificar una red de área local virtual (VLAN).	Lleva a cabo las tareas de planificación necesarias antes de crear una VLAN.	“Cómo planificar la configuración de una VLAN” en la página 157
Configurar una VLAN.	Crea y modifica VLAN en la red.	“Cómo configurar una VLAN” en la página 158
Planificar adiciones.	Diseña la adición y lleva a cabo las tareas de planificación necesarias para configurar las adiciones.	“Descripción general de agregaciones de vínculos” en la página 160
Configurar una adición.	Lleva a cabo las tareas relativas a la adición de vínculos.	“Cómo crear una agregación de vínculos” en la página 164
Planificar y configurar un grupo IPMP.	Configura los fallos y las recuperaciones tras los fallos para las interfaces que son miembro de un grupo IPMP.	“Cómo planificar un grupo IPMP” en la página 769 “Cómo configurar un grupo IPMP con múltiples interfaces” en la página 771

Aspectos básicos sobre la administración de interfaces físicas

Las *interfaces de red* proporcionan una conexión entre un sistema y una red. Un sistema basado en Oracle Solaris puede tener dos tipos de interfaces: física y lógica. Las *interfaces físicas* se componen de un controlador de software y un conector en el que puede conectar los medios de red, como un cable Ethernet. Las interfaces físicas se pueden agrupar para fines administrativos o de disponibilidad. Las *interfaces lógicas* se configuran en interfaces físicas existentes, normalmente para agregar direcciones y crear puntos finales de túnel en las interfaces físicas.

Nota – Las interfaces de redes lógicas se describen en las tareas en las que se utilizan: tareas IPv6, IPMP, DHCP y otras.

La mayoría de los sistemas informáticos tienen como mínimo una interfaz física que *incorpora* el fabricante en la placa del sistema principal. Algunos sistemas también pueden tener más de una interfaz integrada.

Además de las interfaces integradas, también puede agregar a un sistema interfaces que haya adquirido por separado. Una interfaz que se adquiere por separado se conoce como *tarjeta de interfaz de red* (NIC). Las tarjetas NIC se instalan de acuerdo con las instrucciones del fabricante.

Nota – Las NIC también se conocen como *adaptadores de red*.

Durante la instalación del sistema, el programa de instalación de Oracle Solaris detecta las interfaces que están instaladas físicamente y muestra el nombre de cada interfaz. Debe configurar como mínimo una interfaz desde la lista de interfaces. La primera interfaz que se configura durante la instalación se convierte en la *interfaz de red principal*. La dirección IP de la interfaz de red principal se asocia con el nombre de host configurado del sistema, que se guarda en el archivo `/etc/nodename`. No obstante, puede configurar interfaces adicionales durante la instalación o posteriormente.

Nombres de interfaz de red

Cada interfaz física se identifica mediante un nombre de dispositivo exclusivo. Los nombres de dispositivo tienen la siguiente sintaxis:

<driver-name><instance-number>

Los nombres de controladores de los sistemas Oracle Solaris pueden incluir `ce`, `hme`, `bge`, `e1000g` y muchos otros nombres de controladores. La variable *número_instancia* puede tener un valor de cero a *n*, en función de cuántas interfaces de ese tipo de controlador haya instaladas en el sistema.

Pongamos por ejemplo una interfaz 100BASE-TX Fast Ethernet, que se suele utilizar como interfaz de red principal en sistemas host y de servidor. Algunos nombres de controlador típicos para esta interfaz son `eri`, `qfe` y `hme`. Cuando se utiliza como interfaz de red principal, la interfaz de Fast Ethernet tiene un nombre de dispositivo como `eri0` o `qfe0`.

Las NIC como `eri` o `hme` sólo tienen una interfaz. Sin embargo, muchas marcas de NIC tienen varias interfaces. Por ejemplo, la tarjeta Quad Fast Ethernet (`qfe`) cuenta con cuatro interfaces, de la `qfe0` a la `qfe3`.

Conexión de una interfaz

Una interfaz debe *conectarse* para que pueda haber tráfico entre el sistema y la red. El proceso de conexión implica asociar una interfaz con un nombre de dispositivo. A continuación, se configuran los flujos para que el protocolo IP pueda utilizar la interfaz. Las interfaces físicas y las interfaces lógicas deben estar conectadas. Las interfaces se conectan como parte de la secuencia de inicio o explícitamente, con la sintaxis apropiada del comando `ifconfig`.

Al configurar una interfaz durante la instalación, dicha interfaz se conecta automáticamente. Si no desea configurar las interfaces adicionales del sistema durante la instalación, dichas interfaces no se conectan.

Tipos de interfaz de Oracle Solaris

A partir de Solaris 10 1/06, Oracle Solaris admite los dos tipos de interfaces siguientes:

- **Interfaces heredadas:** Estas interfaces son interfaces DLPI y GLDv2. Algunos tipos de interfaces heredadas son `eri`, `qfe` y `ce`. Al comprobar el estado de la interfaz con el comando `dladm show-link`, estas interfaces aparecen como heredadas.
- **Interfaces no VLAN:** Estas interfaces son interfaces GLDv3.

Nota – Actualmente se admite GLDv3 en los siguientes tipos de interfaces: `bge`, `xge` y `e1000g`.

Administración de interfaces de red individuales

Tras la instalación de Oracle Solaris, puede configurar o administrar interfaces en un sistema para las siguientes finalidades:

- Para actualizar el sistema y convertirlo en un host múltiple. Para más información, consulte [“Configuración de hosts múltiples” en la página 129](#).
- Para cambiar un host por un enrutador. Para obtener instrucciones sobre cómo configurar los enrutadores, consulte [“Configuración de un enrutador IPv4” en la página 121](#).

- Para configurar las interfaces como parte de una VLAN. Para más información, consulte [“Administración de redes de área local virtuales” en la página 154](#).
- Para configurar las interfaces como miembros de una adición. Para obtener más información, consulte [“Descripción general de agregaciones de vínculos” en la página 160](#).
- Para agregar una interfaz a un grupo IPMP. Para obtener instrucciones sobre cómo configurar un grupo IPMP, consulte [“Configuración de grupos IPMP” en la página 769](#).

Esta sección incluye información sobre cómo configurar interfaces de red individuales, a partir de Solaris 10 1/06. Consulte las secciones siguientes para obtener información sobre cómo configurar las interfaces de las siguientes agrupaciones:

- Para configurar las interfaces de una VLAN, consulte [“Administración de redes de área local virtuales” en la página 154](#).
- Para configurar las interfaces de una adición, consulte [“Descripción general de agregaciones de vínculos” en la página 160](#).
- Para configurar las interfaces como miembros de grupos IPMP, consulte [“Configuración de grupos IPMP” en la página 769](#).

▼ Cómo obtener el estado de una interfaz

A partir de Solaris 10 1/06, este procedimiento explica cómo determinar qué interfaces están disponibles en un sistema y su estado. Este procedimiento también muestra qué interfaces están conectadas. Si utiliza la versión anterior, Solaris 10 3/05, consulte [“Cómo obtener información sobre una interfaz específica” en la página 205](#).

- 1 En el sistema cuyas interfaces se deben configurar, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

- 2 Determine qué interfaces hay instaladas en el sistema.**

```
# dladm show-link
```

En este paso se utiliza el comando `dladm`, que se explica detalladamente en la página del comando `man dladm(1M)`. Este comando muestra todos los controladores de interfaces que encuentra, al margen de si las interfaces están configuradas.

- 3 Determine qué interfaces del sistema están conectadas.**

```
# ifconfig -a
```

El comando `ifconfig` cuenta con múltiples funciones adicionales, incluida la conexión de una interfaz. Para más información, consulte la página del comando `man ifconfig(1M)`.

Ejemplo 6-1 Cómo obtener el estado de una interfaz con el comando `dladm`

En el ejemplo siguiente se muestra el estado con el comando `dladm`.

```
# dladm show-link
ce0          type: legacy      mtu: 1500      device: ce0
ce1          type: legacy      mtu: 1500      device: ce1
bge0         type: non-vlan    mtu: 1500      device: bge0
bge1         type: non-vlan    mtu: 1500      device: bge1
bge2         type: non-vlan    mtu: 1500      device: bge2
```

El resultado de `dladm show-link` indica que hay disponibles cuatro controladores de interfaz para el host local. Pueden configurarse las interfaces `ce` y `bge` para las VLAN. Sin embargo, sólo se pueden utilizar las interfaces GLDV3 con el tipo `non-VLAN` para las adiciones de vínculos.

El ejemplo siguiente muestra la visualización del estado con el comando `ifconfig -a`.

```
# ifconfig -a
lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu
8232 index 1
    inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 3
    inet 192.168.84.253 netmask fffffff0 broadcast 192.168.84.255
    ether 0:3:ba:7:84:5e
bge0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,DHCP,IPv4>mtu 1500 index 2
    inet 10.8.57.39 netmask fffffff0 broadcast 10.8.57.255
    ether 0:3:ba:29:fc:cc
```

El resultado del comando `ifconfig -a` muestra las estadísticas sólo para dos interfaces, `ce0` y `bge0`. Este resultado muestra que sólo se han conectado `ce0` y `bge0` y están listos para ser utilizados en el tráfico de red. Estas interfaces se pueden utilizar en una VLAN. Dado que se ha conectado `bge0`, ya no puede utilizar esta interfaz en una adición.

▼ Cómo configurar una interfaz física tras la instalación del sistema

Antes de empezar

- Determine las direcciones IPv4 que desee utilizar para las interfaces adicionales.
- Asegúrese de que la interfaz física que se va a configurar esté instalada en el sistema. Para obtener información sobre cómo instalar hardware NIC que haya adquirido por separado, consulte las instrucciones del fabricante que se incluyen con la tarjeta NIC.
- Si acaba de instalar la interfaz, lleve a cabo un inicio de reconfiguración antes de continuar con la tarea siguiente.

- 1 **En el sistema cuyas interfaces se deben configurar, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Determine qué interfaces hay instaladas en el sistema.**

```
# dladm show-link
```

- 3 **Configure y sondee todos los comandos interfaz.**

```
# ifconfig interface plumb up
```

Por ejemplo, para `qfe0` escribiría:

```
# ifconfig qfe0 plumb up
```

Nota – Las interfaces que se configuran explícitamente con el comando `ifconfig` no persisten tras un reinicio.

- 4 **Asigne una dirección IPv4 y una máscara de red a la interfaz.**

```
# ifconfig interface IPv4-address netmask+netmask
```

Por ejemplo, para `qfe0` escribiría:

```
# ifconfig
qfe0 192.168.84.3 netmask + 255.255.255.0
```

Nota – Puede especificar una dirección IPv4 en la notación IPv4 tradicional o la notación CIDR.

- 5 **Compruebe que las interfaces que acaba de configurar estén sondeadas y configuradas, o "UP".**

```
# ifconfig
-a
```

Compruebe la línea de estado para cada interfaz que se muestre. Asegúrese de que el resultado contenga un indicador UP en la línea de estado, por ejemplo:

```
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 2
```

- 6 **(Opcional) Para que la configuración de la interfaz persista tras los reinicios, siga estos pasos:**

- a. **Cree un archivo `/etc/hostname.interface` para todas las interfaces que deba configurar.**

Por ejemplo, para agregar una interfaz `qfe0`, debe crear el siguiente archivo:

```
# vi /etc/hostname.qfe0
```

Nota – Si crea archivos alternativos de host para la misma interfaz, también deben seguir el formato de asignación de nombres `hostname.[0-9]*`, como, por ejemplo, `hostname.qfe0.a123`. Nombres como `hostname.qfe0.bak` o `hostname.qfe0.old` no son válidos y serán ignorados por las secuencias durante el inicio del sistema.

Tenga en cuenta también que sólo puede haber un archivo de nombre de host para una interfaz determinada. Si crea archivos alternativos de host para una interfaz con un nombre de archivo válido como, por ejemplo, `/etc/hostname.qfe` y `/etc/hostname.qfe.a123`, las secuencias de comandos de inicio intentarán la configuración mediante la referencia a los contenidos de ambos archivos de host, y se generarán errores. Para evitar esos errores, proporcione un nombre de archivo no válido para el sistema host que no desea utilizar en una configuración concreta.

b. Edite el archivo `/etc/hostname.interfaz`.

Como mínimo, agregue la dirección IPv4 de la interfaz al archivo. Puede utilizar la notación IPv4 tradicional o la notación CIDR para especificar la dirección IP de la interfaz. También puede agregar al archivo una máscara de red u otra información de configuración.

Nota – Para agregar una dirección IPv6 a una interfaz, consulte [“Modificación de la configuración de una interfaz de IPv6 para hosts y servidores” en la página 181](#)

c. Para 11/06 y las versiones anteriores de Oracle Solaris 10, agregue entradas para las nuevas interfaces en el archivo `/etc/inet/ipnodes`.

d. Agregue entradas para las nuevas interfaces en el archivo `/etc/inet/hosts`.

e. Efectúe un inicio de reconfiguración.

```
# reboot -- -r
```

f. Compruebe que la interfaz que ha creado en el archivo `/etc/hostname.interfaz` se haya configurado.

```
# ifconfig -a
```

Para ver un ejemplo, consulte el [Ejemplo 6-2](#).

Ejemplo 6-2 Cómo agregar configuraciones de interfaces persistentes

El ejemplo muestra cómo configurar las interfaces `qfe0` y `qfe1` en un host. Estas interfaces siguen siendo persistentes tras los reinicios.

```
# dladm show-link
eri0    type: legacy    mtu: 1500    device: eri0
qfe0    type: legacy    mtu: 1500    device: qfe0
```

```

qfe1    type: legacy    mtu: 1500    device: qfe1
qfe2    type: legacy    mtu: 1500    device: qfe2
qfe3    type: legacy    mtu: 1500    device: qfe3
bge0    type: non-vlan  mtu: 1500    device: bge0
# vi /etc/hostname.qfe0
192.168.84.3 netmask 255.255.255.0
# vi /etc/hostname.qfe1
192.168.84.72 netmask 255.255.255.0
# vi /etc/inet/hosts
# Internet host table
#
127.0.0.1        localhost
10.0.0.14        myhost
192.168.84.3     interface-2
192.168.84.72    interface-3
For Solaris 10 11/06 and earlier releases:# vi /etc/inet/ipnodes
10.0.0.14 myhost
192.168.84.3     interface-2
192.168.84.72    interface-3

```

En este punto, debe reiniciar el sistema.

```
# reboot -- -r
```

Cuando se inicie el sistema, verifique la configuración de la interfaz.

```

ifconfig -a
# ifconfig -a lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu
8232 index 1
    inet 127.0.0.1 netmask ff000000
eri0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.14netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:c1:8b:c3
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 192.168.84.3 netmask fffffff0 broadcast 192.255.255.255
    ether 8:0:20:c8:f4:1d
qfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 4
    inet 192.168.84.72 netmask fffffff0 broadcast 10.255.255.255
    ether 8:0:20:c8:f4:1e

```

- Véase también**
- Para configurar una dirección IPv6 en una interfaz, consulte [“Cómo habilitar una interfaz de IPv6 para la sesión actual” en la página 172](#).
 - Para configurar la detección de fallos y la recuperación tras un fallo para las interfaces utilizando las rutas múltiples de redes IP (IPMP), consulte el [Capítulo 31, “Administración de IPMP \(tareass\)”](#).

▼ Cómo eliminar una interfaz física

- 1 **En el sistema cuya interfaz debe eliminar, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica.](#)

- 2 **Elimine la interfaz física.**

```
# ifconfig interface down unplumb
```

Por ejemplo, para eliminar la interfaz qfe1, debe escribir:

```
# ifconfig qfe1 down unplumb
```

▼ SPARC: Cómo asegurarse de que la dirección MAC de una interfaz sea única

Siga este procedimiento para configurar direcciones MAC.

Algunas aplicaciones requieren que cada interfaz esté en un host para tener una dirección MAC exclusiva. Sin embargo, cada sistema basado en SPARC tiene una dirección MAC para todo el sistema, que utilizan todas las interfaces de modo predeterminado. A continuación se exponen dos situaciones en las que se podría configurar las direcciones MAC instaladas de fábrica para las interfaces en un sistema SPARC.

- Para las adiciones de vínculos, debe utilizar las direcciones MAC de fábrica de las interfaces en la configuración de la adición.
- Para los grupos IPMP, cada interfaz del grupo debe tener una dirección MAC exclusiva. Estas interfaces deben utilizar sus direcciones MAC de fábrica.

El parámetro EEPROM `local-mac-address?` determina si todas las interfaces del sistema SPARC utilizan la dirección MAC de todo el sistema o una dirección MAC exclusiva. El siguiente procedimiento muestra cómo utilizar el comando `eeprom` para comprobar el valor actual de `local-mac-address?` y cambiarlo, si es preciso.

- 1 **En el sistema cuyas interfaces se deben configurar, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica.](#)

2 Determine si todas las interfaces del sistema utilizan la dirección MAC del sistema.

```
# eeprom local-mac-address?
local-mac-address?=false
```

En el ejemplo, la respuesta al comando `eeprom, local-mac-address?=false`, indica que todas las interfaces utilizan la dirección MAC del sistema. El valor de `local-mac-address?=false` debe cambiarse a `local-mac-address?=true` para que las interfaces puedan pasar a ser miembros de un grupo IPMP. También debe cambiar `local-mac-address?=false` a `local-mac-address?=true` para las adiciones.

3 Si es preciso, cambie el valor de `local-mac-address?`, tal como se indica:

```
# eeprom local-mac-address?=true
```

Al reiniciar el sistema, las interfaces con las direcciones MAC de fábrica ahora utilizan esta configuración de fábrica, en lugar de la dirección MAC de todo el sistema. Las interfaces sin las direcciones MAC de fábrica siguen utilizando la dirección MAC de todo el sistema.

4 Compruebe las direcciones MAC de todas las interfaces del sistema.

Busque los casos en que varias interfaces tengan la misma dirección MAC. En este ejemplo, todas las interfaces utilizan la dirección MAC de todo el sistema, `8:0:20:0:0:1`.

```
ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ffffffff
hme0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.112 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:0:0:1
ce0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.114 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:0:0:1
ce1: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.118 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:0:0:1
```

Nota – Continúe con el paso siguiente sólo si hay más de una interfaz de red con la misma dirección MAC. De lo contrario, vaya al último paso.

5 Si es preciso, configure manualmente las interfaces restantes para que todas tengan direcciones MAC exclusivas.

Especifique una dirección MAC exclusiva en el archivo `/etc/hostname.interfaz` para la interfaz concreta.

En el ejemplo del paso anterior, debe configurar `ce0` y `ce1` con direcciones MAC administradas localmente. Por ejemplo, para volver a configurar `ce1` con la dirección MAC administrada localmente `06:05:04:03:02`, debe agregar la línea siguiente a `/etc/hostname.ce1`:

```
ether 06:05:04:03:02
```

Nota – Para evitar la posibilidad de que una dirección MAC configurada manualmente entre en conflicto con otras direcciones MAC de la red, siempre debe configurar las direcciones MAC *administradas localmente*, tal como define el estándar IEEE 802.3.

También puede utilizar el comando `ifconfig ether` para configurar la dirección MAC de una interfaz para la sesión actual. Sin embargo, los cambios que efectúe directamente con `ifconfig` no se conservarán tras los reinicios. Consulte la página del comando `man ifconfig(1M)` para obtener más información.

6 Reinicie el sistema.

Administración de redes de área local virtuales

Una *red de área local virtual (VLAN)* es una subdivisión de una red de área local en la capa de vínculo de datos de la pila de protocolo TCP/IP. Puede crear redes VLAN para redes de área local que utilicen tecnología de nodo. Al asignar los grupos de usuarios en redes VLAN, puede mejorar la administración de red y la seguridad de toda la red local. También puede asignar interfaces del mismo sistema a redes VLAN diferentes.

Es recomendable dividir una red de área local en redes VLAN si necesita lo siguiente:

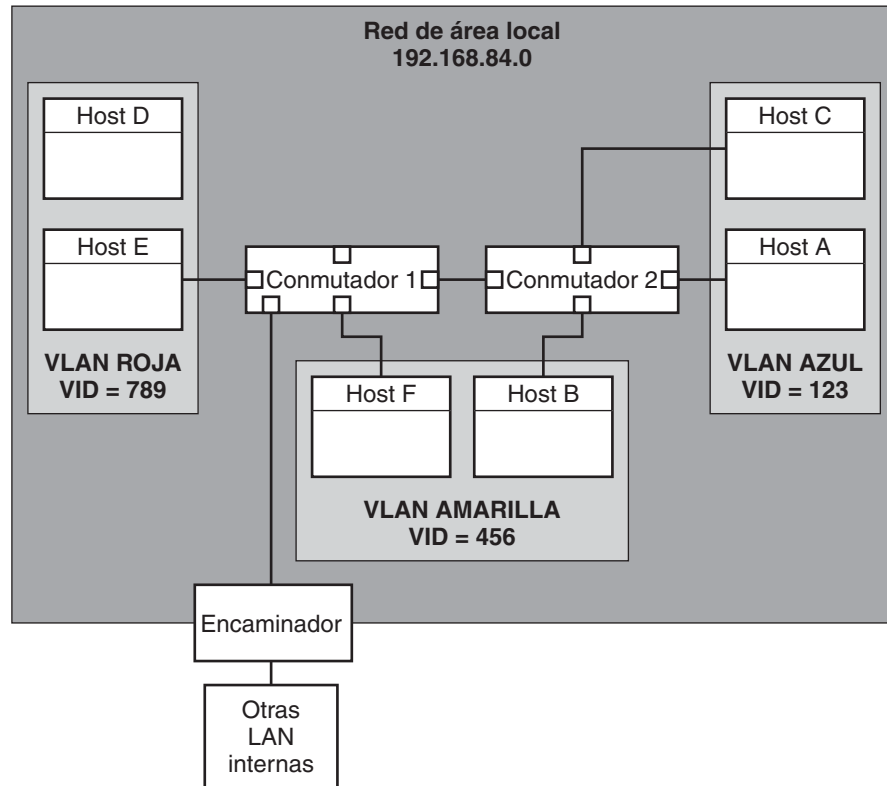
- Cree una división lógica de grupos de trabajo.
Por ejemplo, suponga que todos los hosts de la planta de un edificio están conectados mediante una red de área local con nodos. Puede crear una VLAN para cada grupo de trabajo de la planta.
- Diseñe diferentes directivas de seguridad para los grupos de trabajo.
Por ejemplo, las necesidades de seguridad del departamento de finanzas y el de informática son muy diferentes. Si los sistemas de ambos departamentos comparten la misma red local, puede crear una red VLAN independiente para cada departamento. Después, puede asignar la directiva de seguridad apropiada para cada VLAN.
- Divida los grupos de trabajo en dominios de emisión administrables.
El uso de redes VLAN reduce el tamaño de los dominios de emisión y mejora la efectividad de la red.

Descripción general de una configuración VLAN

La tecnología de red LAN con nodos permite organizar los sistemas de una red local en redes VLAN. Para poder dividir una red de área local en redes VLAN, debe tener nodos compatibles con la tecnología VLAN. Puede configurar todos los puertos de un nodo para que transfieran datos para una única VLAN o para varias VLAN, según el diseño de configuración VLAN. Cada fabricante utiliza procedimientos diferentes para configurar los puertos de un nodo.

En la figura siguiente se muestra una red de área local con la dirección de subred 192 . 168 . 84 . 0. Esta red LAN está subdividida en tres redes VLAN, Roja, Amarilla y Azul.

FIGURA 6-1 Red de área local con tres redes VLAN



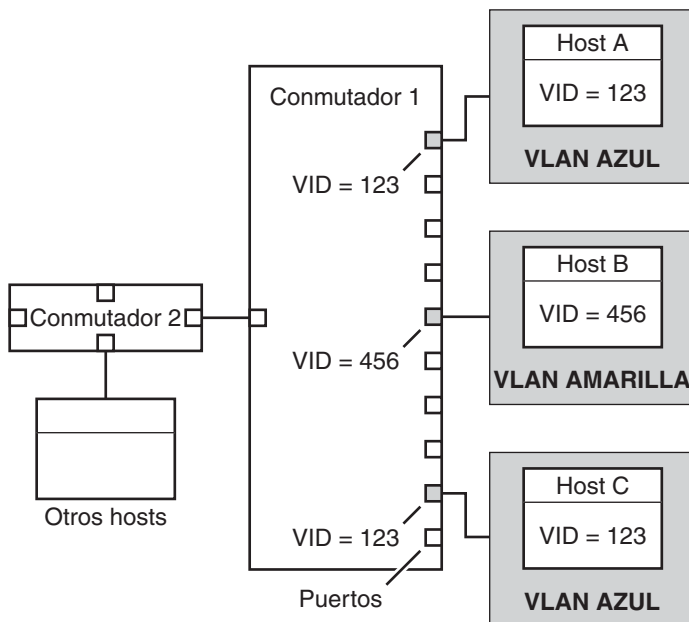
Los conmutadores 1 y 2 se encargan de la conexión a la red LAN 192 . 168 . 84 . 0. La red VLAN contiene sistemas del grupo de trabajo Contabilidad. Los sistemas del grupo de trabajo Recursos humanos se encuentran en la red VLAN Amarilla. Los sistemas del grupo de trabajo Tecnologías de la información se asignan a la VLAN Azul.

Etiquetas VLAN y puntos de conexión físicos

Cada VLAN de una red de área local está identificada por una etiqueta VLAN, o *ID VLAN* (VID). El VID se asigna durante la configuración de la red VLAN. El VID es un identificador de 12 bits entre 1 y 4094 que proporciona una identidad única para cada VLAN. En la [Figura 6-1](#), la VLAN Roja tiene el VID 789, la VLAN Amarilla tiene el VID 456 y la VLAN Azul tiene el VID 123.

Al configurar los nodos para que admitan redes VLAN, es necesario asignar un VID a cada puerto. El VID del puerto debe ser el mismo que el VID asignado a la interfaz que se conecta al puerto, como se muestra en la siguiente figura.

FIGURA 6-2 Configuración de nodos de una red con redes VLAN



La Figura 6-2 muestra varios hosts que están conectados a diferentes VLAN. Hay dos hosts que pertenecen a la misma VLAN. En esta figura, las interfaces de red primaria de los tres hosts se conectan al conmutador 1. El host A es miembro de la red VLAN Azul. Por lo tanto, la interfaz del host A está configurada con el VID 123. Esta interfaz se conecta al puerto 1 en el conmutador 1, que se configura con el VID 123. El host B es miembro de la red VLAN Amarilla con el VID 456. La interfaz del host B se conecta al puerto 5 en el conmutador 1, que se configura con el VID 456. Por último, la interfaz del host C se conecta al puerto 9 en el conmutador 1. La red VLAN Azul se configura con el VID 123.

La figura también muestra que un único host puede también pertenecer a más de una VLAN. Por ejemplo, Host A tiene dos VLAN configuradas a través de la interfaz del host. La segunda VLAN está configurada con el VID 456 y se conecta al puerto 3 que también está configurado con el VID 456. Por lo tanto, el Host A es miembro del Blue VLAN y del Yellow VLAN.

Durante la configuración de la red VLAN, debe especificar el *punto de conexión físico* o PPA de la red VLAN. El valor PPA se obtiene con esta fórmula:

$$\text{driver-name} + \text{VID} * 1000 + \text{device-instance}$$

El número de *instancia de dispositivo* debe ser menor que 1000.

Por ejemplo, para configurar una interfaz ce1 como parte de la red VLAN 456, se crearía el siguiente PPA:

```
ce + 456 * 1000 + 1= ce456001
```

Planificación de una red para redes VLAN

Utilice el procedimiento siguiente para planificar las VLAN de la red.

▼ Cómo planificar la configuración de una VLAN

- 1 **Examine la distribución de red local y determine dónde es apropiado realizar las subdivisiones en redes VLAN.**

Para ver un ejemplo básico de esta topología, consulte la [Figura 6-1](#).

- 2 **Cree un esquema numerado para los VID y asigne un VID a cada VLAN.**

Nota – Puede que ya haya un esquema numerado de VLAN en la red. En tal caso, deberá crear los VID dentro del esquema numerado de VLAN.

- 3 **En cada sistema, determine las interfaces que deben ser miembros de una VLAN determinada.**

- a. **Determine las interfaces que se configuran en un sistema.**

```
# dladm show-link
```

- b. **Identifique qué VID debe asociarse con cada vínculo de datos del sistema.**

- c. **Cree puntos PPA para cada interfaz que vaya a configurarse con una VLAN.**

No es necesario configurar todas las interfaces de un sistema en la misma red VLAN.

- 4 **Compruebe las conexiones de las interfaces con los nodos de red.**

Anote el VID de cada interfaz y el puerto de nodo al que están conectadas.

- 5 **Configure cada puerto del nodo con el mismo VID de la interfaz al que está conectado.**

Consulte la documentación del fabricante del nodo para ver las instrucciones de configuración.

Configuración de redes VLAN

Ahora Oracle Solaris admite redes de área local virtuales en los siguientes tipos de interfaz:

- ce
- bge
- xge
- e1000g

De los tipos de interfaces antiguas, sólo la interfaz ce puede hacerse miembro de una red VLAN. Puede configurar interfaces de diferentes tipos en la misma red VLAN.

Nota – Puede configurar varias redes VLAN en un grupo IPMP. Para obtener más información sobre los grupos IPMP, consulte [“Configuraciones de interfaces IPMP” en la página 757](#).

▼ Cómo configurar una VLAN

1 Asuma el rol de administrador principal, o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Determine los tipos de interfaces que se utilizan en el sistema.

```
# dladm show-link
```

El resultado muestra los tipos de interfaz disponibles:

ce0	type: legacy	mtu: 1500	device: ce0
ce1	type: legacy	mtu: 1500	device: ce1
bge0	type: non-vlan	mtu: 1500	device: bge0
bge1	type: non-vlan	mtu: 1500	device: bge1
bge2	type: non-vlan	mtu: 1500	device: bge2

3 Configure una interfaz como parte de una red VLAN.

```
# ifconfig interface-PPA plumb IP-address up
```

Por ejemplo, para configurar la interfaz ce1 con una nueva dirección IP 10.0.0.2 en una red VLAN con el VID 123, se utilizaría el siguiente comando:

```
# ifconfig ce123001 plumb 10.0.0.2  
up
```

Nota – Puede asignar direcciones IPv4 e IPv6 a VLAN, como sucede con otras interfaces.

- 4 (Optativo) Para que la configuración VLAN persista cuando se reinicia, cree un archivo `hostname.PPA` de interfaz para cada interfaz configurada como parte de una VLAN.

```
# cat hostname.interface-PPA
IPv4-address
```
- 5 En el nodo, configure las etiquetas y los puertos VLAN para que se correspondan con las redes VLAN configuradas en el sistema.

Ejemplo 6-3 Configuración de una VLAN

En este ejemplo se muestra cómo configurar los dispositivos bge1 y bge2 en una VLAN con el VID 123.

```
# dladm show-link
ce0          type: legacy      mtu: 1500      device: ce0
ce1          type: legacy      mtu: 1500      device: ce1
bge0        type: non-vlan    mtu: 1500      device: bge0
bge1        type: non-vlan    mtu: 1500      device: bge1
bge2        type: non-vlan    mtu: 1500      device: bge2
# ifconfig bge123001 plumb 10.0.0.1 up
# ifconfig bge123002 plumb 10.0.0.2 up
# cat hostname.bge123001 10.0.0.1
# cat hostname.bge123002 10.0.0.2
# ifconfig -a
lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
bge123001: flags=201000803<UP,BROADCAST,MULTICAST,IPv4,CoS> mtu 1500 index 2
    inet 10.0.0.1 netmask ff000000 broadcast 10.255.255.255
    ether 0:3:ba:7:84:5e
bge123002: flags=201000803 <UP,BROADCAST,MULTICAST,IPv4,CoS> mtu 1500 index 3
    inet 10.0.0.2 netmask ff000000 broadcast 10.255.255.255
    ether 0:3:ba:7:84:5e
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 4
    inet 192.168.84.253 netmask ffffffff broadcast 192.168.84.255
    ether 0:3:ba:7:84:5e
# dladm show-link
ce0          type: legacy      mtu: 1500      device: ce0
ce1          type: legacy      mtu: 1500      device: ce1
bge0        type: non-vlan    mtu: 1500      device: bge0
bge1        type: non-vlan    mtu: 1500      device: bge1
bge2        type: non-vlan    mtu: 1500      device: bge2
bge123001    type: vlan 123    mtu: 1500      device: bge1
bge123002    type: vlan 123    mtu: 1500      device: bge2
```

Descripción general de agregaciones de vínculos

Nota – La versión original de Oracle Solaris 10 y las versiones anteriores de Oracle Solaris 10 no admiten agregaciones de vínculos. Para crear agregaciones de vínculos para estas versiones antiguas de Oracle Solaris, utilice Sun Trunking, como se describe en *Sun Trunking 1.3 Installation and Users Guide*.

Oracle Solaris admite la organización de interfaces de red en agregaciones de vínculos. Una *agregación de vínculos* consiste en varias interfaces de un sistema que se configuran juntas como una unidad lógica única. Las agregaciones de vínculos, también denominadas *truncaciones*, se definen en [IEEE 802.3ad Link Aggregation Standard \(http://www.ieee802.org/3/index.html\)](http://www.ieee802.org/3/index.html).

El estándar IEEE 802.3ad Link Aggregation proporciona un método para combinar la capacidad de varios vínculos Ethernet duplex en un único vínculo lógico. Este grupo de agregación de vínculos se trata como si fuera un único vínculo.

A continuación se enumeran las funciones de agregaciones de vínculos:

- **Ancho de banda ampliado** – La capacidad de varios vínculos se combina en un vínculo lógico.
- **Recuperación de fallos automática** – El tráfico de un vínculo que ha fallado se transfiere a vínculos activos de la agregación.
- **Equilibrio de carga** – El tráfico entrante y saliente se distribuye de acuerdo con directivas de equilibrio de carga definidas por el usuario, como las direcciones MAC e IP de origen y destino.
- **Admisión de duplicación** – Dos sistemas pueden configurarse con agregaciones paralelas.
- **Administración mejorada** – Todas las interfaces se administran como una única unidad.
- **Menos drenaje en la agrupación de direcciones de red** – Puede asignarse una dirección IP a la agregación completa.

Conceptos básicos de agregaciones de vínculos

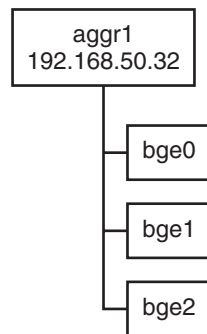
La topología básica de agregación de vínculos consta de una única agregación compuesta por un conjunto de interfaces físicas. Puede usar la agregación de vínculos básica en las siguiente situaciones:

- En sistemas con una aplicación con un gran volumen de tráfico distribuido, puede dedicar una agregación al tráfico de dicha aplicación.
- Para ubicaciones con espacio de direcciones IP limitado pero que requieren una gran cantidad de ancho de banda, sólo se necesita una dirección IP para una gran agregación de interfaces.

- Para ubicaciones que necesitan ocultar la existencia de interfaces internas, la dirección IP de la agregación oculta las interfaces a aplicaciones externas.

La [Figura 6–3](#) muestra una agregación de un servidor que aloja un sitio web muy visitado. Este sitio requiere un gran ancho de banda para el tráfico de peticiones entre los clientes en Internet y el servidor de base de datos del sitio. Por cuestiones de seguridad, la existencia de interfaces individuales en el servidor debe ocultarse a las aplicaciones externas. La solución es la agregación `aggr1` con la dirección IP `192.168.50.32`. Esta adición se compone de tres interfaces, de `bge0` a `bge2`. Estas interfaces se dedican a enviar el tráfico de respuesta a las peticiones de los clientes. La dirección saliente del tráfico de paquetes de todas las interfaces es la dirección IP de `aggr1`, `192.168.50.32`.

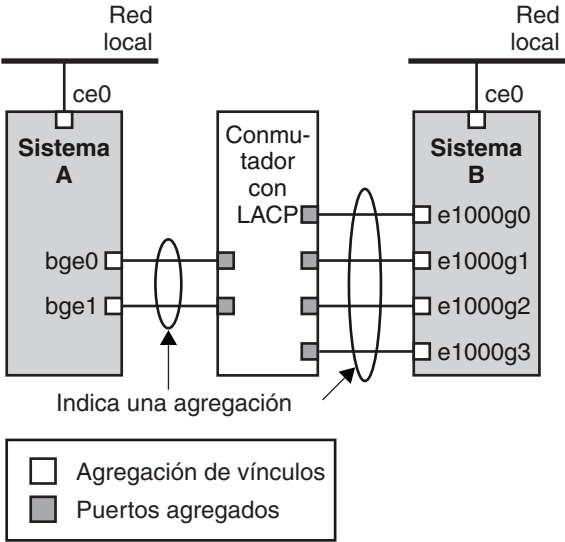
FIGURA 6–3 Configuración de agregación de vínculos básica



La [Figura 6–4](#) representa una red local con dos sistemas, cada uno con una agregación configurada. Los dos sistemas están conectados mediante un nodo (concentrador). Si necesita ejecutar una agregación a través de un nodo, el nodo debe admitir la tecnología de agregaciones. Este tipo de configuración resulta especialmente útil para sistemas de alta disponibilidad y con duplicación.

En la figura, el Sistema A tiene una agregación que consta de dos interfaces, `bge0` y `bge1`. Estas interfaces están conectadas al nodo mediante puertos agregados. El Sistema B tiene una agregación de cuatro interfaces, de `e1000g0` a `e1000g3`. Estas interfaces también están conectadas mediante puertos agregados del nodo.

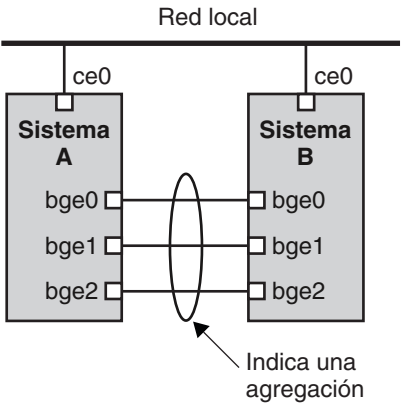
FIGURA 6-4 Configuración de agregación vínculos con nodo



Agregaciones de vínculos de extremo a extremo

La configuración de agregación de vínculos de extremo a extremo consta de dos sistemas independientes conectados directamente el uno al otro, como se muestra en la siguiente figura. Los sistemas ejecutan agregaciones paralelas.

FIGURA 6-5 Configuración de agregación de extremo a extremo básica



En esta figura, el dispositivo `bge0` del Sistema A está vinculado directamente a `bge0` en el Sistema B, etc. De este modo, los sistemas A y B permiten duplicación y alta disponibilidad, así

como comunicaciones a alta velocidad entre ambos sistemas. Cada sistema también tiene la interfaz `ce0` configurada para el flujo de tráfico de la red local.

La aplicación más común para agregaciones de vínculo de extremo a extremo son los servidores de base de datos reflejados. Ambos servidores deben actualizarse a la vez y, por lo tanto, necesitan bastante ancho de banda, flujo de tráfico de alta velocidad y fiabilidad. El uso más habitual de las agregaciones de vínculos de extremo a extremo es en los centros de datos.

Directivas y equilibrio de la carga

Si planea utilizar una agregación de vínculos, es recomendable definir una directiva para el tráfico saliente. Esta directiva puede especificar cómo deben distribuirse los paquetes entre los vínculos disponibles de una agregación y, por lo tanto, establece el equilibrio de la carga. A continuación se enumeran los posibles especificadores de capa y su efecto en la directiva de agregación:

- **L2:** determina el vínculo de salida numerando el encabezado MAC (L2) de cada paquete
- **L3:** determina el vínculo de salida numerando el encabezado IP (L3) de cada paquete
- **L4:** determina el vínculo de salida numerando el encabezado TCP, UDP u otro ULP (L4) de cada paquete

También es válida cualquier combinación de estas directivas. La directiva predeterminada es L4. Si necesita más información, consulte la página de comando `man dladm(1M)`.

Modo de agregación y nodos

Si su configuración de agregación requiere conexión a través de un nodo, el nodo debe admitir el *protocolo de control de agregación de vínculos (LACP)*. Si el nodo admite LACP, debe configurar LACP para el nodo y la agregación. Sin embargo, puede definir uno de los siguientes *modos* de funcionamiento de LACP:

- **Modo inactivo:** el modo predeterminado para agregaciones. Los paquetes LACP, llamados *LACPDU* no se generan.
- **Modo activo:** el sistema genera paquetes LACPDU en intervalos regulares, que puede especificar el usuario.
- **Modo pasivo:** el sistema genera un LACPDU sólo cuando recibe un LACPDU del nodo. Si la agregación y el nodo están configurados en modo pasivo, no pueden intercambiar paquetes LACPDU.

Si necesita información sobre sintaxis, consulte la página de comando `man dladm(1M)` y la documentación del fabricante del nodo.

Requisitos para agregaciones de vínculos

La configuración de agregación de vínculos tiene los siguientes requisitos:

- Debe usar el comando `dladm` para configurar agregaciones.
- Una interfaz sondeada no puede ser miembro de una agregación.
- Las interfaces deben ser del tipo GLDV3: `xge`, `e1000g` y `bge`.
- Todas las interfaces de la agregación deben ejecutarse a la misma velocidad y en modo duplex total.
- Debe definir el valor de direcciones MAC en “true” en el parámetro EEPROM `local-mac-address?` Si necesita instrucciones, consulte [Cómo asegurarse de que la dirección MAC de una interfaz sea única](#).

▼ Cómo crear una agregación de vínculos

Antes de empezar

Nota – Una agregación de vínculos sólo funciona en vínculos de punto a punto duplex total y con velocidad idéntica. Asegúrese de que las interfaces de su agregación cumplen este requisito.

Si utiliza un nodo en su configuración de agregación, asegúrese de hacer lo siguiente:

- Configure los puertos del nodo para que se utilicen como una agregación
- Si el nodo admite LACP, configure LACP en modo activo o pasivo

1 Asuma el rol de administrador principal, o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Determine qué interfaces hay instaladas en el sistema.

```
# dladm show-link
```

3 Determine qué interfaces se han sondeado.

```
# ifconfig -a
```

4 Cree una agregación.

```
# dladm create-aggr -d interface -d interface [...]key
```

interfaz Representa el nombre de dispositivo de la interfaz que pasará a formar parte de la agregación.

clave Es el número que identifica la agregación. El número de clave menor es 1. Los ceros no se pueden utilizar como claves.

Por ejemplo:

```
# dladm create-aggr -d bge0 -d bge1 1
```

5 Configure y sondee la agregación creada.

```
# ifconfig aggrkey plumb IP-address up
```

Por ejemplo:

```
# ifconfig aggr1 plumb 192.168.84.14 up
```

6 Compruebe el estado de la agregación que acaba de crear.

```
# dladm show-aggr
```

Recibirá el siguiente resultado:

```
key: 1 (0x0001) policy: L4      address: 0:3:ba:7:84:5e (auto)
device  address      speed      duplex link  state
bge0    0:3:ba:7:b5:a7  1000 Mbps   full   up    attached
bge1    0:3:ba:8:22:3b   0 Mbps    unknown down  standby
```

El resultado muestra que se ha creado una agregación con la clave 1 y la directiva L4.

7 (Optativo) Haga que la configuración IP de la agregación de vínculos persista al reiniciar.

a. Para realizar agregaciones de vínculos con direcciones IPv4, cree un archivo `/etc/hostname.aggrclave`. Para realizar agregaciones de vínculos basadas en IPv6, cree un archivo `/etc/hostname6.aggr.clave`.

b. Escriba la dirección IPv4 o IPv6 de la agregación de vínculos en el archivo.

Por ejemplo, para la agregación creada en este procedimiento, se crearía el siguiente archivo:

```
# vi /etc/hostname.aggr1
192.168.84.14
```

c. Efectúe un inicio de reconfiguración.

```
# reboot -- -r
```

d. Verifique que la configuración de agregación de vínculos especificada en el archivo `/etc/hostname.aggrclave` se ha configurado.

```
# ifconfig -a
.
.
aggr1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 192.168.84.14 netmask ff000000 broadcast 192.255.255.
```

Ejemplo 6-4 Creación de una agregación de vínculos

Este ejemplo muestra los comandos que se utilizan para crear una agregación de vínculos con dos dispositivos, bge0 y bge1, y el resultado.

```
# dladm show-link
ce0          type: legacy      mtu: 1500      device: ce0
ce1          type: legacy      mtu: 1500      device: ce1
bge0         type: non-vlan    mtu: 1500      device: bge0
bge1         type: non-vlan    mtu: 1500      device: bge1
bge2         type: non-vlan    mtu: 1500      device: bge2

# ifconfig -a
lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.84.253 netmask ffffffff00 broadcast 192.168.84.255
    ether 0:3:ba:7:84:5e

# dladm create-aggr -d bge0 -d bge1 1
# ifconfig aggr1 plumb 192.168.84.14 up
# dladm show-aggr
key: 1 (0x0001) policy: L4      address: 0:3:ba:7:84:5e (auto)
device  address      speed      duplex link      state
bge0    0:3:ba:7:b5:a7  1000      Mbps      full   up      attached
bge1    0:3:ba:8:22:3b   0         Mbps      unknown down  standby

# ifconfig -a
lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.84.253 netmask ffffffff00 broadcast 192.168.84.255
    ether 0:3:ba:7:84:5e
aggr1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 192.168.84.14 netmask ff000000 broadcast 192.255.255.255
    ether 0:3:ba:7:84:5e
```

Como puede comprobar, las dos interfaces usadas para la agregación se habían sondeado previamente con ifconfig.

▼ Cómo modificar una agregación

Este procedimiento muestra cómo realizar los siguientes cambios en una definición de agregación:

- Modificar la directiva de la agregación
- Cambiar el modo de la agregación

1 Asuma el rol de administrador principal, o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Modifique la agregación para cambiar la directiva.

```
# dladm modify-aggr -P policy key
```

directiva Representa una o varias de las directivas L2, L3 y L4, como se explica en [“Directivas y equilibrio de la carga” en la página 163](#).

clave Es un número que identifica la agregación. El número de clave menor es 1. Los ceros no se pueden utilizar como claves.

3 Si protocolo de control de agregación de vínculos (LACP) se está ejecutando en el conmutador al que están conectados los dispositivos de la agregación, modifique la agregación de modo que admita LACP.

Si el nodo utiliza LACP en modo pasivo, asegúrese de configurar el modo activo para la agregación.

```
# dladm modify-aggr -l LACP mode -t timer-value key
```

-l modo LACP Indica el modo LACP de la agregación. Los valores son active, passive y off.

-t valor de tiempo Indica el valor de tiempo LACP, short o long.

clave Es un número que identifica la agregación. El número de clave menor es 1. Los ceros no se pueden utilizar como claves.

Ejemplo 6–5 Modificación de una agregación de vínculos

Este ejemplo muestra cómo modificar la directiva de adición aggr1 a L2 y, a continuación, activar el modo LACP activo.

```
# dladm modify-aggr -P L2 1
# dladm modify-aggr -l active -t short 1
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device  address      speed      duplex  link    state
bge0    0:3:ba:7:b5:a7    1000      Mbps    full   up      attached
bge1    0:3:ba:8:22:3b    0         Mbps    unknown down    standby
```

▼ Cómo eliminar una interfaz de una agregación**1 Asuma el rol de administrador principal, o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Elimine una interfaz de la agregación.

```
# dladm remove-aggr -d interface
```

Ejemplo 6–6 Eliminar interfaces de una agregación

Este ejemplo muestra cómo eliminar las interfaces de la agregación `aggr1`.

```
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device address      speed      duplex link      state
bge0    0:3:ba:7:b5:a7 1000  Mbps    full  up      attached
bge1    0:3:ba:8:22:3b  0     Mbps    unknown down  standby
# dladm remove-aggr -d bge1 1
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device address      speed      duplex link      state
bge0    0:3:ba:7:b5:a7 1000  Mbps    full  up      attached
```

▼ Cómo eliminar una agregación

1 Asuma el rol de administrador principal, o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tarefas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Elimine la agregación.

```
# dladm delete-aggr key
```

clave Es un número que identifica la agregación. El número de clave menor es 1. Los ceros no se pueden utilizar como claves.

Ejemplo 6–7 Cómo eliminar una agregación

Este ejemplo muestra cómo eliminar la agregación `aggr1`.

```
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device address      speed      duplex link      state
# dladm delete-aggr -d 1
```


▼ Cómo configurar VLAN a través de una adición de vínculos

Del mismo modo en que se configura VLAN a través de una interfaz, también se pueden crear VLAN en una adición de vínculos. Puede ver descripciones de VLAN en [“Administración de redes de área local virtuales” en la página 154](#). En esta sección se combina la configuración de VLAN y las adiciones de vínculos.

Antes de empezar

Configure en primer lugar la adición de vínculos con una dirección IP válida. Tenga en cuenta el valor de la `clave` de la adición que necesitará cuando se cree el VLAN a través de la adición. Para crear adiciones de vínculos, consulte [“Cómo crear una agregación de vínculos” en la página 164](#).

- 1 Si ya se ha creado una adición de vínculo, obtenga la clave de dicha adición.

```
# dladm show-aggr
```

- 2 Cree el VLAN a través de la adición de vínculos.

```
# ifconfig aggrVIDkey plumb
```

donde

VID El ID de la VLAN

clave La tecla de la adición de vínculos a través de la cual se ha creado el VLAN. La tecla debe tener un formato de 3 dígitos. Por ejemplo, si la tecla de adición es 1, el número de tecla que se incluye en el nombre de la VLAN es 001.

- 3 Repita el paso 2 para crear otras VLAN a través de la adición.

- 4 Configure las VLAN con direcciones IP válidas.

- 5 Para crear configuraciones VLAN persistentes, agregue la información de la dirección IP a los archivos de configuración `/etc/hostname.VLAN` correspondientes.

Ejemplo 6–8 Configuración de varias VLAN a través de una adición de vínculos

En este ejemplo se configuran dos VLAN en una adición de vínculos. La salida del comando `dladm show-aggr` indica que la clave de adición del enlace es 1. A las VLAN se asignan los VID 193 y 194, respectivamente.

```
# dladm show-aggr
key: 1 (0x0001) policy: L4 address: 0:3:ba:7:84:5e (auto)
device address speed duplex link state
bge0 0:3:ba:7:b5:a7 1000 Mbps full up attached
bge1 0:3:ba:8:22:3b 0 Mbps unknown down standby
```

```
# ifconfig aggr193001 plumb
# ifconfig aggr193001 192.168.10.5/24 up

# ifconfig aggr194001 plumb
# ifconfig aggr194001 192.168.10.25/24 up

# vi /etc/hostname.aggr193001
192.168.10.5/24

# vi /etc/hostname.aggr194001
192.168.10.25/24
```

Configuración de una red IPv6 (tareas).

Este capítulo presenta tareas para configurar IPv6 en una red. Se tratan los temas principales siguientes:

- “Configuración de una interfaz de IPv6” en la página 171
- “Habilitación de IPv6 en una interfaz (mapa de tareas)” en la página 172
- “Configuración de un enrutador IPv6” en la página 177
- “Modificación de la configuración de una interfaz de IPv6 para hosts y servidores” en la página 181
- “Modificación de la configuración de una interfaz de IPv6 (mapa de tareas)” en la página 181
- “Configuración de túneles para compatibilidad con IPv6” en la página 190
- “Tareas de configuración de túneles para compatibilidad con IPv6 (mapa de tareas)” en la página 189
- “Configuración de la compatibilidad con el servicio de nombres para IPv6” en la página 198

Para obtener una descripción general de los conceptos relativos a IPv6, consulte el [Capítulo 3, “Introducción a IPv6 \(descripción general\)”](#). Para obtener información sobre tareas de planificación de IPv6, consulte el [Capítulo 4, “Planificación de una red IPv6 \(tareas\)”](#). Para buscar información de referencia sobre las tareas del presente capítulo, consulte el [Capítulo 11, “IPv6 en profundidad \(referencia\)”](#).

Configuración de una interfaz de IPv6

Lo primero que debe hacerse es habilitar IPv6 en una interfaz. La admisión de IPv6 puede establecerse durante la instalación de Oracle Solaris o configurando IPv6 en las interfaces de un sistema instalado.

En el proceso de instalación de Oracle Solaris, IPv6 se puede habilitar en una o varias interfaces del sistema. Tras la instalación, se colocan los siguientes archivos y tablas relativos a IPv6:

- Cada interfaz habilitada para IPv6 tiene asociado un archivo `/etc/hostname6.interfaz`, por ejemplo `hostname6.dmfe0`.

- En Solaris 10 11/06 y versiones anteriores, se ha creado el archivo `/etc/inet/ipnodes`. Después de la instalación, en general este archivo sólo contiene las direcciones de bucle de retorno de IPv6 e IPv4.
- Se ha modificado el archivo `/etc/nsswitch.conf` para permitir búsquedas mediante direcciones IPv6.
- Se crea la tabla de directrices de selección de direcciones IPv6. En esta tabla se da prioridad al formato de direcciones IP que debe utilizarse en las transmisiones a través de una interfaz habilitada para IPv6.

En esta sección se explica cómo habilitar IPv6 en las interfaces de un sistema instalado.

Habilitación de IPv6 en una interfaz (mapa de tareas)

La tabla siguiente muestra diferentes tareas para la configuración de las interfaces IPv6. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener instrucciones
Habilitar IPv6 en una interfaz de un sistema en el que ya se haya instalado Oracle Solaris.	Esta tarea se utiliza para habilitar IPv6 en una interfaz después de haberse instalado Oracle Solaris.	“Cómo habilitar una interfaz de IPv6 para la sesión actual” en la página 172
Mantener la interfaz habilitada para IPv6 en los reinicios.	Esta tarea se utiliza para convertir en permanente la dirección IPv6 de la interfaz.	“Cómo habilitar interfaces de IPv6 de manera permanente” en la página 174
Desactivar la configuración automática de direcciones IPv6.	Esta tarea se utiliza para configurar manualmente la sección del ID de interfaz de la dirección IPv6.	“Cómo desactivar la configuración automática de direcciones IPv6” en la página 176

▼ Cómo habilitar una interfaz de IPv6 para la sesión actual

Comience el proceso de configuración de IPv6. Para ello, habilite IPv6 en las interfaces de todos los sistemas que se convertirán en nodos de IPv6. Al principio, la interfaz obtiene su dirección IPv6 mediante el proceso de configuración automática, como se explica en [“Configuración automática de direcciones IPv6” en la página 83](#). Posteriormente, puede adaptar a su conveniencia la configuración del nodo a partir de su función en la red IPv6 como host, servidor o enrutador.

Nota – Si la interfaz se ubica en el mismo vínculo como enrutador que anuncia un prefijo de IPv6, la interfaz obtiene el prefijo de sitio como parte de sus direcciones configuradas automáticamente. Para obtener más información, consulte [“Cómo configurar un enrutador habilitado para IPv6” en la página 178](#).

En el procedimiento siguiente se explica cómo habilitar IPv6 para una interfaz incorporada después de instalar Oracle Solaris.

Antes de empezar

Complete las tareas de planificación de la red IPv6, por ejemplo, actualizar hardware y software, y preparar un plan direcciones. Para obtener más información, consulte [“Planificación de IPv6 \(mapas de tareas\)” en la página 87](#).

1 Inicie sesión en el posible nodo de IPv6 como administrador principal o superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Cree la interfaz si no existe.

```
# ipadm create-ip interface
```

3 Habilite IPv6 en una interfaz.

```
# ifconfig inet6 interface plumb up
```

4 Inicie el daemon de IPv6 in.ndpd.

```
# /usr/lib/inet/in.ndpd
```

Nota – Mediante el comando `ifconfig -a6`, puede visualizarse el estado de las interfaces habilitadas para IPv6 de un nodo.

Ejemplo 7–1 Habilitación de una interfaz para IPv6 tras la instalación

En este ejemplo, se muestra cómo habilitar IPv6 en la interfaz `qfe0`. Antes de comenzar, compruebe el estado de todas las interfaces configuradas en el sistema.

```
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ffffffff
qfe0: flags=1000863 <UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500
    index 2
    inet 172.16.27.74 netmask ffffffff broadcast 172.16.27.255
    ether 0:3:ba:13:14:e1
```

Para este sistema sólo está configurada la interfaz `qfe0`. Habilite IPv6 en esta interfaz de la forma que se indica a continuación:

```
# ifconfig inet6 qfe0 plumb up
# /usr/lib/inet/in.ndpd
# ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 0:3:ba:13:14:e1
    inet6 fe80::203:baff:fe13:14e1/10
```

En el ejemplo se muestra el estado de la interfaz del sistema antes y después de habilitar para IPv6 la interfaz qfe0. La opción -a6 de ifconfig muestra únicamente la información de IPv6 para qfe0 y la interfaz de bucle de retorno. La salida denota que sólo se ha configurado una dirección local de vínculo para qfe0, fe80::203:baff:fe13:14e1/10. Esta dirección indica que hasta ahora ningún enrutador del vínculo local del nodo anuncia un prefijo de sitio.

Tras habilitar IPv6, el comando ifconfig -a es apto para visualizar direcciones IPv4 e IPv6 de todas las interfaces de un sistema.

- Pasos siguientes**
- Para configurar el nodo de IPv6 como enrutador, consulte [“Configuración de un enrutador IPv6” en la página 177](#).
 - Para mantener la configuración de la interfaz de IPv6 en todos los reinicios, consulte [“Cómo habilitar interfaces de IPv6 de manera permanente” en la página 174](#).
 - Para anular la configuración automática de direcciones en el nodo, consulte [“Cómo desactivar la configuración automática de direcciones IPv6” en la página 176](#).
 - Para adaptar el nodo como servidor, tenga en cuenta las sugerencias de [“Administración de interfaces habilitadas para IPv6 en servidores” en la página 188](#).

▼ Cómo habilitar interfaces de IPv6 de manera permanente

Este procedimiento explica la forma de habilitar las interfaces de IPv6 con direcciones IPv6 configuradas automáticamente que se mantengan después de reinicios sucesivos.

Nota – Si la interfaz se ubica en el mismo vínculo como enrutador que anuncia un prefijo de IPv6, la interfaz obtiene el prefijo de sitio como parte de sus direcciones configuradas automáticamente. Para obtener más información, consulte [“Cómo configurar un enrutador habilitado para IPv6” en la página 178](#).

1 Inicie sesión en el nodo de IPv6 como administrador principal o superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Cree direcciones IPv6 para interfaces que se hayan agregado después de la instalación.

a. Cree el archivo de configuración.

```
# touch /etc/hostname6.interface
```

b. Agregue direcciones al archivo de configuración.

```
inet6 ipv6-address up
addif inet6 ipv6-address up
...
```

3 Cree una ruta IPv6 estática predeterminada.

```
# /usr/sbin/route -p add -inet6 default ipv6-address
```

4 (Opcional) Cree un archivo `/etc/inet/ndpd.conf` que defina parámetros para variables de interfaz en el nodo.

Si tiene que crear direcciones temporales para la interfaz del host, consulte [“Uso de direcciones temporales para una interfaz” en la página 182](#). Para obtener más información sobre `/etc/inet/ndpd.conf`, consulte la página de comando `man ndpd.conf(4)` y [“Archivo de configuración ndpd.conf” en la página 264](#).

5 Reinicie el nodo.

```
# reboot -- -r
```

El proceso de reinicio envía paquetes de descubrimiento de enrutadores. Si un enrutador responde con un prefijo de sitio, el nodo puede configurar cualquier interfaz con el pertinente archivo de interfaz `/etc/hostname6.interface` con una dirección IPv6 global. De lo contrario, las interfaces habilitadas para IPv6 se configuran únicamente con direcciones locales de vínculo. Al reiniciarse también se reinician `in.ndpd` y otros daemon de red en modo IPv6.

Ejemplo 7–2 Cómo hacer que una interfaz de IPv6 se mantenga en los reinicios subsiguientes

En este ejemplo se muestra cómo hacer que la configuración IPv6 de la interfaz `qfe0` se mantenga en los reinicios subsiguientes. En este ejemplo, un enrutador del vínculo local anuncia el prefijo de sitio y el ID de subred `2001:db8:3c4d:15/64`.

En primer lugar, compruebe el estado de las interfaces del sistema.

```
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
qfe0: flags=1000863 <UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500
    index 2
    inet 172.16.27.74 netmask fffffff0 broadcast 172.16.27.255
    ether 0:3:ba:13:14:e1

# touch /etc/hostname6.qfe0
# vi /etc/hostname6.qfe0
inet6 fe80::203:baff:fe13:1431/10 up
```

```
addif inet6 2001:db8:3c4d:15:203:baff:fe13:14e1/64 up

# route -p add -inet6 default fe80::203:baff:fe13:1431
# reboot -- -r
```

Verifique que la dirección IPv6 configurada se siga aplicando a la interfaz qfe0.

```
# ifconfig -a6
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 0:3:ba:13:14:e1
    inet6 fe80::203:baff:fe13:14e1/10
qfe0:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500
    index 2
    inet6 2001:db8:3c4d:15:203:baff:fe13:14e1/64
```

La salida de `ifconfig -a6` muestra dos entradas para `qfe0`. La entrada `qfe0` estándar incluye la dirección MAC y la dirección local de vínculo. Una segunda entrada, `qfe0:1`, indica que se ha creado una pseudointerfaz para la dirección IPv6 adicional de la interfaz `qfe0`. La nueva dirección global IPv6, `2001:db8:3c4d:15:203:baff:fe13:14e1/64`, incluye el sitio de prefijo y el ID de subred anunciado por el enrutador local.

- Pasos siguientes**
- Para configurar el nuevo nodo de IPv6 como enrutador, consulte [“Configuración de un enrutador IPv6” en la página 177](#).
 - Para deshabilitar la configuración automática de direcciones en el nodo, consulte [“Cómo desactivar la configuración automática de direcciones IPv6” en la página 176](#).
 - Para adaptar el nodo nuevo como servidor, tenga en cuenta las sugerencias de [“Administración de interfaces habilitadas para IPv6 en servidores” en la página 188](#).

▼ Cómo desactivar la configuración automática de direcciones IPv6

En general, la configuración automática de direcciones se emplea para generar las direcciones IPv6 de las interfaces de hosts y servidores. No obstante, en ocasiones quizá quiera desactivar la configuración automática de direcciones, sobre todo a la hora de configurar manualmente un token, como se explica en [“Configuración de un token IPv6” en la página 185](#).

1 Inicie sesión en el nodo de IPv6 como administrador principal o superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tarear\)” de Guía de administración del sistema: administración básica](#).

2 Cree un archivo `/etc/inet/ndpd.conf` para el nodo.

El archivo `/etc/inet/ndpd.conf` define las variables de interfaz del nodo en particular. Este archivo debería contener lo siguiente a fin de desactivar la configuración automática de direcciones en todas las interfaces del servidor:

```
if-variable-name StatelessAddrConf false
```

Para obtener más información sobre `/etc/inet/ndpd.conf`, consulte la página de comando `man ndpd.conf(4)` y “[Archivo de configuración ndpd.conf](#)” en la [página 264](#).

3 Actualice el daemon de IPv6 con los cambios.

```
# pkill -HUP in.ndpd
```

Configuración de un enrutador IPv6

Lo primero que se hace para configurar IPv6 en una red es configurar IPv6 en un enrutador. Para configurar un enrutador debe realizar una serie de tareas que se describen en esta sección. En función de los requisitos, deberá efectuar todas las tareas o sólo algunas de ellas.

Configuración de IPv6 en enrutadores (mapa de tareas)

Realice las tareas detalladas en la tabla siguiente en el orden en que aparecen, para configurar la red IPv6. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener instrucciones
1. Antes de comenzar la configuración de IPv6, comprobar que se hayan cumplido todos los requisitos previos.	Antes de configurar un enrutador habilitado para IPv6, debe completar las tareas de planificación e instalación de Oracle Solaris con interfaces habilitadas para IPv6.	Capítulo 4, “Planificación de una red IPv6 (tareas)” y “Configuración de una interfaz de IPv6” en la página 171.
2. Configurar un enrutador.	Defina el prefijo de sitio de la red.	“Cómo configurar un enrutador habilitado para IPv6” en la página 178
3. Configurar interfaces de túnel en el enrutador.	Configure en el enrutador un túnel manual o una interfaz de túnel 6to4. La red IPv6 local necesita túneles para comunicarse con otras redes IPv6 aisladas.	<ul style="list-style-type: none">■ “Cómo configurar un túnel 6to4” en la página 192■ “Cómo configurar manualmente IPv6 a través de túneles IPv4” en la página 190■ “Cómo configurar manualmente túneles IPv6 a través de IPv6” en la página 191■ “Cómo configurar túneles IPv4 a través de IPv6” en la página 192

Tarea	Descripción	Para obtener instrucciones
4. Configurar los conmutadores de red.	Si en la configuración de red hay conmutadores, es ahora cuando los debe configurar para IPv6.	Consulte la documentación del fabricante de conmutadores.
5. Configurar los concentradores de red.	Si en la configuración de red hay concentradores, es ahora cuando los debe configurar para IPv6.	Consulte la documentación del fabricante de concentradores.
6. Configurar el nombre de servicio de redes para IPv6.	Configure el servicio de nombres principal (DNS, NIS o LDAP) para reconocer las direcciones IPv6 después de configurar para IPv6 el enrutador.	“Cómo agregar direcciones IPv6 a DNS” en la página 198
7. (Opcional) Modificar las direcciones de las interfaces habilitadas para IPv6 en hosts y servidores.	Después de configurar el enrutador para IPv6, realice las modificaciones pertinentes en los hosts y servidores habilitados para IPv6.	“Modificación de la configuración de una interfaz de IPv6 para hosts y servidores” en la página 181
8. Configurar aplicaciones para que admitan IPv6.	Para admitir IPv6, es posible que cada aplicación necesite unas acciones determinadas.	Consulte la documentación de las aplicaciones.

▼ Cómo configurar un enrutador habilitado para IPv6

Este procedimiento presupone que todas las interfaces del enrutador se han configurado para IPv6 durante la instalación de Oracle Solaris.

- 1 En el sistema que se va a convertir en enrutador de IPv6, asuma la función de administrador principal o de superusuario.**
La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica.](#)

- 2 Revise las interfaces del enrutador que se han configurado para IPv6 durante la instalación.**

ifconfig -a

Compruebe la salida con el fin de asegurarse de que las interfaces que quería configurar para IPv6 estén conectadas con direcciones locales de vínculo. La siguiente salida de ejemplo del comando `ifconfig -a` muestra las direcciones IPv4 e IPv6 que se configuraron para las interfaces del enrutador.

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
dmfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 172.16.26.232 netmask ffffffff broadcast 172.16.26.255
```

```

ether 0:3:ba:11:b1:15
dmfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
inet 172.16.26.220 netmask ffffffff broadcast 172.16.26.255
ether 0:3:ba:11:b1:16
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
inet6 ::1/128
dmfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
ether 0:3:ba:11:b1:15
inet6 fe80::203:baff:fe11:b115/10
dmfe1: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 3
ether 0:3:ba:11:b1:16
inet6 fe80::203:baff:fe11:b116/10

```

Asimismo, la salida muestra que la interfaz de red principal `dmfe0` y la interfaz adicional `dmfe1` se configuraron durante la instalación con las direcciones locales de vínculo IPv6 `fe80::203:baff:fe11:b115/10` y `fe80::203:baff:fe11:b116/10`.

3 Configure el reenvío de paquetes IPv6 en todas las interfaces del enrutador.

En Solaris 10 11/03 y versiones anteriores, utilice el comando siguiente:

```
# routeadm -e ipv6-forwarding -u
```

Utilice cualquiera de las opciones siguientes para habilitar el reenvío de paquetes:

- Utilice el comando `routeadm`, del modo siguiente:

```
# routeadm -e ipv6-forwarding -u
```

- Utilice el siguiente comando de la Utilidad de gestión de servicios (SMF) como se indica:

```
# svcadm enable ipv6-forwarding
```

4 Inicie el daemon de enrutamiento.

El daemon `in.ripngd` se encarga del enrutamiento de IPv6.

En Solaris 10 11/06 y versiones anteriores, inicie `in.ripngd` escribiendo el comando siguiente:

```
# routeadm -e ipv6-routing
# routeadm -u
```

Active el enrutamiento de IPv6 mediante cualquiera de las opciones siguientes:

- Utilice el comando `routeadm` como se indica a continuación:

```
# routeadm -e ipv6-routing -u
```

- Utilice SMF para habilitar el enrutamiento de IPv6:

```
# svcadm enable ripng:default
```

Para obtener información sobre la sintaxis del comando `routeadm`, consulte la página de comando `man routeadm(1M)`.

5 Cree el archivo `/etc/inet/ndpd.conf`.

Especifique el prefijo de sitio que debe anunciar el enrutador y demás datos de configuración en `/etc/inet/ndpd.conf`. El daemon `in.ndpd` lee este archivo e implementa el protocolo de descubrimiento de vecinos de IPv6.

Para obtener una lista de variables y valores admitidos, consulte [“Archivo de configuración ndpd.conf” en la página 264](#) y la página de comando `man ndpd.conf(4)`.

6 Escriba el texto siguiente en el archivo `/etc/inet/ndpd.conf`:

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

Este texto indica al daemon `in.ndpd` que envíe anuncios de enrutador en todas las interfaces del enrutador que se hayan configurado para IPv6.

7 Añada texto al archivo `/etc/inet/ndpd.conf` para configurar el prefijo de sitio en las distintas interfaces del enrutador.

El texto debe tener el formato siguiente:

```
prefix global-routing-prefix:subnet ID/64 interface
```

El siguiente archivo de ejemplo `/etc/inet/ndpd.conf` configura el enrutador para que anuncie el prefijo de sitio `2001:0db8:3c4d::/48` en las interfaces `dmfe0` y `dmfe1`.

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

```
if dmfe0 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:15::0/64 dmfe0
```

```
if dmfe1 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:16::0/64 dmfe1
```

8 Reinicie el sistema.

El enrutador de IPv6 comienza a anunciar en el vínculo cualquier prefijo de sitio que esté en el archivo `ndpd.conf`.

Ejemplo 7–3 Salida de `ifconfig` que muestra interfaces de IPv6

El ejemplo siguiente muestra la salida del comando `ifconfig` - a tal como se recibiría una vez finalizado el procedimiento de [“Configuración de un enrutador IPv6” en la página 177](#).

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ffffffff
dmfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 172.16.15.232 netmask ffffffff broadcast 172.16.26.255
    ether 0:3:ba:11:b1:15
dmfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 172.16.16.220 netmask ffffffff broadcast 172.16.26.255
    ether 0:3:ba:11:b1:16
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
dmfe0: flags=2100841 <UP,RUNNING,MULTICAST,ROUTER,IPv6> mtu 1500 index 2
    ether 0:3:ba:11:b1:15
    inet6 fe80::203:baff:fe11:b115/10
dmfe0:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6> mtu 1500
```

```

        index 2
        inet6 2001:db8:3c4d:15:203:baff:fe11:b115/64
dmfe1: flags=2100841 <UP,RUNNING,MULTICAST,ROUTER,IPv6> mtu 1500 index 3
        ether 0:3:ba:11:b1:16
        inet6 fe80::203:baff:fe11:b116/10
dmfe1:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6> mtu 1500
        index 3
        inet6 2001:db8:3c4d:16:203:baff:fe11:b116/64

```

En este ejemplo, cada interfaz configurada para IPv6 dispone ahora de dos direcciones. La entrada con el nombre de la interfaz, por ejemplo `dmfe0`, muestra la dirección de vínculo local de dicha interfaz. La entrada con el formato *interfaz:n*, por ejemplo, `dmfe0:1`, muestra una dirección IPv6 global. Esta dirección incluye el prefijo de sitio configurado en el archivo `/etc/ndp.conf`, además del ID de interfaz.

- Véase también**
- Para configurar túneles desde los enrutadores identificados en la topología de redes IPv6, consulte [“Configuración de túneles para compatibilidad con IPv6” en la página 190](#).
 - Para obtener información sobre cómo configurar conmutadores y concentradores en la red, consulte la documentación del fabricante.
 - Para configurar hosts de IPv6, consulte [“Modificación de la configuración de una interfaz de IPv6 para hosts y servidores” en la página 181](#).
 - Para mejorar la compatibilidad de IPv6 en los servidores, consulte [“Administración de interfaces habilitadas para IPv6 en servidores” en la página 188](#).
 - Para obtener más información sobre comandos, archivos y daemons de IPv6, consulte [“Oracle Solaris implementación de IPv6” en la página 263](#).

Modificación de la configuración de una interfaz de IPv6 para hosts y servidores

Esta sección explica el procedimiento para modificar la configuración de interfaces habilitadas para IPv6 en nodos que son hosts o servidores. En la mayoría de los casos, deberá utilizar la configuración automática de direcciones para interfaces habilitadas para IPv6, como se explica en [“Descripción general de configuración automática sin estado” en la página 84](#). Sin embargo, la dirección IPv6 de una interfaz se puede modificar, si hace falta, como se explica en las tareas de la presente sección.

Modificación de la configuración de una interfaz de IPv6 (mapa de tareas)

La tabla siguiente muestra diferentes tareas para modificar una red IPv6 existente. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener instrucciones
Desactivar la configuración automática de direcciones IPv6.	Esta tarea se utiliza para configurar manualmente la sección del ID de interfaz de la dirección IPv6.	“Cómo desactivar la configuración automática de direcciones IPv6” en la página 176
Crear una dirección temporal para un host.	Oculte el ID de interfaz de un host. Para ello, configure una dirección temporal creada aleatoriamente que se utilice como los 64 bits inferiores de la dirección.	“Cómo configurar una dirección temporal” en la página 183
Configurar un token para el ID de interfaz de un sistema.	Cree un token de 64 bits para emplearse como ID de interfaz en una dirección IPv6.	“Cómo configurar un token IPv6 especificado por el usuario” en la página 186

Uso de direcciones temporales para una interfaz

Una *dirección temporal* IPv6 emplea un número de 64 bits generado aleatoriamente como ID de interfaz, en lugar de la dirección MAC de la interfaz. Puede utilizar direcciones temporales para cualquier interfaz de un nodo de IPv6 que desee mantener anónimo. Por ejemplo, puede utilizar direcciones temporales para las interfaces de un host que deba acceder a servidores web públicos. Las direcciones temporales implementan mejoras de privacidad de IPv6. Estas mejoras se describen en RFC 3041, que está disponible en “[Privacy Extensions for Stateless Address Autoconfiguration in IPv6](http://www.ietf.org/rfc/rfc3041.txt?number=3041)” (<http://www.ietf.org/rfc/rfc3041.txt?number=3041>).

Las direcciones temporales se habilitan en el archivo `/etc/inet/ndpd.conf` para una o varias interfaces, si es preciso. Sin embargo, a diferencia de las direcciones IPv6 estándar configuradas automáticamente, una dirección temporal consta del prefijo de subred de 64 bits y un número de 64 bits generado aleatoriamente. Ese número aleatorio constituye el segmento de ID de interfaz de la dirección IPv6. Una dirección local de vínculo no se genera con la dirección temporal como ID de interfaz.

Las direcciones temporales tienen un *periodo de vida preferente* predeterminado de un día. Al habilitar la generación de direcciones temporales, también puede configurar las variables siguientes en el archivo `/etc/inet/ndpd.conf`:

<i>periodo de vida válido</i> TmpValidLifetime	Lapso durante el cual existe la dirección temporal; una vez transcurrido, la dirección se elimina del host.
<i>periodo de vida preferente</i> TmpPreferredLifetime	Tiempo transcurrido antes de prescindir de la dirección temporal. Ese lapso de tiempo debe ser más breve que el periodo de vida válido.
<i>regeneración de direcciones</i>	Intervalo de tiempo antes de la conclusión del periodo de vida preferente durante el cual el host debe generar otra dirección temporal.

La duración de las direcciones temporales se especifica de la manera siguiente:

<i>n</i>	<i>n</i> cantidad de segundos, que es el valor predeterminado
<i>n</i> h	<i>n</i> cantidad de horas (h)
<i>n</i> d	<i>n</i> cantidad de días (d)

▼ Cómo configurar una dirección temporal

1 Inicie sesión en el host de IPv6 como administrador principal o superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Si es preciso, habilite IPv6 en las interfaces del host.

Consulte “[Cómo habilitar una interfaz de IPv6 para la sesión actual](#)” en la [página 172](#).

3 Edite el archivo `/etc/inet/ndpd.conf` para activar la generación de direcciones temporales.

- Para configurar direcciones temporales en todas las interfaces de un host, agregue la línea siguiente en el archivo `/etc/inet/ndpd.conf`:

```
ifdefault TmpAddrsEnabled true
```

- Para configurar una dirección temporal para una determinada interfaz, agregue la línea siguiente en el archivo `/etc/inet/ndpd.conf`:

```
if interface TmpAddrsEnabled true
```

4 (Opcional) Especifique el periodo de vida válido de la dirección temporal.

```
ifdefault TmpValidLifetime duration
```

Esta sintaxis especifica el periodo de vida válido de todas las interfaces en un host. El valor de *duración* debe especificarse en segundos, horas o días. El periodo de vida válido predeterminado es 7 días. `TmpValidLifetime` también puede usarse con las palabras clave `if` *interfaz* para especificar el periodo de vida válido de una dirección temporal relativa a una determinada interfaz.

5 (Opcional) Especifique un periodo de vida preferente para la dirección temporal; una vez transcurrido, se prescinde de la dirección.

```
if interface TmpPreferredLifetime duration
```

Esta sintaxis especifica el periodo de vida preferente de la dirección temporal de una determinada interfaz. El periodo de vida preferente predeterminado es un día. `TmpPreferredLifetime` también se puede utilizar con la palabra clave `ifdefault` para indicar el periodo de vida preferente de las direcciones temporales relativas a todas las interfaces de un host.

Nota – La selección de direcciones predeterminadas otorga una prioridad inferior a las direcciones IPv6 que se han descartado. Si se prescinde de una dirección IPv6 temporal, la selección de direcciones predeterminadas elige una dirección no descartada como dirección de origen de un paquete. Una dirección no descartada podría ser la dirección IPv6 generada de manera automática o, posiblemente, la dirección IPv4 de la interfaz. Para obtener más información sobre la selección de direcciones predeterminadas, consulte [“Administración de selección de direcciones predeterminadas” en la página 225](#).

- 6 (Opcional) Especifique el tiempo de generación antes del descarte de direcciones durante el cual el host debe generar otra dirección temporal.**

```
ifdefault TmpRegenAdvance duration
```

Esta sintaxis indica el tiempo de generación antes del descarte de dirección de las direcciones temporales relativas a todas las interfaces de un host. El valor predeterminado es 5 segundos.

- 7 Cambie la configuración del daemon `in.ndpd`.**

```
# kill -HUP in.ndpd
# /usr/lib/inet/in.ndpd
```

- 8 Verifique que las direcciones temporales se hayan creado mediante la ejecución del comando `ifconfig -a6`, como se indica en el [Ejemplo 7-5](#).**

En la salida del comando `ifconfig`, la palabra `TEMPORARY` debería estar en la misma línea en que figura la definición de interfaz.

Ejemplo 7-4 Variables de direcciones temporales en el archivo `/etc/inet/ndpd.conf`

En el ejemplo siguiente se muestra un segmento de un archivo `/etc/inet/ndpd.conf` con direcciones temporales habilitadas para la interfaz de red principal.

```
ifdefault TmpAddrsEnabled true
ifdefault TmpValidLifetime 14d
ifdefault TmpPreferredLifetime 7d
ifdefault TmpRegenAdvance 6s
```

Ejemplo 7-5 Salida del comando `ifconfig -a6` con direcciones temporales habilitadas

En este ejemplo se muestra la salida del comando `ifconfig` tras la creación de direcciones temporales.

```
# ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
```



```
hme0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
      ether 8:0:20:b9:4c:54
      inet6 fe80::a00:20ff:feb9:4c54/10
hme0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
      inet6 2001:db8:3c4d:15:a00:20ff:feb9:4c54/64
hme0:2: flags=802080841<UP,RUNNING,MULTICAST,ADDRCONF,IPv6,TEMPORARY> mtu 1500 index 2
      inet6 2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64
```

En la línea siguiente a la interfaz hme0:2 figura la palabra TEMPORARY. Eso significa que la dirección 2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64 tiene un ID de interfaz temporal.

- Véase también**
- Para configurar la compatibilidad del servicio de nombres para direcciones IPv6, consulte [“Configuración de la compatibilidad con el servicio de nombres para IPv6” en la página 198.](#)
 - Para configurar direcciones IPv6 para un servidor, consulte [“Cómo configurar un token IPv6 especificado por el usuario” en la página 186.](#)
 - Para supervisar actividades en nodos de IPv6, consulte el [Capítulo 8, “Administración de redes TCP/IP \(tareas\)”](#).

Configuración de un token IPv6

El ID de interfaz de 64 bits de una dirección IPv6 también se denomina *token*, como se mencionó en [“Descripción general de las direcciones IPv6” en la página 76](#). Durante la configuración automática de direcciones, el token se asocia con la dirección MAC de la interfaz. En la mayoría de los casos, los nodos sin enrutadores, es decir los hosts y servidores IPv6, deben utilizar sus tokens configurados automáticamente.

No obstante, el uso de tokens configurados automáticamente puede comportar problemas en servidores cuyas interfaces se intercambien de manera rutinaria como parte de la administración de sistemas. Si se cambia la tarjeta de interfaz, también se cambia la dirección MAC. Como consecuencia, los servidores que necesiten direcciones IP estables pueden tener problemas. Las distintas partes de la infraestructura de red, por ejemplo DNS o NIS, pueden tener guardadas determinadas direcciones IPv6 para las interfaces del servidor.

Para prevenir los problemas de cambio de dirección, puede configurar manualmente un token para emplearse como ID de interfaz en una dirección IPv6. Para crear el token, especifique un número hexadecimal de 64 bits o menos para ocupar la parte del ID de interfaz de la dirección IPv6. En la subsiguiente configuración automática de direcciones, el descubrimiento de vecinos no crea un ID de interfaz que se base en la dirección MAC de la interfaz. En lugar de ello, el token creado manualmente se convierte en el ID de interfaz. Este token queda asignado a la interfaz, incluso si se sustituye una tarjeta.

Nota – La diferencia entre los tokens especificados por el usuario y las direcciones temporales es que estas segundas se generan aleatoriamente, no las crea el usuario.

▼ **Cómo configurar un token IPv6 especificado por el usuario**

Las instrucciones siguientes suelen ser útiles en el caso de servidores cuyas interfaces se reemplazan de manera rutinaria. También son aptas para configurar tokens especificados por el usuario en cualquier nodo de IPv6.

1 Verifique que la interfaz que desea configurar con un token esté conectada.

Antes de poder configurar un token para su dirección IPv6, debe estar conectada una interfaz.

```
# ifconfig a6
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 0:3:ba:13:14:e1
    inet6 fe80::203:baff:fe13:14e1/10
```

Esta salida indica que la interfaz de red `qfe0` está conectada y que tiene la dirección local de vínculo `fe80::203:baff:fe13:14e1/10`. Esta dirección se ha configurado automáticamente durante la instalación.

2 Cree uno o varios números hexadecimales de 64 bits para utilizar como tokens para las interfaces del nodo. Para obtener ejemplos de tokens, consulte [“Dirección unidifusión local de vínculo” en la página 81](#).

3 Configure cada interfaz con un token.

Utilice la forma siguiente del comando `ifconfig` para cada interfaz para disponer de un ID de interfaz especificado por el usuario (token):

```
ifconfig interface inet6 token address/64
```

Por ejemplo, utilice el comando siguiente para configurar la interfaz `qfe0` con un token:

```
# ifconfig qfe0 inet6 token ::1a:2b:3c:4d/64
```

Repita este paso con cada interfaz que deba tener un token especificado por el usuario.

4 (Opcional) Haga que la nueva dirección IPv6 se mantenga después de cada reinicio.

a. Cree o edite un archivo `/etc/hostname6.interface` para cada interfaz que haya configurado con un token.

b. Agregue el texto siguiente al final de cada archivo `/etc/hostname.6.interface`:

```
token ::token-name/64
```

Agregue, pongamos por caso, el texto siguiente al final de un archivo `/etc/hostname6.interfaz`:

```
token ::1a:2b:3c:4d/64
```

Una vez se haya reiniciado el sistema, el token que haya configurado en un archivo `/etc/hostname6.interfaz` se aplica a la dirección IPv6 de interfaz. Esta dirección IPv6 se mantiene en los sucesivos reinicios que tengan lugar.

5 Actualice el daemon de IPv6 con los cambios.

```
# pkill -HUP -in.ndpd
```

Ejemplo 7-6 Configuración de un token especificado por el usuario en una interfaz de IPv6

En el ejemplo siguiente, la interfaz `bge0:1` tiene una dirección IPv6 configurada automáticamente. Un enrutador en el vínculo local del nodo anuncia el prefijo de subred `2001:db8:3c4d:152:/64`. El ID de interfaz `2c0:9fff:fe56:8255` se genera a partir de la dirección MAC de `bge0:1`.

```
# ifconfig -a6
lo0: flags=2002000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
    inet6 ::1/128
bge0: flags=2100801 <UP,MULTICAST,IPv6> mtu 1500 index 5
    inet6 fe80::2c0:9fff:fe56:8255/10
    ether 0:c0:9f:56:82:55
bge0:1: flags=2180801 <UP, MULTICAST,ADDRCONF,IPv6>mtu 1500 index 5
    inet6 2001:db8:3c4d:152:c0:9fff:fe56:8255/64
# ifconfig bge0 inet6 token ::1a:2b:3c:4d/64
# vi /etc/hostname6.bge0
token ::1a:2b:3c:4d/64
# pkill -HUP -in.ndpd
# ifconfig -a6
lo0: flags=2002000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
    inet6 ::1/128
bge0: flags=2100801 <UP,MULTICAST,IPv6> mtu 1500 index 5
    inet6 fe80::2c0:9fff:fe56:8255/10
    ether 0:c0:9f:56:82:55
bge0:1: flags=2180801 <UP, MULTICAST,ADDRCONF,IPv6>mtu 1500 index 5
    inet6 2001:db8:3c4d:152:1a:2b:3c:4d/64
```

Después de configurar el token, la dirección global de la segunda línea de estado de `bge0:1` tiene configurado `1a:2b:3c:4d` para su ID de interfaz.

- Véase también**
- Para actualizar los servicios de nombres con las direcciones IPv6 del servidor, consulte [“Configuración de la compatibilidad con el servicio de nombres para IPv6”](#) en la página 198.
 - Para supervisar el rendimiento del servidor, consulte el [Capítulo 8, “Administración de redes TCP/IP \(tareass\)”](#).

Administración de interfaces habilitadas para IPv6 en servidores

Si tiene previsto implementar IPv6 en un servidor, debe adoptar una serie de medidas al habilitar IPv6 en las interfaces del servidor. Las decisiones repercuten en la estrategia que se aplica en la configuración de los ID de interfaz, o *tokens*, de una dirección IPv6 de interfaz.

▼ Cómo habilitar IPv6 en las interfaces de un servidor

Antes de empezar

En el procedimiento que se expone a continuación se da por sentado lo siguiente:

- El servidor ya tiene instalado Oracle Solaris.
- IPv6 se ha habilitado en las interfaces del servidor durante la instalación de Oracle Solaris o posteriormente, siguiendo las instrucciones de [“Configuración de una interfaz de IPv6” en la página 171](#).

Si procede, actualice el software de las aplicaciones para que admitan IPv6. Numerosas aplicaciones que se ejecutan en la pila de protocolo IPv4 también funcionan correctamente en IPv6. Para obtener más información, consulte [“Cómo preparar servicios de red para admitir IPv6” en la página 92](#).

1 En el servidor, adquiera la función de administrador principal o la de superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Compruebe que el prefijo de subred IPv6 esté configurado en un enrutador en el mismo vínculo que el servidor.

Para obtener más información, consulte [“Configuración de un enrutador IPv6” en la página 177](#).

3 Aplique la estrategia pertinente relativa al ID de interfaz en las interfaces habilitadas para IPv6 del servidor.

De forma predeterminada, la configuración automática de direcciones IPv6 utiliza la dirección MAC de una interfaz al crear la parte del ID de interfaz de la dirección IPv6. Si se conoce bien la dirección IPv6 de la interfaz, el intercambio de interfaces puede resultar problemático. La dirección MAC de la nueva interfaz será distinta. En el proceso de configuración automática de direcciones, se genera un nuevo ID de interfaz.

- En una interfaz habilitada para IPv6 que no tenga previsto reemplazar, utilice la dirección IPv6 configurada automáticamente como se ha indicado en [“Configuración automática de direcciones IPv6” en la página 83](#).

- En el caso de interfaces habilitadas para IPv6 que deben figurar como anónimas fuera de la red local, plantee la posibilidad de utilizar para el ID de interfaz un token generado aleatoriamente. Para obtener instrucciones y un ejemplo, consulte [“Cómo configurar una dirección temporal” en la página 183](#).
- En las interfaces habilitadas para IPv6 que tenga previsto intercambiar con regularidad, cree tokens para los ID de interfaz. Para obtener instrucciones y un ejemplo, consulte [“Cómo configurar un token IPv6 especificado por el usuario” en la página 186](#).

Tareas de configuración de túneles para compatibilidad con IPv6 (mapa de tareas)

La tabla siguiente muestra diferentes tareas para configurar distintos tipos de túneles IPv6. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener instrucciones
Configurar manualmente IPv6 en túneles de IPv4.	Se crea manualmente un túnel de IPv6 en una red IPv4; solución para contactar con redes IPv6 remotas en dentro de una red más grande, casi siempre una red empresarial IPv4.	“Cómo configurar manualmente IPv6 a través de túneles IPv4” en la página 190
Configurar manualmente IPv6 en túneles de IPv6.	Se configura manualmente un túnel de IPv6 en una red IPv6; en general, se usa dentro de una red empresarial de gran tamaño.	“Cómo configurar manualmente túneles IPv6 a través de IPv6” en la página 191
Configurar manualmente IPv4 en túneles de IPv6.	Se configura manualmente un túnel de IPv4 en una red IPv6; resulta útil en redes de gran tamaño con redes IPv4 e IPv6.	“Cómo configurar túneles IPv4 a través de IPv6” en la página 192
Configurar automáticamente IPv6 en túneles de IPv4 (túneles de 6to4).	Se crea automáticamente un túnel de 6to4; solución para conectar con un sitio de IPv6 externo por Internet.	“Cómo configurar un túnel 6to4” en la página 192
Configurar un túnel entre un enrutador 6to4 y un enrutador de relés 6to4.	Se habilita un túnel a un enrutador de relés 6to4 mediante el comando 6to4relay.	“Cómo configurar un túnel 6to4 hasta un enrutador de reenvío 6to4” en la página 196

Configuración de túneles para compatibilidad con IPv6

Las redes IPv6 suelen ser entidades aisladas dentro del entorno IPv4 de mayor tamaño. Los nodos de la red IPv6 quizá tengan que comunicarse con nodos de redes IPv6 aisladas, ya sea dentro de la empresa o de manera remota. Lo normal es configurar un túnel entre enrutadores IPv6, si bien los hosts de IPv6 también sirven como puntos finales de túnel. Para obtener información sobre planificación de túneles, consulte [“Planificación de túneles en la topología de red” en la página 93](#).

Los túneles para redes IPv6 se pueden configurar automática o manualmente. La implementación de IPv6 en Oracle Solaris permite los siguientes tipos de encapsulado de túneles:

- IPv6 en túneles de IPv4
- IPv6 en túneles de IPv6
- IPv4 en túneles de IPv6
- Túneles de 6to4

Para obtener descripciones conceptuales de los túneles, consulte [“Túneles de IPv6” en la página 286](#).

▼ Cómo configurar manualmente IPv6 a través de túneles IPv4

Este procedimiento describe cómo configurar un túnel desde un nodo IPv6 a un nodo IPv6 remoto a través de una red IPv4.

1 Acceda al punto final del túnel local como administrador principal o superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Cree el archivo `/etc/hostname6.ip.tun n`.

La letra *n* representa el número de túnel, el primer túnel tiene el número cero. A continuación, añada entradas siguiendo estos pasos:

a. Añada la dirección de origen y la dirección de destino del túnel.

```
tsrc IPv4-source-address tdst IPv4-destination-address up
```

b. (Optativo) Añada una interfaz lógica para la dirección IPv6 de origen y para las direcciones IPv6 de destino.

```
addif IPv6-source-address IPv6-destination-address
```

Puede omitir este paso si quiere que la dirección se autoconfigure para esta interfaz. No es necesario configurar direcciones de vínculo local para el túnel.

- 3 **Reinicie el sistema.**
- 4 **Repita estas tareas en el punto final opuesto del túnel.**

Ejemplo 7-7 Entrada del archivo `/etc/hostname6.ip.tun` para un túnel manual IPv6 a través de IPv4

Este archivo `/etc/hostname6.ip.tun` de ejemplo muestra un túnel para el que las direcciones de origen y las direcciones de destino globales se configuran manualmente.

```
tsrc 192.168.8.20 tdst 192.168.7.19 up
addif 2001:db8:3c4d:8::fe12:528 2001:db8:3c4d:7:a00:20ff:fe12:1234 up
```

▼ **Cómo configurar manualmente túneles IPv6 a través de IPv6**

Este procedimiento describe cómo configurar un túnel desde un nodo IPv6 a un nodo IPv6 remoto a través de una red IPv6.

- 1 **Acceda al punto final del túnel local como administrador principal o superusuario.**
La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.
- 2 **Cree el archivo `/etc/hostname6.ip6.tun n`.**
Utilice los valores 0, 1, 2, etc. para *n*. A continuación, añada entradas siguiendo estos pasos.
 - a. **Añada la dirección de origen y la dirección de destino del túnel.**

```
tsrc IPv6-source-address tdst IPv6-destination-address
IPv6-packet-source-address IPv6-packet-destination-address up
```
 - b. **(Opcativo) Añada una interfaz lógica para la dirección IPv6 de origen y para la dirección IPv6 de destino.**

```
addif IPv6-source-address IPv6-destination-address up
```

Puede omitir este paso si quiere que la dirección se autoconfigure para esta interfaz. No es necesario configurar direcciones de vínculo local para el túnel.
- 3 **Reinicie el sistema.**
- 4 **Repita este procedimiento en el punto final opuesto del túnel.**

Ejemplo 7-8 Entrada del archivo `/etc/hostname6.ip6.tun` para un túnel IPv6 a través de IPv6

En este ejemplo se muestra la entrada para un túnel IPv6 a través de IPv6.

```
tsrc 2001:db8:3c4d:22:20ff:0:fe72:668c tdst 2001:db8:3c4d:103:a00:20ff:fe9b:a1c3
fe80::4 fe80::61 up
```

▼ Cómo configurar túneles IPv4 a través de IPv6

Este procedimiento explica cómo configurar un túnel entre dos hosts IPv4 a través de una red IPv6. Este procedimiento es útil para redes heterogéneas, con subredes IPv6 que separan subredes IPv4.

1 Acceda al punto final del túnel IPv4 local como administrador principal o superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Cree el archivo `/etc/hostname.ip6.tun n` .

Utilice los valores 0, 1, 2, etc. para n . A continuación, añada entradas siguiendo estos pasos:

a. Añada la dirección de origen y la dirección de destino del túnel.

```
tsrc IPv6-source-address tdst IPv6-destination-address
```

b. (Opcativo) Añada una interfaz lógica para la dirección IPv6 de origen y para la dirección IPv6 de destino.

```
addif IPv6-source-address IPv6-destination-address up
```

3 Reinicie el host local.

4 Repita este procedimiento en el punto final opuesto del túnel.

Ejemplo 7-9 Entrada del archivo `/etc/hostname6.ip6.tun` para un túnel IPv4 a través de IPv6

Este ejemplo muestra la entrada para un túnel IPv4 a través de IPv6.

```
tsrc 2001:db8:3c4d:114:a00:20ff:fe72:668c tdst 2001:db8:3c4d:103:a00:20ff:fe9b:a1c3
10.0.0.4 10.0.0.61 up
```

▼ Cómo configurar un túnel 6to4

Si la red IPv6 necesita comunicarse con una red IPv4 remota, es recomendable utilizar túneles 6to4 automáticos. El proceso para configurar un túnel 6to4 incluye la configuración del

enrutador de límite de sistema como un enrutador *6to4*. El enrutador *6to4* funciona como el punto final de un túnel *6to4* entre la red y un enrutador de punto final de una red IPv6 remota.

Antes de empezar

Antes de configurar el enrutamiento *6to4* en una red IPv6, debe haber hecho lo siguiente:

- Configurado IPv6 en todos los nodos correspondientes de la ubicación que se vaya a definir como *6to4*, como se describe en “[Modificación de la configuración de una interfaz de IPv6 para hosts y servidores](#)” en la página 181.
- Seleccionado al menos un enrutador con una conexión a una red IPv4 para que sea el enrutador *6to4*.
- Configurado una dirección IPv4 globalmente única para la interfaz del enrutador que se vaya a definir como *6to4* hasta la red IPv4. La dirección IPv4 debe ser estática.

Nota – No utilice una dirección IPv4 de asignación dinámica, como se describe en el [Capítulo 12, “Acerca de DHCP \(descripción general\)”](#). Las direcciones de asignación dinámica globales pueden cambiar cuando haya pasado un tiempo, lo que puede tener efectos negativos en la planificación de direcciones IPv6.

1 Acceda al enrutador que vaya a definir como 6to4 como administrador principal o superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Configure una pseudo-interfaz 6to4 en el enrutador creando el archivo /etc/hostname6.ip.6to4tun0.

- Si piensa usar la conversión recomendada de ID de subred=0 e ID de host=1, utilice el formato corto para `/etc/hostname6.ip.6to4tun0`:
`tsrc IPv4-address up`
- Si piensa usar otras convenciones para el ID de subred e ID de host, utilice el formato largo para `/etc/hostname6.ip.6to4tun0`:
`tsrc IPv4-address 2002:IPv4-address:subnet-ID:interface-ID:/64 up`

A continuación se muestran los parámetros requeridos para `/etc/hostname6.ip.6to4tun0`:

<code>tsrc</code>	Indica que esta interfaz se utiliza como un origen de túnel.
<code>dirección_IPv4</code>	Especifica, en formato decimal con puntos, la dirección IPv4 configurada en la interfaz física que será la pseudo-interfaz <i>6to4</i> .

El resto de parámetros son optativos. Pero si especifica uno de los parámetros opcionales, debe especificarlos todos.

<code>2002</code>	Especifica el prefijo <i>6to4</i> .
-------------------	-------------------------------------

<i>dirección IPv4</i>	Especifica, como notación hexadecimal, la dirección IPv4 de la pseudo-interfaz.
<i>ID de subred</i>	Especifica, como notación hexadecimal, un ID de subred que no sea 0.
<i>ID_interfaz</i>	Especifica un ID de interfaz que no sea 1.
<i>/64</i>	Indica que el prefijo 6to4 tiene una tamaño de 64 bits.
<i>up</i>	Configura la interfaz 6to4 como "up".

Nota – Dos túneles IPv6 de la red no pueden tener la misma dirección de origen y la misma dirección de destino. Como resultado, se descartarían los paquetes. Este tipo de evento puede suceder si un enrutador 6to4 también realiza tareas de túnel mediante el comando `atun`. Para obtener más información sobre `atun`, consulte la página de comando `man tun(7M)`.

3 (Optativo) Cree pseudo-interfaces 6to4 adicionales en el enrutador.

Cada pseudo-interfaz que se vaya a definir como 6to4 debe tener ya configurada una dirección IPv4 globalmente única.

4 Reinicie el enrutador 6to4.

5 Verifique el estado de la interfaz.

```
# ifconfig ip.6to4tun0 inet6
```

Si la interfaz está configurada correctamente, recibirá un resultado similar al siguiente:

```
ip.6to4tun0: flags=2200041<UP,RUNNING,NUD,IPv6>mtu 1480 index 11
    inet tunnel src 111.222.33.44
    tunnel hop limit 60
    inet6 2002:6fde:212c:10:/64
```

6 Edite el archivo `/etc/inet/ndpd.conf` para anunciar el enrutamiento 6to4.

Si necesita información detallada, consulte la página de comando `man ndpd.conf(4)`.

a. Especifique la subred que recibirá el anuncio en la primera línea.

Cree una entrada `if` con el siguiente formato:

```
if subnet-interface AdvSendAdvertisements 1
```

Por ejemplo, para anunciar el enrutamiento 6to4 a la subred conectada a la interfaz `hme0`, reemplace *interfaz de subred* por `hme0`.

```
if hme0 AdvSendAdvertisements 1
```

b. Añada el prefijo 6to4 como segunda línea del anuncio.

Cree una entrada `prefix` con el siguiente formato:

```
prefix 2002:IPv4-address:subnet-ID::/64 subnet-interface
```

7 Reinicie el enrutador.

También puede enviar un comando `sighup` al daemon `/etc/inet/in.ndpd` para que empiece a enviar anuncios de enrutador. Los nodos IPv6 de cada subred que recibirá el prefijo 6to4 se autoconfiguran con las nuevas direcciones derivadas 6to4.

8 Añada las nuevas direcciones derivadas 6to4 de los nodos al servicio de nombre utilizado en la ubicación 6to4.

Si necesita instrucciones, consulte [“Configuración de la compatibilidad con el servicio de nombres para IPv6” en la página 198](#).

Ejemplo 7-10 Configuración de enrutador 6to4 (Forma corta)

A continuación puede ver un ejemplo de la forma corta de `/etc/hostname6.ip.6to4tun0`:

```
# cat /etc/hostname6.ip.6to4tun0
tsrc 111.222.33.44 up
```

Ejemplo 7-11 Configuración de enrutador 6to4 (Forma larga)

A continuación puede ver un ejemplo de la forma larga de `/etc/hostname6.ip.6to4tun0`:

```
# cat /etc/hostname6.ip.6to4tun0
tsrc 111.222.33.44 2002:6fde:212c:20:1/64 up
```

Ejemplo 7-12 Resultado de `ifconfig` que muestra la pseudo-interfaz 6to4

El siguiente ejemplo muestra el resultado del comando `ifconfig` para una pseudo-interfaz 6to4:

```
# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NOUD,IPv6> mtu 1480 index 11
    inet tunnel src 192.168.87.188
    tunnel hop limit 60
    inet6 2002:c0a8:57bc::1/64
```

Ejemplo 7-13 Anuncio 6to4 en `/etc/inet/ndpd.conf`

El siguiente archivo `/etc/inet/ndpd.conf` de ejemplo anuncia enrutamiento 6to4 a dos subredes:

```
if qfe0 AdvSendAdvertisements 1
prefix 2002:c0a8:57bc:10::/64 qfe0

if qfe1 AdvSendAdvertisements 1
prefix 2002:c0a8:57bc:2::/64 qfe1
```

Más información Configuración de varios enrutadores en la ubicación 6to4

Para ubicaciones con varios enrutadores, los enrutadores que se encuentran detrás del enrutador 6to4 pueden necesitar tareas de configuración adicionales para admitir 6to4. Si en su ubicación se utiliza RIP, debe configurar en cada enrutador no 6to4 las rutas estáticas hasta el enrutador 6to4. Si utiliza un protocolo de enrutamiento comercial, no necesita crear rutas estáticas hasta el enrutador 6to4.

▼ Cómo configurar un túnel 6to4 hasta un enrutador de reenvío 6to4



Precaución – Por problemas graves de seguridad, Oracle Solaris tiene inhabilitada la compatibilidad con enrutadores de reenvío. Consulte [“Cuestiones de seguridad al transmitir datos mediante túnel a un enrutador de reenvío 6to4” en la página 232.](#)

Antes de empezar

Antes de habilitar un túnel hasta un enrutador de reenvío 6to4, debe haber realizado las siguientes tareas:

- Configurar un enrutador 6to4 en la ubicación, como se ha explicado en [“Cómo configurar un túnel 6to4” en la página 192](#)
- Revisar los problemas de seguridad relacionados con el establecimiento de un túnel hasta un enrutador de reenvío 6to4

1 Acceda al enrutador 6to4 como administrador principal o superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica.](#)

2 Habilite un túnel hasta el enrutador de reenvío 6to4 utilizando uno de los siguientes formatos:

- Habilitar un túnel a un enrutador de reenvío 6to4 de difusión por proximidad.

```
# /usr/sbin/6to4relay -e
```

La opción `-e` establece un túnel entre el enrutador 6to4 y un enrutador de reenvío 6to4 de difusión por proximidad. Los enrutadores de reenvío 6to4 de difusión por proximidad

tienen la dirección IPv4 192.88.99.1. El enrutador de reenvío de difusión por proximidad que se encuentre más cerca físicamente de su ubicación pasa a ser el punto final del túnel 6to4. Este enrutador de reenvío gestiona el reenvío de paquetes entre su ubicación 6to4 y una ubicación IPv6 nativa.

Si necesita información detallada sobre enrutadores de reenvío 6to4 de difusión por proximidad, consulte RFC 3068, "An Anycast Prefix for 6to4 Relay Routers" (<ftp://ftp.rfc-editor.org/in-notes/rfc3068.txt>).

- Habilite un túnel hasta un enrutador de reenvío 6to4 específico.

```
# /usr/sbin/6to4relay -e -a relay-router-address
```

La opción `-a` indica que a continuación se especifica una dirección de un enrutador determinado. Reemplace *dirección de enrutador de reenvío* con la dirección IPv4 del enrutador de reenvío 6to4 específico con el que quiera establecer un túnel.

El túnel hasta el enrutador de reenvío 6to4 permanece activo hasta que se elimine la pseudo-interfaz de túnel 6to4.

3 Elimine el túnel hasta el enrutador de reenvío 6to4 cuando ya no sea necesario:

```
# /usr/sbin/6to4relay -d
```

4 (Optativo) Haga que el túnel hasta el enrutador de reenvío 6to4 se mantenga al reiniciar.

Es posible que en su ubicación sea necesario restablecer el túnel hasta el enrutador de reenvío 6to4 cada vez que se reinicia en enrutador 6to4. Para ello, debe hacer lo siguiente:

a. Edite el archivo `/etc/default/inetinit`.

La línea que se debe modificar se encuentra al final del archivo.

b. Cambie el valor "NO" de la línea `ACCEPT6TO4RELAY=NO` por "YES".

c. (Optativo) Cree un túnel a un enrutador de reenvío 6to4 específico que se mantenga al reiniciar.

En el parámetro `RELAY6TO4ADDR`, cambie la dirección 192.88.99.1 por la dirección IPv4 del enrutador de reenvío 6to4 que quiera usar.

Ejemplo 7-14 Obtención de información de estado sobre la compatibilidad con enrutador de reenvío 6to4

Puede usar el comando `/usr/bin/6to4relay` para averiguar si la compatibilidad con enrutadores de reenvío 6to4 está activada. El siguiente ejemplo muestra el resultado cuando la compatibilidad con enrutadores de reenvío 6to4 está desactivada, que es la opción predeterminada en Oracle Solaris:

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is disabled.
```

Si la compatibilidad con enrutadores de reenvío 6to4 está activada, recibirá el siguiente resultado:

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is enabled.
IPv4 remote address of Relay Router=192.88.99.1
```

Configuración de la compatibilidad con el servicio de nombres para IPv6

En esta sección se explica cómo configurar los servicios de nombres DNS y NIS para admitir los servicios de IPv6.

Nota – LDAP admite IPv6 sin tener que realizar tareas de configuración propias de IPv6.

Para obtener información exhaustiva sobre la administración de DNS, NIS y LDAP, consulte la [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

▼ Cómo agregar direcciones IPv6 a DNS

- 1 **Inicie sesión en el servidor DNS principal o secundario como administrador principal o superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de [Guía de administración del sistema: administración básica](#).

- 2 **Edite el pertinente archivo de zona de DNS agregando registros de AAAA por cada nodo habilitado para IPv6:**

```
host-name IN AAAA host-address
```

- 3 **Edite el archivo de zona inversa de DNS y agregue registros PTR:**

```
host-address IN PTR hostname
```

Para obtener más información sobre administración de DNS, consulte [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

Ejemplo 7–15 Archivo de zona inversa de DNS

En este ejemplo se muestra una dirección IPv6 en el archivo de zona inversa.

```
$ORIGIN      ip6.int.
8.2.5.0.2.1.e.f.f.9.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.2.0.0.0 \
      IN              PTR      vallejo.Eng.apex.COM.
```

Adición de direcciones IPv6 a NIS

En Solaris 10 11/06 y versiones anteriores, se habían agregado dos mapas para NIS: `ipnodes.byname` e `ipnodes.byaddr`. Dichos mapas contenían asociaciones de direcciones y nombres de host IPv4 e IPv6. Las herramientas que tienen en cuenta IPv6 utilizaban los mapas de NIS `ipnodes`. Los mapas de `hosts.byname` y `hosts.byaddr` sólo contenían asociaciones de direcciones y nombres de host IPv4. Estos mapas no se modifican con el fin de que puedan facilitar las aplicaciones existentes. La administración de los mapas de `ipnodes` se parece a la de los mapas de `hosts.byname` y `hosts.byaddr`. En Solaris 10 11/06, es importante el hecho de que, al actualizar los mapas de `hosts` con direcciones IPv4, también se actualice con la misma información los mapas de `ipnode`.

Nota – Las versiones posteriores de Oracle Solaris 10 no utilizan los mapas de `ipnodes`. Las funciones de IPv6 de los mapas de `ipnodes` se mantienen ahora en los mapas de `hosts`.

Para obtener información sobre cómo administrar mapas de NIS, consulte el [Capítulo 5, “Instalación y configuración del servicio NIS”](#) de *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*.

▼ Cómo visualizar información sobre servicios de nombres de IPv6

El comando `nslookup` se utiliza para visualizar información sobre servicios de nombres de IPv6.

1 Desde la cuenta de usuario, ejecute el comando `nslookup`.

```
% /usr/sbin/nslookup
```

Se muestran la dirección y el nombre de servidor predeterminados, seguidos del símbolo de comillas angulares del comando `nslookup`.

- 2 **Visualice información de un determinado host. Para ello, en el símbolo de comillas angulares escriba los comandos siguientes:**

```
>set q=any  
>host-name
```

- 3 **Escriba el comando siguiente para ver sólo registros AAAA:**

```
>set q=AAAA  
hostname
```

- 4 **Salga del comando nslookup. Para ello, escriba exit.**

Ejemplo 7-16 Uso del comando nslookup para visualizar información relativa a IPv6

En este ejemplo se muestra el resultado del comando nslookup en un entorno de red IPv6.

```
% /usr/sbin/nslookup  
Default Server: dnsserve.local.com  
Address: 10.10.50.85  
> set q=AAAA  
> host85  
Server: dnsserve.local.com  
Address: 10.10.50.85  
  
host85.local.com IPv6 address = 2::9256:a00:fe12:528  
> exit
```

▼ **Cómo verificar que los registros PTR de DNS IPv6 se actualicen correctamente**

En este procedimiento, el comando nslookup se utiliza para visualizar los registros PTR relativos a DNS IPv6.

- 1 **En la cuenta de usuario, ejecute el comando nslookup.**

```
% /usr/sbin/nslookup
```

Se muestran la dirección y el nombre de servidor predeterminados, seguidos del símbolo de comillas angulares del comando nslookup.

- 2 **En el símbolo de comillas angulares, escriba lo siguiente para ver los registros PTR:**

```
>set q=PTR
```

- 3 **Salga del comando. Para ello, escriba exit.**

Ejemplo 7-17 Uso del comando `nslookup` para visualizar registros PTR

El ejemplo siguiente muestra la visualización de registros PTR generada a partir del comando `nslookup`.

```
% /usr/sbin/nslookup
Default Server:  space1999.Eng.apex.COM
Address:  192.168.15.78
> set q=PTR
> 8.2.5.0.2.1.e.f.f.f.0.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.2.0.0.0.ip6.int

8.2.5.0.2.1.e.f.f.f.0.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.2.0.0.0.ip6.int name =
vallejo.ipv6.Eng.apex.COM
ip6.int nameserver = space1999.Eng.apex.COM
> exit
```

▼ **Cómo visualizar información de IPv6 mediante NIS**

En este procedimiento, el comando `ypmatch` se utiliza para visualizar información relativa a IPv6 mediante NIS:

- En la cuenta de usuario, escriba lo siguiente para visualizar direcciones IPv6 en NIS:

```
% ypmatch hostname hosts ipnodes.byname
```

Aparece la información relativa al *nombre_host* especificado.

Nota – Las versiones de Oracle Solaris posteriores a 11/06 no incluyen los mapas de `ipnodes`. Las funciones relativas a IPv6 de `ipnodes` se mantienen ahora en los mapas de `hosts`.

Ejemplo 7-18 Salida de direcciones IPv6 con el comando `ypmatch`

En Solaris 10 11/06 y versiones anteriores, el ejemplo siguiente muestra los resultados de una operación del comando `ypmatch` en la base de datos de `ipnodes.byname`.

```
% ypmatch farhost hosts ipnodes.byname
2001:0db8:3c4d:15:a00:20ff:fe12:5286      farhost
```

▼ **Cómo visualizar información relativa a IPv6 al margen del servicio de nombres**

Este procedimiento sólo se puede utilizar en Solaris 10 11/06 y versiones anteriores. En versiones posteriores, la misma operación puede realizarse en la base de datos de `hosts`.

- **En la cuenta de usuario, escriba el comando siguiente:**

```
% getent ipnodes hostname
```

Aparece la información relativa al *nombre_host* especificado.

Ejemplo 7–19 Visualización de información relativa a IPv6 en la base de datos de ipnodes

En el ejemplo siguiente se muestra la salida del comando `getent`:

```
% getent ipnodes vallejo
```

```
2001:0db8:8512:2:56:a00:fe87:9aba    myhost myhost  
fe80::56:a00:fe87:9aba    myhost myhost
```

Administración de redes TCP/IP (tareas)

El presente capítulo presenta tareas para la administración de redes TCP/IP. Contiene los temas siguientes:

- “Tareas de administración principales de TCP/IP (mapa de tareas)” en la página 204
- “Supervisión de la configuración de interfaz con el comando `ifconfig`” en la página 205
- “Supervisión del estado de la red con el comando `netstat`” en la página 209
- “Sondeo de hosts remotos con el comando `ping`” en la página 216
- “Administración y registro de la visualización del estado de la red” en la página 217
- “Visualización de información de enrutamiento con el comando `traceroute`” en la página 220
- “Control de transferencias de paquetes con el comando `snoop`” en la página 221
- “Administración de selección de direcciones predeterminadas” en la página 225

Nota – Para supervisar las interfaces de red, consulte [“Supervisión de la configuración de interfaz con el comando `ifconfig`” en la página 205](#).

Las tareas dan por sentado que se dispone de una red TCP/IP operativa, ya sea IPv4y o IPv4/IPv6 de doble pila. Si desea implementar IPv6 en el sistema pero no lo ha hecho, para obtener más información consulte los capítulos siguientes:

- Para programar una implementación de IPv6, consulte el [Capítulo 4, “Planificación de una red IPv6 \(tareas\)”](#).
- Para configurar IPv6 y crear un entorno de red de pila doble, consulte el [Capítulo 7, “Configuración de una red IPv6 \(tareas\)”](#).

Tareas de administración principales de TCP/IP (mapa de tareas)

La tabla siguiente muestra diversas tareas (por ejemplo, mostrar información de red) para la administración de la red tras la configuración inicial. La tabla incluye una descripción de lo que hace cada tarea y la sección de la documentación actual en que se detalla el procedimiento correspondiente.

Tarea	Descripción	Para obtener información
Visualizar información de configuración relativa a una interfaz.	Determinar la configuración actual de cada interfaz en un sistema.	“Cómo obtener información sobre una interfaz específica” en la página 205
Visualizar asignaciones de direcciones de interfaces.	Determinar las asignaciones de direcciones de todas las interfaces del sistema local.	“Cómo mostrar asignaciones de dirección de interfaz” en la página 207
Visualizar estadísticas según el protocolo.	Supervisar el rendimiento de los protocolos de red en un determinado sistema.	“Cómo visualizar estadísticas por protocolo” en la página 209
Visualizar el estado de la red.	Supervisar el sistema visualizando todos los sockets y las entradas de la tabla de enrutamiento. En la salida figuran la familia de direcciones inet4 de IPv4 y la familia de direcciones inet6 de IPv6.	“Cómo visualizar el estado de los sockets” en la página 212
Visualizar el estado de las interfaces de red.	Supervisar el rendimiento de las interfaces de red, útil para resolver problemas de transmisiones.	“Cómo visualizar el estado de interfaces de red” en la página 212
Visualizar el estado de la transmisión de paquetes.	Supervisar el estado de los paquetes conforme se van transmitiendo.	“Cómo visualizar el estado de las transmisiones de paquetes de un determinado tipo de dirección” en la página 214
Controlar la salida en pantalla de los comandos relacionados con IPv6.	Se controla de la salida de los comandos ping, netstat, ifconfig y traceroute. Se crea un archivo denominado inet_type. En este archivo se establece la variable DEFAULT_IP.	“Cómo controlar la salida de visualización de comandos relacionados con IP” en la página 217
Supervisar el tráfico de la red.	Se visualizan todos los paquetes IP mediante el comando snoop.	“Cómo supervisar tráfico de redes IPv6” en la página 224

Tarea	Descripción	Para obtener información
Efectuar el seguimiento de todas las rutas conocidas en los enrutadores de la red.	Se utiliza el comando <code>traceroute</code> para mostrar todas las rutas.	“Cómo efectuar el seguimiento de todas las rutas” en la página 221

Supervisión de la configuración de interfaz con el comando `ifconfig`

El comando `ifconfig` se utiliza para asignar direcciones IP a interfaces y configurar parámetros de interfaces manualmente. Además, las secuencias de comandos de inicio de Oracle Solaris ejecutan `ifconfig` para configurar pseudo-interfaces, como los puntos finales de túnel 6to4.

En este libro se presentan numerosas tareas que emplean las distintas opciones de un comando tan versátil como `ifconfig`. Para ver una descripción completa de este comando, sus opciones y sus variables, consulte la página de comando `man ifconfig(1M)`. A continuación se muestra la sintaxis básica de `ifconfig`:

```
ifconfig interfaz [familia de protocolo]
```

▼ Cómo obtener información sobre una interfaz específica

Utilice el comando `ifconfig` para determinar información básica sobre las interfaces de un sistema específico. Por ejemplo, una consulta `ifconfig simple` proporciona la siguiente información:

- Nombres de dispositivo de todas las interfaces de un sistema
- Todas las direcciones IPv4 y, si las hay, IPv6 asignadas a las interfaces
- Si estas interfaces están configuradas

El siguiente procedimiento muestra cómo usar el comando `ifconfig` para obtener información de configuración básica sobre las interfaces de un sistema.

- 1 En el host local, adquiera la función de administrador principal o la de superusuario.**
La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica.](#)
- 2 Obtenga información sobre una interfaz específica.**

```
# ifconfig interface
```

El resultado del comando `ifconfig` tiene el siguiente formato:

- **Línea de estado**
La primera línea del resultado del comando `ifconfig` contiene el nombre de la interfaz y marcas de estado asociadas a la interfaz. La línea de estado también incluye la unidad de transmisión máxima (MTU) configurada para la interfaz y un número de índice. Utilice la línea de estado para determinar el estado actual de la interfaz.
- **Línea de información de dirección IP**
La segunda línea del resultado de `ifconfig` contiene la dirección IPv4 o IPv6 configurada para la interfaz. Si se trata de una dirección IPv4, la máscara de red y dirección de emisión configuradas también se muestran.
- **Línea de dirección MAC**
Cuando se ejecuta el comando `ifconfig` como superusuario o con una función similar, el resultado de `ifconfig` contiene una tercera línea. Para una dirección IPv4, la tercera línea muestra la dirección MAC (dirección de capa Ethernet) asignada a la interfaz. Para una dirección IPv6, la tercera línea del resultado muestra la dirección de vínculo local que el daemon IPv6 `in.ndpd` genera a partir de la dirección MAC.

Ejemplo 8–1 Información de interfaz básica del comando `ifconfig`

El siguiente ejemplo muestra cómo obtener información sobre la interfaz `eri` en un host específico con el comando `ifconfig`.

```
# ifconfig eri
eri0: flags=863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 1
    inet 10.0.0.112 netmask ffffffff broadcast 10.8.48.127
    ether 8:0:20:b9:4c:54
```

La siguiente tabla describe la información de variables en una consulta `ifconfig` y también incluye la descripción de cómo la variable se puede mostrar en la pantalla y el tipo de información que se proporciona. Se utiliza como ejemplo el resultado anterior.

Variable	Resultado en pantalla	Descripción
Nombre de interfaz	<code>eri0</code>	Indica el nombre de dispositivo de la interfaz cuyo estado se solicita mediante el comando <code>ifconfig</code> .
Estado de interfaz	<code>flags=863<UP</code>	Muestra el estado de la interfaz, con cualquier marca asociada con la interfaz. Con esta información puede determinar si la interfaz está iniciada (UP) o no (DOWN).
Estado de emisión	<code>BROADCAST</code>	Indica que la interfaz admite emisiones IPv4.
Estado de transmisión	<code>RUNNING</code>	Indica que el sistema está transmitiendo paquetes a través de la interfaz.

Variable	Resultado en pantalla	Descripción
Estado multidifusión	MULTICAST, IPv4	Muestra que la interfaz admite transmisiones multidifusión. La interfaz de ejemplo admite transmisiones multidifusión IPv4.
Unidad de transmisión máxima	mtu 1500	Muestra que esta interfaz tiene un tamaño de transferencia máxima de 1500 octetos.
Dirección IP	inet 10.0.0.112	Muestra la dirección IPv4 o IPv6 asignada a la interfaz. La interfaz de ejemplo <code>eri0</code> tiene la dirección IPv4 10.0.0.112.
Máscara de red	netmask ffffffff80	Muestra la máscara de red IPv4 de la interfaz específica. Las direcciones IPv6 no utilizan máscaras de red.
Dirección MAC	ether 8:0:20:b9:4c:54	Muestra la dirección de capa Ethernet de la interfaz.

▼ Cómo mostrar asignaciones de dirección de interfaz

Los enrutadores y hosts múltiples tienen más de una interfaz y, a menudo, más de una dirección IP asignada a cada interfaz. Puede usar el comando `ifconfig` para mostrar todas las direcciones asignadas a las interfaces de un sistema. También puede usar el comando `ifconfig` para mostrar sólo las asignaciones de direcciones IPv4 o IPv6. Para ver también las direcciones MAC de las interfaces, debe iniciar una sesión como superusuario o adquirir la función necesaria.

Si necesita más información sobre el comando `ifconfig`, consulte la página de comando [man ifconfig\(1M\)](#).

1 En el sistema local, asuma la función de administrador de red o hágase superusuario.

Las funciones incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre las funciones, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

2 Obtenga información sobre todas las interfaces.

Puede usar variaciones del comando `ifconfig -a` para hacer lo siguiente:

- Ver todas las direcciones de todas las interfaces del sistema.

```
# ifconfig -a
```
- Ver todas las direcciones IPv4 asignadas a las interfaces de un sistema.

```
# ifconfig -a4
```
- Si el sistema local tiene IPv6, mostrar todas las direcciones IPv6 asignadas a las interfaces de un sistema.

```
ifconfig -a6
```

Ejemplo 8-2 Mostrar la información de direcciones de todas las interfaces

Este ejemplo muestra entradas de un host con una única interfaz principal, `qfe0`. Aunque el resultado de `ifconfig` muestra que hay tres tipos de direcciones asignadas a `qfe0`: loopback (`lo0`), IPv4 (`inet`), e IPv6 (`inet6`). En la sección IPv6 del resultado, la línea de la interfaz `qfe0` muestra la dirección IPv6 de vínculo local. La segunda dirección de `qfe0` se muestra en la línea `qfe0:1`.

```
% ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
qfe0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.112 netmask ffffffff80 broadcast 10.0.0.127
    ether 8:0:20:b9:4c:54
lo0: flags=2000849 <UP,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 8:0:20:b9:4c:54
    inet6 fe80::a00:20ff:feb9:4c54/10
qfe0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
    inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64
```

Ejemplo 8-3 Mostrar la información de direcciones de todas las interfaces IPv4

Este ejemplo muestra la dirección IPv4 configurada para un host múltiple. No necesita ser superusuario para ejecutar este tipo de comando `ifconfig`.

```
% ifconfig -a4
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
qfe0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.112 netmask ffffffff80 broadcast 10.0.0.127
    ether 8:0:20:b9:4c:54
qfe1: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.118 netmask ffffffff80 broadcast 10.0.0.127
    ether 8:0:20:6f:5e:17
```

Ejemplo 8-4 Mostrar la información de dirección de todas las interfaces IPv6

Este ejemplo muestra sólo las direcciones IPv6 configuradas para un host específico. No necesita ser superusuario para ejecutar este tipo de comando `ifconfig`.

```
% ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 8:0:20:b9:4c:54
    inet6 fe80::a00:20ff:feb9:4c54/10
qfe0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
    inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64
```

Este resultado de `ifconfig` muestra los tres tipos de dirección IPv6 siguientes que están asignados a la única interfaz de un host:

lo0

Dirección en bucle IPv6.

inet6 fe80::a00:20ff:feb9:4c54/10

Dirección de vínculo local asignada a la interfaz de red principal.

inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64

Dirección IPv6, con prefijo de subred. El término ADDRCONF en el resultado indica que esta dirección fue autoconfigurada por el host.

Supervisión del estado de la red con el comando netstat

El comando netstat genera visualizaciones que muestran el estado de la red y estadísticas de protocolo. El estado de los protocolos TCP, SCTP y los puntos finales de UDP puede visualizarse en formato de tabla. También puede visualizarse información sobre la tabla de enrutamiento e información de interfaces.

El comando netstat muestra varios tipos de datos de red, según la opción de línea de comandos que se haya seleccionado. Estas visualizaciones son sumamente útiles para administrar sistemas. A continuación se muestra la sintaxis básica del comando netstat:

```
netstat [-m] [-n] [-s] [-i | -r] [-f familia_direcciones]
```

En esta sección se describen las opciones que más se usan del comando netstat. Para obtener más información sobre todas las opciones de netstat, consulte la página de comando [man netstat\(1M\)](#).

▼ Cómo visualizar estadísticas por protocolo

La opción netstat -s muestra estadísticas de los protocolos UDP, TCP, SCTP, ICMP e IP.

Nota – Puede utilizar su cuenta de usuario de Oracle Solaris para obtener salidas del comando netstat.

- **Visualice el estado del protocolo.**

```
$ netstat -s
```

Ejemplo 8–5 Estadísticas de protocolos de red

En el ejemplo siguiente se muestra la salida del comando netstat -s. Se han truncado algunas partes. La salida puede indicar áreas en que el protocolo tiene problemas. Por ejemplo, la información estadística de ICMPv4 e ICMPv6 puede indicar dónde ha encontrado errores el protocolo ICMP.

```

RAWIP
    rawipInDatagrams      = 4701      rawipInErrors      = 0
    rawipInCksumErrs      = 0         rawipOutDatagrams   = 4
    rawipOutErrors        = 0

UDP
    udpInDatagrams        = 10091     udpInErrors         = 0
    udpOutDatagrams       = 15772     udpOutErrors        = 0

TCP
    tcpRtoAlgorithm        = 4         tcpRtoMin           = 400
    tcpRtoMax              = 60000     tcpMaxConn          = -1
    .
    .
    tcpListenDrop          = 0         tcpListenDropQ0     = 0
    tcpHalfOpenDrop        = 0         tcpOutSackRetrans   = 0

IPv4
    ipForwarding           = 2         ipDefaultTTL        = 255
    ipInReceives            = 300182    ipInHdrErrors        = 0
    ipInAddrErrors          = 0         ipInCksumErrs       = 0
    .
    .
    ipsecInFailed          = 0         ipInIPv6             = 0
    ipOutIPv6              = 3         ipOutSwitchIPv6      = 0

IPv6
    ipv6Forwarding         = 2         ipv6DefaultHopLimit = 255
    ipv6InReceives         = 13986     ipv6InHdrErrors      = 0
    ipv6InTooBigErrors      = 0         ipv6InNoRoutes       = 0
    .
    .
    rawipInOverflows       = 0         ipv6InIPv4           = 0
    ipv6OutIPv4            = 0         ipv6OutSwitchIPv4    = 0

ICMPv4
    icmpInMsgs             = 43593     icmpInErrors         = 0
    icmpInCksumErrs        = 0         icmpInUnknowns       = 0
    .
    .
    icmpInOverflows        = 0

ICMPv6
    icmp6InMsgs            = 13612     icmp6InErrors        = 0
    icmp6InDestUnreaches   = 0         icmp6InAdminProhibs  = 0
    .
    .
    icmp6OutGroupQueries    = 0         icmp6OutGroupResps   = 2
    icmp6OutGroupReds       = 0

IGMP:
    12287 messages received
        0 messages received with too few bytes
        0 messages received with bad checksum
    12287 membership queries received

SCTP
    sctpRtoAlgorithm        = vanj
    sctpRtoMin              = 1000
    sctpRtoMax              = 60000
    sctpRtoInitial          = 3000
    sctpTimHearBeatProbe    = 2
    sctpTimHearBeatDrop     = 0
    sctpListenDrop          = 0
    sctpInClosed            = 0

```

▼ Cómo visualizar el estado de protocolos de transporte

El comando `netstat` permite visualizar información sobre el estado de los protocolos de transporte. Para obtener más información, consulte la página de comando [man netstat\(1M\)](#).

1 Visualice el estado de los protocolos de transporte TCP y SCTP en un sistema.

```
$ netstat
```

2 Visualice el estado de un determinado protocolo de transporte en un sistema.

```
$ netstat -P transport-protocol
```

Los valores de la variable `protocolo_transporte` son `tcp`, `sctp` o `udp`.

Ejemplo 8-6 Visualización del estado de los protocolos de transporte TCP y SCTP

En este ejemplo se muestra la salida del comando `netstat` básico. Sólo se muestra información de IPv4.

```
$ netstat
```

TCP: IPv4

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State
lhost-1.login	abc.def.local.Sun.COM.980	49640	0	49640	0	ESTABLISHED
lhost-1.login	ghi.jkl.local.Sun.COM.1020	49640	1	49640	0	ESTABLISHED
remhost-1.1014	mno.pqr.remote.Sun.COM.nfsd	49640	0	49640	0	TIME_WAIT

SCTP:

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	StrsI/O	State
*.echo	0.0.0.0	0	0	102400	0	128/1	LISTEN
*.discard	0.0.0.0	0	0	102400	0	128/1	LISTEN
*.9001	0.0.0.0	0	0	102400	0	128/1	LISTEN

Ejemplo 8-7 Visualización del estado de un determinado protocolo de transporte

En este ejemplo se muestran los resultados que se obtienen al especificar la opción `-P` del comando `netstat`.

```
$ netstat -P tcp
```

TCP: IPv4

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State
lhost-1.login	abc.def.local.Sun.COM.980	49640	0	49640	0	ESTABLISHED
lhost.login	ghi.jkl.local.Sun.COM.1020	49640	1	49640	0	ESTABLISHED
remhost.1014	mno.pqr.remote.Sun.COM.nfsd	49640	0	49640	0	TIME_WAIT

TCP: IPv6

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State	If
localhost.38983	localhost.32777	49152	0	49152	0	ESTABLISHED	

```
localhost.32777 localhost.38983 49152 0 49152 0 ESTABLISHED
localhost.38986 localhost.38980 49152 0 49152 0 ESTABLISHED
```

▼ Cómo visualizar el estado de interfaces de red

La opción `i` del comando `netstat` muestra el estado de las interfaces de red que se configuran en el sistema local. Esta opción permite determinar la cantidad de paquetes que transmite un sistema y que recibe cada red.

- Visualice el estado de las interfaces de red.

```
$ netstat -i
```

Ejemplo 8-8 Visualización del estado de las interfaces de red

En el ejemplo siguiente se muestra el estado de un flujo de paquetes IPv4 e IPv6 a través de las interfaces del host.

Por ejemplo, la cantidad de paquetes de entrada (`Ipkts`) que aparece en un servidor puede aumentar cada vez que un cliente intenta iniciar, mientras que la cantidad de paquetes de salida (`Opkts`) no se modifica. De esta salida puede inferirse que el servidor está viendo los paquetes de solicitud de inicio del cliente. Sin embargo, parece que el servidor no sabe responder. Esta confusión podría deberse a una dirección incorrecta en la base de datos `hosts`, `ipnodes`, o `ethers`.

No obstante, si la cantidad de paquetes de entrada permanece invariable, el equipo no ve los paquetes. De este resultado puede inferirse otra clase de error, posiblemente un problema de hardware.

```
Name Mtu Net/Dest Address Ipkts Ierrs Opkts Oerrs Collis Queue
lo0 8232 loopback localhost 142 0 142 0 0 0
hme0 1500 host58 host58 1106302 0 52419 0 0 0

Name Mtu Net/Dest Address Ipkts Ierrs Opkts Oerrs Collis
lo0 8252 localhost localhost 142 0 142 0 0
hme0 1500 fe80::a00:20ff:feb9:4c54/10 fe80::a00:20ff:feb9:4c54 1106305 0 52422 0 0
```

▼ Cómo visualizar el estado de los sockets

Mediante la opción `-a` del comando `netstat` se puede visualizar el estado de los sockets en el host local.

- Escriba lo siguiente para visualizar el estado de los sockets y las entradas de tabla de enrutador:

Puede emplear su cuenta de usuario para ejecutar esta opción de `netstat`.

```
% netstat -a
```

Ejemplo 8-9 Visualización de todos los sockets y las entradas de tabla de enrutador

La salida del comando `netstat -a` muestra estadísticas exhaustivas. En el ejemplo siguiente se muestran partes de una salida típica de `netstat -a`.

```

UDP: IPv4
  Local Address      Remote Address      State
-----
*.bootpc             Idle
host85.bootpc        Idle
*.                  Unbound
*.                  Unbound
*.sunrpc             Idle
*.                  Unbound
*.32771              Idle
*.sunrpc             Idle
*.                  Unbound
*.32775              Idle
*.time              Idle
.
*.daytime            Idle
*.echo              Idle
*.discard            Idle

UDP: IPv6
  Local Address      Remote Address      State  If
-----
*.                  Unbound
*.                  Unbound
*.sunrpc            Idle
*.                  Unbound
*.32771            Idle
*.32778            Idle
*.syslog            Idle
.

TCP: IPv4
  Local Address      Remote Address      Swind Send-Q Rwind Recv-Q  State
-----
*.                  *.                  0      0 49152    0 IDLE
localhost.4999      *.                  0      0 49152    0 LISTEN
*.sunrpc            *.                  0      0 49152    0 LISTEN
*.                  *.                  0      0 49152    0 IDLE
*.sunrpc            *.                  0      0 49152    0 LISTEN
.
*.printer           *.                  0      0 49152    0 LISTEN
*.time              *.                  0      0 49152    0 LISTEN
*.daytime           *.                  0      0 49152    0 LISTEN
*.echo              *.                  0      0 49152    0 LISTEN
*.discard           *.                  0      0 49152    0 LISTEN
*.chargen           *.                  0      0 49152    0 LISTEN
*.shell             *.                  0      0 49152    0 LISTEN
*.shell             *.                  0      0 49152    0 LISTEN
*.kshell            *.                  0      0 49152    0 LISTEN
*.login
.

```

*TCP: IPv6		0	0	49152	0	LISTEN	
Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State	If
.	*.*	0	0	49152	0	IDLE	
*.sunrpc	*.*	0	0	49152	0	LISTEN	
.	*.*	0	0	49152	0	IDLE	
*.32774	*.*	0	0	49152			

▼ **Cómo visualizar el estado de las transmisiones de paquetes de un determinado tipo de dirección**

Utilice la opción -f del comando netstat para ver estadísticas relacionadas con transmisiones de paquetes de una determinada familia de direcciones.

- **Visualice estadísticas de transmisiones de paquetes de IPv4 o IPv6.**

\$ netstat -f inet | inet6

Para ver información sobre transmisiones de IPv4, escriba inet como argumento de netstat -f. Utilice inet6 como argumento de netstat -f para ver información de IPv6.

Ejemplo 8–10 Estado de transmisión de paquetes de IPv4

En el ejemplo siguiente se muestra la salida del comando netstat -f inet.

TCP: IPv4							
Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State	
host58.734	host19.nfsd	49640	0 49640	0	0	ESTABLISHED	
host58.38063	host19.32782	49640	0 49640	0	0	CLOSE_WAIT	
host58.38146	host41.43601	49640	0 49640	0	0	ESTABLISHED	
host58.996	remote-host.login	49640	0 49206	0	0	ESTABLISHED	

Ejemplo 8–11 Estado de transmisión de paquetes de IPv6

En el ejemplo siguiente se muestra la salida del comando netstat -f inet6.

TCP: IPv6							
Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State	If
localhost.38065	localhost.32792	49152	0 49152	0	0	ESTABLISHED	
localhost.32792	localhost.38065	49152	0 49152	0	0	ESTABLISHED	
localhost.38089	localhost.38057	49152	0 49152	0	0	ESTABLISHED	

▼ Cómo visualizar el estado de rutas conocidas

La opción -r del comando netstat muestra la tabla de rutas del host local. En esta tabla se muestra el estado de todas las rutas de las que el host tiene conocimiento. Esta opción de netstat puede ejecutarse desde la cuenta de usuario.

- Visualice la tabla de rutas IP.

```
$ netstat -r
```

Ejemplo 8-12 Salida de tabla de rutas con el comando netstat

En el ejemplo siguiente se muestra la salida del comando netstat -r.

Routing Table: IPv4						
Destination	Gateway	Flags	Ref	Use	Interface	
<hr/>						
host15	myhost	U	1	31059	hme0	
10.0.0.14	myhost	U	1	0	hme0	
default	distantrouter	UG	1	2	hme0	
localhost	localhost	UH	42019361		lo0	
<hr/>						
Routing Table: IPv6						
Destination/Mask	Gateway	Flags	Ref	Use	If	
<hr/>						
2002:0a00:3010:2::/64	2002:0a00:3010:2:1b2b:3c4c:5e6e:abcd	U	1	0	hme0:1	
fe80::/10	fe80::1a2b:3c4d:5e6f:12a2	U	1	23	hme0	
ff00::/8	fe80::1a2b:3c4d:5e6f:12a2	U	1	0	hme0	
default	fe80::1a2b:3c4d:5e6f:12a2	UG	1	0	hme0	
localhost	localhost	UH	9	21832	lo0	

La tabla siguiente describe el significado de los distintos parámetros de salida de pantalla del comando netstat -r.

Parámetro	Descripción
Destination	Indica el host que es el punto final de destino de la ruta. La tabla de ruta IPv6 muestra el prefijo de un punto final de túnel 6to4
Destination/Mask	(2002:0a00:3010:2::/64) como punto final de destino de la ruta.
Gateway	Especifica el portal que se usa para enviar paquetes.
Flags	Indica el estado actual de la ruta. El indicador U especifica que la ruta está activa. El indicador G especifica que la ruta es a un portal.
Use	Muestra la cantidad de paquetes enviados.
Interface	Indica la interfaz concreta del host local que es el punto final de origen de la transmisión.

Sondeo de hosts remotos con el comando ping

El comando ping se usa para determinar el estado de un host remoto. Al ejecutar el comando ping, el protocolo ICMP envía al host un determinado datagrama para solicitar una respuesta. El protocolo ICMP se ocupa de los errores en las redes TCP/IP. Al utilizar ping, se puede saber si el host remoto dispone de conexión IP.

A continuación se muestra la sintaxis básica del comando ping:

```
/usr/sbin/ping host [tiempo_espera]
```

En esta sintaxis, *host* corresponde al nombre del host remoto. El argumento *tiempo_espera* opcional indica el tiempo en segundos para que el comando ping siga intentando contactar con el host remoto. El valor predeterminado es de 20 segundos. Para obtener más información sobre sintaxis y opciones, consulte la página de comando man [ping\(1M\)](#).

▼ Cómo determinar si un host remoto está en ejecución

- **Escriba la forma siguiente del comando ping:**

```
$ ping hostname
```

Si el host *nombre_host* acepta transmisiones ICMP, se muestra el mensaje siguiente:

```
hostname is alive
```

Este mensaje indica que *nombre_host* ha respondido a la solicitud de ICMP. Sin embargo, si *nombre_host* está desconectado o no puede recibir los paquetes de ICMP, el comando ping genera la respuesta siguiente:

```
no answer from hostname
```

▼ Cómo determinar si un host descarta paquetes

Utilice la opción `-s` del comando ping para determinar si un host remoto está en ejecución y por otro lado pierde paquetes.

- **Escriba la forma siguiente del comando ping:**

```
$ ping -s hostname
```

Ejemplo 8–13 Salida de ping para la detección de paquetes descartados

El comando ping `-s nombre_host` envía constantemente paquetes al host especificado hasta que se envía un carácter de interrupción o finaliza el tiempo de espera. Las respuestas que aparecen en pantalla tienen un aspecto parecido al siguiente:


```
& ping -s host1.domain8
PING host1.domain8 : 56 data bytes
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=0. time=1.67 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=1. time=1.02 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=2. time=0.986 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=3. time=0.921 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=4. time=1.16 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=5. time=1.00 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=5. time=1.980 ms

^C

---host1.domain8 PING Statistics---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip (ms)  min/avg/max/stddev = 0.921/1.11/1.67/0.26
```

La estadística de pérdida de paquetes indica si el host ha descartado paquetes. Si falla el comando ping, compruebe el estado de la red que indican los comandos `ifconfig` y `netstat`. Consulte [“Supervisión de la configuración de interfaz con el comando ifconfig”](#) en la página 205 y [“Supervisión del estado de la red con el comando netstat”](#) en la página 209.

Administración y registro de la visualización del estado de la red

Las tareas siguientes enseñan a comprobar el estado de la red mediante comandos de red perfectamente conocidos.

▼ Cómo controlar la salida de visualización de comandos relacionados con IP

Puede controlar la salida de los comandos `netstat` e `ifconfig` para visualizar sólo información de IPv4, o de IPv4 e IPv6.

- 1 Cree el archivo `/etc/default/inet_type`.
- 2 Agregue una de las entradas siguientes a `/etc/default/inet_type`, según lo que necesite la red:
 - Para visualizar únicamente información de IPv4:


```
DEFAULT_IP=IP_VERSION4
```
 - Para visualizar información de IPv4 e IPv6:


```
DEFAULT_IP=BOTH
```

o

```
DEFAULT_IP=IP_VERSION6
```

Para obtener más información acerca del archivo `inet_type`, consulte la página de comando `man inet_type(4)`.

Nota – Los indicadores `-4` y `-6` del comando `ifconfig` anulan los valores establecidos en el archivo `inet_type`. El indicador `-f` del comando `netstat` también anula los valores establecidos en el archivo `inet_type`.

Ejemplo 8–14 Control de la salida para seleccionar información de IPv4 e IPv6

- Si especifica la variable `DEFAULT_IP=BOTH` o `DEFAULT_IP=IP_VERSION6` en el archivo `inet_type`, en principio debe obtenerse el siguiente resultado:

```
% ifconfig -a
lo0: flags=1000849 mtu 8232 index 1
    inet 10.10.0.1 netmask ff000000
qfe0: flags=1000843 mtu 1500 index 2
    inet 10.46.86.54 netmask ffffffff broadcast 10.46.86.255
    ether 8:0:20:56:a8
lo0: flags=2000849 mtu 8252 index 1
    inet6 ::1/128
qfe0: flags=2000841 mtu 1500 index 2
    ether 8:0:20:56:a8
    inet6 fe80::a00:fe73:56a8/10
qfe0:1: flags=2080841 mtu 1500 index 2
    inet6 2001:db8:3c4d:5:a00:fe73:56a8/64
```

- Si se especifica la variable `DEFAULT_IP=IP_VERSION4` en el archivo `inet_type`, debe obtener el siguiente resultado:

```
% ifconfig -a
lo0: flags=849 mtu 8232
    inet 10.10.0.1 netmask ff000000
qfe0: flags=843 mtu 1500
    inet 10.46.86.54 netmask ffffffff broadcast 10.46.86.255
    ether 8:0:20:56:a8
```

▼ Cómo registrar acciones del daemon de rutas de IPv4

Si tiene la impresión de que el comando `routed`, daemon de rutas de IPv4, funciona de modo incorrecto, inicie un registro que efectúe el seguimiento de la actividad del daemon. El registro incluye todas las transferencias de paquetes al iniciarse el daemon `routed`.

1 En el host local, adquiera la función de administrador principal o la de superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Cree un archivo de registro de acciones de daemon de enrutamiento:

```
# /usr/sbin/in.routed /var/log-file-name
```



Precaución – En una red que esté ocupada, este comando puede generar salida casi continua.

Ejemplo 8–15 Registro de red del daemon `in.routed`

En el ejemplo siguiente se muestra el comienzo del archivo de registro que se crea mediante el procedimiento “[Cómo registrar acciones del daemon de rutas de IPv4](#)” en la página 218.

```
-- 2003/11/18 16:47:00.000000 --
Tracing actions started
RCVBUF=61440
Add interface lo0 #1 127.0.0.1 -->127.0.0.1/32
<UP|LOOPBACK|RUNNING|MULTICAST|IPv4> <PASSIVE>
Add interface hme0 #2 10.10.48.112 -->10.10.48.0/25
<UP|BROADCAST|RUNNING|MULTICAST|IPv4>
turn on RIP
Add 10.0.0.0 -->10.10.48.112 metric=0 hme0 <NET_SYN>
Add 10.10.48.85/25 -->10.10.48.112 metric=0 hme0 <IF|NOPROP>
```

▼ Cómo efectuar el seguimiento de las actividades del daemon de descubrimiento cercano de IPv6

Si tiene la impresión de que el daemon `in.ndpd` funciona de modo incorrecto, inicie un registro que efectúe el seguimiento de la actividad del daemon. Dicho seguimiento se refleja en la salida estándar hasta su conclusión. En el seguimiento figuran todas las transferencias de paquetes al iniciarse el daemon `in.ndpd`.

1 En el nodo IPv6 local, asuma la función de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Inicie el seguimiento del daemon `in.ndpd`.

```
# /usr/lib/inet/in.ndpd -t
```

3 Concluya el seguimiento a su conveniencia. Para ello, pulse las teclas Control+C.

Ejemplo 8–16 Seguimiento del daemon `in.ndpd`

En la salida siguiente se muestra el inicio de un seguimiento del daemon `in.ndpd`.

```
# /usr/lib/inet/in.ndpd -t
Nov 18 17:27:28 Sending solicitation to ff02::2 (16 bytes) on hme0
Nov 18 17:27:28 Source LLA: len 6 <08:00:20:b9:4c:54>
```

```

Nov 18 17:27:28 Received valid advert from fe80::a00:20ff:fee9:2d27 (88 bytes) on hme0
Nov 18 17:27:28      Max hop limit: 0
Nov 18 17:27:28      Managed address configuration: Not set
Nov 18 17:27:28      Other configuration flag: Not set
Nov 18 17:27:28      Router lifetime: 1800
Nov 18 17:27:28      Reachable timer: 0
Nov 18 17:27:28      Reachable retrans timer: 0
Nov 18 17:27:28      Source LLA: len 6 <08:00:20:e9:2d:27>
Nov 18 17:27:28      Prefix: 2001:08db:3c4d:1::/64
Nov 18 17:27:28          On link flag:Set
Nov 18 17:27:28          Auto addrconf flag:Set
Nov 18 17:27:28          Valid time: 2592000
Nov 18 17:27:28          Preferred time: 604800
Nov 18 17:27:28      Prefix: 2002:0a00:3010:2::/64
Nov 18 17:27:28          On link flag:Set
Nov 18 17:27:28          Auto addrconf flag:Set
Nov 18 17:27:28          Valid time: 2592000
Nov 18 17:27:28          Preferred time: 604800

```

Visualización de información de enrutamiento con el comando `traceroute`

El comando `traceroute` efectúa el seguimiento de la ruta que sigue un paquete de IP en dirección a un sistema remoto. Para obtener más información sobre `traceroute`, consulte la página de comando [man traceroute\(1M\)](#).

El comando `traceroute` se usa para descubrir cualquier error de configuración de enrutamiento y errores de ruta de enrutamiento. Si no se puede conectar con un determinado host, el comando `traceroute` sirve para comprobar la ruta que sigue el paquete hasta el host remoto y detectar los errores que pudiera haber.

Asimismo, el comando `traceroute` muestra el tiempo de ida y vuelta en cada portal de la ruta del host de destino. Esta información resulta útil para analizar dónde hay tráfico lento entre dos host.

▼ Cómo saber la ruta de un host remoto

- Para descubrir la ruta de un sistema remoto, escriba lo siguiente:

```
% traceroute destination-hostname
```

Esta forma del comando `traceroute` se puede ejecutar desde la cuenta de usuario.

Ejemplo 8–17 Uso del comando `traceroute` para mostrar la ruta de un host remoto

La salida siguiente del comando `traceroute` muestra la ruta de siete saltos de un paquete que va del sistema local `nearhost` al sistema remoto `farhost`. También muestra los intervalos de tiempo que emplea el paquete en atravesar cada salto.

```
istanbul% traceroute farhost.faraway.com
traceroute to farhost.faraway.com (172.16.64.39), 30 hops max, 40 byte packets
 1 frbldg7c-86 (172.16.86.1)  1.516 ms  1.283 ms  1.362 ms
 2 bldg1a-001 (172.16.1.211)  2.277 ms  1.773 ms  2.186 ms
 3 bldg4-bldg1 (172.16.4.42)  1.978 ms  1.986 ms  13.996 ms
 4 bldg6-bldg4 (172.16.4.49)  2.655 ms  3.042 ms  2.344 ms
 5 ferbldg11a-001 (172.16.1.236)  2.636 ms  3.432 ms  3.830 ms
 6 frbldg12b-153 (172.16.153.72)  3.452 ms  3.146 ms  2.962 ms
 7 sanfrancisco (172.16.64.39)  3.430 ms  3.312 ms  3.451 ms
```

▼ Cómo efectuar el seguimiento de todas las rutas

Este procedimiento emplea la opción `-a` del comando `traceroute` para realizar el seguimiento de todas las rutas.

● Escriba el comando siguiente en el sistema local:

```
% traceroute -a host-name
```

Esta forma del comando `traceroute` se puede ejecutar desde la cuenta de usuario.

Ejemplo 8-18 Seguimiento de todas las rutas de un host de doble pila

En este ejemplo figuran todas las rutas de un host de doble pila.

```
% traceroute -a v6host.remote.com
traceroute: Warning: Multiple interfaces found; using 2::56:a0:a8 @ eri0:2
traceroute to v6host (2001:db8:4a3b::102:a00:fe79:19b0), 30 hops max, 60 byte packets
 1 v6-rout86 (2001:db8:4a3b:56:a00:fe1f:59a1)  35.534 ms  56.998 ms *
 2 2001:db8::255:0:c0a8:717  32.659 ms  39.444 ms *
 3 farhost.faraway.COM (2001:db8:4a3b::103:a00:fe9a:ce7b)  401.518 ms  7.143 ms *
 4 distant.remote.com (2001:db8:4a3b::100:a00:fe7c:cf35)  113.034 ms  7.949 ms *
 5 v6host (2001:db8:4a3b::102:a00:fe79:19b0)  66.111 ms *  36.965 ms

traceroute to v6host.remote.com (192.168.10.75), 30 hops max, 40 byte packets
 1 v6-rout86 (172.16.86.1)  4.360 ms  3.452 ms  3.479 ms
 2 flrmpj17u.here.COM (172.16.17.131)  4.062 ms  3.848 ms  3.505 ms
 3 farhost.farway.com (10.0.0.23)  4.773 ms *  4.294 ms
 4 distant.remote.com (192.168.10.104)  5.128 ms  5.362 ms *
 5 v6host (192.168.15.85)  7.298 ms  5.444 ms *
```

Control de transferencias de paquetes con el comando snoop

El comando `snoop` es apto para supervisar el estado de las transferencias de datos. El comando `snoop` captura paquetes de red y muestra su contenido en el formato que se especifica. Los paquetes se pueden visualizar nada más recibirse o se pueden guardar en un archivo. Si el comando `snoop` escribe en un archivo intermedio, es improbable que haya pérdidas de paquete en situaciones de seguimiento ocupado. El propio comando `snoop` se utiliza para interpretar el archivo.

Para capturar paquetes en y desde la interfaz predeterminada en modo promiscuo, se debe adquirir la función de administración de redes o convertirse en superusuario. En el formato resumido, snoop sólo muestra los datos relativos al protocolo de nivel más alto. Por ejemplo, un paquete de NFS muestra únicamente información de NFS. Se suprime la información subyacente de RPC, UDP, IP y Ethernet; sin embargo, se puede visualizar en caso de elegir cualquiera de las opciones detalladas.

Utilice el comando snoop con frecuencia y buen criterio para familiarizarse con el comportamiento normal del sistema. Para obtener asistencia en el análisis de paquetes, busque documentación técnica reciente y funciones de petición de comentarios; asimismo, solicite el consejo de un experto en un ámbito determinado, por ejemplo NFS o NIS. Para obtener más información sobre el comando snoop y sus opciones, consulte la página de comando `man snoop(1M)`.

▼ Cómo comprobar paquetes de todas las interfaces

1 En el host local, adquiera la función de administrador de redes o la de superusuario.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

2 Imprima la información relativa a las interfaces conectadas al sistema.

```
# ifconfig -a
```

El comando snoop suele utilizar el primer dispositivo que no es de bucle de retorno, en general la interfaz de red principal.

3 Comience a capturar paquetes escribiendo el comando snoop sin argumentos, como se muestra en el [Ejemplo 8–19](#).

4 Para detener el proceso, pulse Control+C.

Ejemplo 8–19 Salida del comando snoop

La salida básica que genera el comando snoop se parece a la siguiente en el caso de un host de doble pila.

```
% snoop
Using device /dev/hme (promiscuous mode)
router5.local.com -> router5.local.com ARP R 10.0.0.13, router5.local.com is
0:10:7b:31:37:80
router5.local.com -> BROADCAST          TFTP Read "network-config" (octet)
farhost.remote.com -> myhost           RLOGIN C port=993
myhost -> nisservice2                   NIS C MATCH 10.0.0.64 in ipnodes.byaddr
nisservice2 -> myhost                  NIS R MATCH No such key
```

```

blue-112 -> slave-253-2      NIS C MATCH 10.0.0.112 in ipnodes.byaddr
myhost -> DNSserver.local.com  DNS C 192.168.10.10.in-addr.arpa. Internet PTR ?
DNSserver.local.com myhost    DNS R 192.168.10.10.in-addr.arpa. Internet PTR
niserve2.
.
.
.
fe80::a00:20ff:febb:e09 -> ff02::9 RIPng R (5 destinations)

```

Los paquetes que se capturan en esta salida muestran una sección de inicio de sesión remoto, incluidas las búsquedas en los servidores NIS y DNS para resolver direcciones. También se incluyen paquetes ARP periódicos del enrutador local y anuncios de la dirección local de vínculos IPv6 en el comando `in.ripngd`.

▼ Cómo capturar salida del comando snoop en un archivo

1 En el host local, adquiera la función de administrador de redes o la de superusuario.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Capture una sesión de snoop en un archivo.

```
# snoop -o filename
```

Por ejemplo:

```
# snoop -o /tmp/cap
Using device /dev/eri (promiscuous mode)
30 snoop: 30 packets captured
```

En el ejemplo, se han capturado 30 paquetes en un archivo que se denomina `/tmp/cap`. El archivo se puede ubicar en cualquier directorio que disponga de suficiente espacio en disco. La cantidad de paquetes capturados se muestra en la línea de comandos, y permite pulsar `Control+C` para cancelar en cualquier momento.

El comando `snoop` crea una evidente carga de red en el equipo `host` que puede distorsionar el resultado. Para ver el resultado real, `snoop` debe ejecutarse desde otro sistema.

3 Inspeccione el archivo de capturas de la salida del comando snoop.

```
# snoop -i filename
```

Ejemplo 8–20 Contenido de un archivo de capturas de la salida del comando snoop

La salida siguiente muestra distintas capturas que se pueden recibir como salida del comando `snoop -i`.

```
# snoop -i /tmp/cap
1  0.00000 fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fe8d:4375
    ICMPv6 Neighbor advertisement
...
10 0.91493 10.0.0.40 -> (broadcast) ARP C Who is 10.0.0.40, 10.0.0.40 ?
34 0.43690 nearserver.here.com -> 224.0.1.1 IP D=224.0.1.1 S=10.0.0.40 LEN=28,
    ID=47453, TO =0x0, TTL=1
35 0.00034 10.0.0.40 -> 224.0.1.1 IP D=224.0.1.1 S=10.0.0.40 LEN=28, ID=57376,
    TOS=0x0, TTL=47
```

▼ Cómo comprobar paquetes entre un cliente y un servidor IPv4

- 1 **Establezca un sistema snoop fuera de un concentrador conectado al cliente o al servidor.**

El tercer sistema (sistema snoop) comprueba todo el tráfico involucrado, de manera que el seguimiento de snoop refleje lo que sucede realmente en la conexión.

- 2 **En el sistema snoop, adquiera la función de administrador de red o conviértase en superusuario.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 3 **Escriba el comando snoop con opciones y guarde la salida que se genere en un archivo.**

- 4 **Inspeccione e interprete la salida.**

Consulte [RFC 1761, Snoop Version 2 Packet Capture File Format \(http://www.ietf.org/rfc/rfc1761.txt?number=1761\)](http://www.ietf.org/rfc/rfc1761.txt?number=1761) para obtener más información sobre el archivo de capturas del comando snoop.

▼ Cómo supervisar tráfico de redes IPv6

El comando snoop puede utilizarse para supervisar únicamente paquetes de IPv6.

- 1 **En el nodo local, adquiera la función de administrador de redes o conviértase en superusuario.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Capture paquetes de IPv6.**

```
# snoop ip6
```

Para obtener más información sobre el comando snoop, consulte la página de comando [man snoop\(1M\)](#).

Ejemplo 8–21 Visualización sólo de tráfico de redes IPv6

En el ejemplo siguiente se muestra una salida típica que puede recibirse tras ejecutar el comando `snoop ip6` en un nodo.

```
# snoop ip6
fe80::a00:20ff:fe9:2d27 -> ff02::1:ffe9:2d27 ICMPv6 Neighbor solicitation
fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fe9:2d27 ICMPv6 Neighbor
solicitation
fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fe9:2d27 ICMPv6 Neighbor
solicitation
fe80::a00:20ff:febb:e09 -> ff02::9          RIPng R (11 destinations)
fe80::a00:20ff:fee9:2d27 -> ff02::1:ffcd:4375 ICMPv6 Neighbor solicitation
```

Administración de selección de direcciones predeterminadas

Oracle Solaris permite que una misma interfaz tenga varias direcciones IP. Por ejemplo, tecnologías como IPMP permiten la conexión de varias tarjetas de interfaz de red en la misma capa de vínculo IP. Ese vínculo puede tener una o varias direcciones IP. Además, las interfaces en sistemas compatibles con IPv6 disponen de una dirección IPv6 local de vínculo, como mínimo una dirección de enrutamiento IPv6 y una dirección IPv4 para al menos una interfaz.

Cuando el sistema inicia una transacción, una aplicación realiza una llamada al socket `getaddrinfo`. `getaddrinfo` descubre la posible dirección que está en uso en el sistema de destino. El núcleo da prioridad a esta lista a fin de buscar el destino más idóneo para el paquete. Este proceso se denomina *ordenación de direcciones de destino*. A continuación, el núcleo de Oracle Solaris selecciona el formato correspondiente para la dirección de origen, a partir de la dirección de destino más apropiada para el paquete. El proceso se denomina *selección de direcciones*. Para obtener más información sobre la ordenación de direcciones de destino, consulte la página de comando `man getaddrinfo(3SOCKET)`.

Los sistemas IPv4 y de doble pila IPv4/IPv6 deben realizar una selección de direcciones predeterminadas. En la mayoría de los casos, no hace falta cambiar los mecanismos de selección de direcciones predeterminadas. Sin embargo, quizá deba cambiar la prioridad de los formatos de direcciones para poder admitir IPMP o preferir los formatos de direcciones 6to4, por ejemplo.

▼ Cómo administrar la tabla de directrices de selección de direcciones IPv6

A continuación se explica el procedimiento para modificar la tabla de directrices de selección de direcciones. Para obtener información sobre la selección de direcciones IPv6 predeterminadas, consulte [“Comando `ipaddrsel`” en la página 269](#).



Precaución – La tabla de directrices de selección de direcciones IPv6 no se debe modificar salvo por los motivos que se exponen en la tarea siguiente. Una tabla de directrices mal configurada puede ocasionar problemas en la red. Efectúe una copia de seguridad de la tabla de directrices, como en el procedimiento siguiente.

1 Asuma el rol de administrador principal, o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Revise la tabla de directrices de selección de direcciones IPv6 actual.

```
# ipaddrsel
# Prefix                Precedence Label
::1/128                  50 Loopback
::/0                     40 Default
2002::/16                30 6to4
::/96                    20 IPv4_Compatible
::ffff:0.0.0.0/96        10 IPv4
```

3 Efectúe una copia de seguridad de la tabla de directrices de direcciones predeterminadas.

```
# cp /etc/inet/ipaddrsel.conf /etc/inet/ipaddrsel.conf.orig
```

4 Si desea personalizar la tabla, utilice un editor de textos en el archivo /etc/inet/ipaddrsel.conf.

Utilice la sintaxis siguiente para las entradas del archivo /etc/inet/ipaddrsel:

prefix/prefix-length precedence label [# comment]

A continuación se muestran varias de las modificaciones habituales que podría querer aplicar a la tabla de directrices:

- Asignar la máxima prioridad a las direcciones 6to4.

```
2002::/16                50 6to4
::1/128                  45 Loopback
```

El formato de dirección 6to4 ahora tiene la prioridad más alta: 50. Bucle, que anteriormente presentaba una prioridad de 50, ahora presenta una prioridad de 45. Los demás formatos de direcciones siguen igual.

- Designar una dirección de origen concreta que se deba utilizar en las comunicaciones con una determinada dirección de destino.

```
::1/128                  50 Loopback
2001:1111:1111::1/128    40 ClientNet
2001:2222:2222::/48      40 ClientNet
::/0                     40 Default
```

Esta entrada en concreto es útil para los host que cuentan sólo con una interfaz física. En este caso, 2001:1111:1111::1/128 se prefiere como dirección de origen de todos los paquetes

cuyo destino previsto es la red 2001:2222:2222::/48. La prioridad 40 otorga una posición preferente a la dirección de origen 2001:1111:1111::1/128 en relación con los demás formatos de direcciones configurados para la interfaz.

- Favorecer direcciones IPv4 respecto a direcciones IPv6.

```
::ffff:0.0.0.0/96          60 IPv4
::1/128                    50 Loopback
.
.
```

El formato de IPv4 ::ffff:0.0.0.0/96 ha cambiado su prioridad predeterminada de 10 a 60, la prioridad máxima de la tabla.

- 5 Cargar en el núcleo la tabla de directrices modificada.

```
ipaddrsel -f /etc/inet/ipaddrsel.conf
```

- 6 Si la tabla de directrices modificada presenta problemas, restaure la tabla predeterminada de directrices de selección de direcciones IPv6.

```
# ipaddrsel -d
```

▼ Cómo modificar la tabla de selección de direcciones IPv6 sólo para la sesión actual

Si edita el archivo `/etc/inet/ipaddrsel.conf`, las modificaciones que efectúe se mantendrán después de cada reinicio. Si quiere aplicar las modificaciones únicamente en la sesión actual, siga este procedimiento.

- 1 Asuma el rol de administrador principal, o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 Copie el contenido de `/etc/inet/ipaddrsel` en *nombre_archivo*; *nombre_archivo* es el archivo que haya seleccionado.

```
# cp /etc/inet/ipaddrsel filename
```

- 3 Modifique la tabla de directrices de *nombre_archivo* a su conveniencia.

- 4 Cargar en el núcleo la tabla de directrices modificada.

```
# ipaddrsel -f filename
```

El núcleo emplea la nueva tabla de directrices hasta que se vuelva a iniciar el sistema.

Resolución de problemas de red (Tareas)

Este capítulo contiene soluciones para problemas comunes que se pueden producir en la red. Contiene los temas siguientes:

- “Consejos de resolución de problemas de red generales” en la página 229
- “Problemas comunes al utilizar IPv6” en la página 231

Novedades de Resolución de problemas de red

En Solaris 10 7/07, el archivo `/etc/inet/ipnodes` queda obsoleto. Utilice `/etc/inet/ipnodes` únicamente para las versiones anteriores de Oracle Solaris 10, tal como se explica en los procedimientos individuales.

Consejos de resolución de problemas de red generales

Uno de los primeros signos de que hay problemas en una red es una pérdida de comunicación de uno o varios hosts. Si un host no aparece la primera vez que se añade a la red, el problema puede ser uno de los archivos de configuración. También puede deberse a una tarjeta de interfaz de red defectuosa. Si un único host comienza a dar problemas de manera repentina, la interfaz de red puede ser la causa. Si los hosts de una red pueden comunicarse entre ellos pero no con otras redes, el problema podría estar en el enrutador. O también podría estar en otra red.

Puede usar el comando `ifconfig` para obtener información sobre interfaces de red. Utilice el comando `netstat` para ver las estadísticas de protocolo y tablas de enrutamiento. Los programas de diagnóstico de otros fabricantes proporcionan varias herramientas de resolución de problemas. Consulte la documentación del fabricante si necesita más información.

Las causas de problemas que afectan al rendimiento de la red resultan más difíciles de identificar. Puede usar herramientas como `ping` para evaluar problemas como la pérdida de paquetes de un host.

Ejecución de comprobaciones de diagnóstico básicas

Si la red tiene problemas, puede ejecutar una serie de comprobaciones de software para diagnosticar y corregir problemas básicos relacionados con el software.

▼ Cómo realizar comprobaciones de software de red básicas

- 1 **En el sistema local, asuma la función de administrador de red o hágase superusuario.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Utilice el comando `netstat` para ver información de red.**

Para ver la sintaxis e información sobre el comando `netstat`, consulte [“Supervisión del estado de la red con el comando `netstat`” en la página 209](#) y la página del comando `man netstat(1M)`.

- 3 **Compruebe la base de datos `hosts` (en Solaris 10 11/06 y versiones anteriores, la base de datos `ipnodes`, si utiliza IPv6) para comprobar que las entradas sean correctas y estén actualizadas.**

Si necesita información sobre la base de datos `/etc/inet/hosts`, consulte [“Base de datos `hosts`” en la página 235](#) y la página de comando `man hosts(4)`. Si necesita información sobre la base de datos `/etc/inet/ipnodes`, consulte [“Base de datos `ipnodes`” en la página 239](#) y la página de comando `man ipnodes(4)`.

- 4 **Si utiliza el protocolo RARP (Reverse Address Resolution Protocol), compruebe las direcciones Ethernet de la base de datos `ethers` para verificar que las entradas son correctas y están actualizadas.**

- 5 **Intente conectarse al host local con el comando `telnet`.**

Si necesita la sintaxis e información sobre `telnet`, consulte la página de comando `man telnet(1)`.

- 6 **Compruebe que el daemon de red `inetd` se esté ejecutando.**

```
# ps -ef | grep inetd
```

El siguiente resultado verifica que el daemon `inetd` se esté ejecutando:

```
root 57 1 0 Apr 04 ? 3:19 /usr/sbin/inetd -s
```

- 7 **Si IPv6 está activado en la red, compruebe que el daemon IPv6 `in.ndpd` se esté ejecutando:**

```
# ps -ef | grep in.ndpd
```

El siguiente resultado verifica que el daemon `in.ndpd` se esté ejecutando:

```
root 123 1 0 Oct 27 ? 0:03 /usr/lib/inet/in.ndpd
```

Problemas comunes al utilizar IPv6

Esta sección describe problemas que pueden producirse al planificar y utilizar IPv6. Para ver las tareas de planificación, consulte el [Capítulo 4, “Planificación de una red IPv6 \(tareas\)”](#).

El enrutador IPv4 no puede actualizarse a IPv6

Si su equipo no puede actualizarse, es posible que necesite comprar equipo preparado para IPv6. Compruebe la documentación del fabricante para ver si hay procedimientos específicos del equipo que tenga que llevar a cabo para que admita IPv6.

Algunos enrutadores IPv4 no pueden actualizarse para admitir IPv6. Si éste es su caso, conecte un enrutador IPv6 junto al enrutador IPv4. De este modo, puede transmitir datos desde el enrutador IPv6 al enrutador IPv4 mediante un túnel. Para obtener información sobre tareas relacionadas con la configuración de túneles, consulte [“Tareas de configuración de túneles para compatibilidad con IPv6 \(mapa de tareas\)”](#) en la [página 189](#).

Problemas tras la actualización de servicios a IPv6

Puede encontrarse con las siguientes situaciones al preparar servicios para que admitan IPv6:

- Algunas aplicaciones, aunque se conviertan a IPv6, no activan IPv6 de manera predeterminada. Es posible que tenga que configurar estas aplicaciones para activar IPv6.
- Un servidor que ejecute varios servicios, algunos sólo IPv4 y otros IPv4 e IPv6, puede producir problemas. Algunos clientes pueden necesitar utilizar varios tipos de servicios, lo que puede generar confusión en el servidor.

El ISP actual no admite IPv6

Si quiere utilizar IPv6 pero su proveedor ISP no ofrece direcciones IPv6, considere las siguientes alternativas en lugar de cambiar de proveedor:

- Contrate los servicios de otro proveedor ISP para que proporcione una segunda línea para las comunicaciones IPv6 de su empresa. Esta solución es cara.
- Consiga un *ISP virtual*. Un ISP virtual proporciona conectividad IPv6 sin vínculo. En su lugar, se crea un túnel desde sus oficinas, a través del ISP IPv4, al ISP virtual.
- Utilice un túnel 6to4 a través de su ISP a otros sitios IPv6. Para las direcciones, utilice las direcciones IPv4 registradas del enrutador 6to4 como sección pública de la dirección IPv6.

Cuestiones de seguridad al transmitir datos mediante túnel a un enrutador de reenvío 6to4

Un túnel entre un enrutador 6to4 y un enrutador de reenvío 6to4 es inseguro en sí mismo. Un túnel de este tipo siempre tendrá los siguientes problemas de seguridad:

- Aunque los enrutadores de reenvío 6to4 encapsulan y desencapsulan paquetes, no comprueban los datos que contienen los paquetes.
- El falseamiento de direcciones es un problema grave de los túneles a enrutadores de reenvío 6to4. Para el tráfico entrante, el enrutador 6to4 no puede comparar la dirección IPv4 del enrutador de reenvío con la dirección IPv6 del origen. Por lo tanto, la dirección del host IPv6 puede falsearse fácilmente. La dirección del enrutador de reenvío 6to4 también puede falsearse.
- De manera predeterminada, no existe ningún mecanismo de confianza entre enrutadores 6to4 y enrutadores de reenvío 6to4. Por lo tanto, un enrutador 6to4 no puede identificar si el enrutador de reenvío 6to4 es de confianza, ni siquiera puede determinar si es un enrutador de reenvío 6to4 legítimo. Debe existir una relación de confianza entre el sitio 6to4 y el destino IPv6, o ambos sitios quedan abiertos a posibles ataques.

Estos problemas y otras cuestiones de seguridad de los enrutadores de reenvío 6to4 se explican en el documento *Security Considerations for 6to4*. En general, sólo es recomendable activar la admisión de enrutadores de reenvío 6to4 en los siguientes casos:

- Pretende comunicarse con una red privada IPv6 de confianza desde su ubicación 6to4. Por ejemplo, puede activar la admisión de enrutadores 6to4 en una red universitaria que consiste en ubicaciones 6to4 aisladas e IPv6 nativas.
- Su ubicación 6to4 tiene motivos importantes de negocios para comunicarse con ciertos hosts IPv6 nativos.
- Ha realizado las comprobaciones y modelos de confianza sugeridos en el documento de *Internet Security Considerations for 6to4*.

Descripción detallada de TCP/IP e IPv4 (referencia)

Este capítulo proporciona información de referencia sobre la red TCP/IP para los archivos de configuración de la red, incluidos los tipos, su finalidad y el formato de las entradas de archivo. Las bases de datos de red existentes también se describen de forma pormenorizada. Asimismo, el capítulo muestra cómo se deriva la estructura de las direcciones IPv4, basándose en clasificaciones de red definidas y en los números de subred.

Este capítulo contiene la información siguiente:

- “Archivos de configuración TCP/IP” en la página 233
- “Bases de datos de red y el archivo `nsswitch.conf`” en la página 244
- “Protocolos de enrutamiento en Oracle Solaris” en la página 253
- “Clases de red” en la página 254

Novedades de TCP/IP e IPv4

En Solaris 10 7/07, el archivo `/etc/inet/ipnodes` pasa a estar obsoleto. Utilice `/etc/inet/ipnodes` únicamente para las versiones anteriores de Oracle Solaris 10, tal como se explica en los procedimientos individuales.

Archivos de configuración TCP/IP

Cada sistema de la red obtiene su información de configuración de TCP/IP de los siguientes archivos de configuración de TCP/IP y bases de datos de red:

- Archivo `/etc/hostname.interfaz`
- Archivo `/etc/nodename`
- Archivo `/etc/defaultdomain`
- Archivo `/etc/defaultrouter` (opcional)
- Base de datos `hosts`
- En Solaris 10 11/06 y versiones anteriores, la base de datos `ipnodes`

- Base de datos netmasks (opcional)

El programa de instalación de Oracle Solaris crea estos archivos como parte del proceso de instalación. También puede editar manualmente los archivos, como se describe en esta sección. `hosts` y `netmasks` son dos de las bases de datos de red que leen los servicios de nombres disponibles en las redes de Oracle Solaris. “[Bases de datos de red y el archivo `nsswitch.conf`](#)” en la [página 244](#) describe detalladamente el concepto de bases de datos de red. En Solaris 10 11/06 y versiones anteriores, para obtener información sobre el archivo `ipnodes`, consulte “[Base de datos `ipnodes`](#)” en la [página 239](#).

Archivo `/etc/hostname.interface`

Este archivo define las interfaces de red físicas en el host local. En el sistema local debe haber como mínimo un archivo `/etc/hostname.interface`. El programa de instalación de Oracle Solaris crea un archivo `/etc/hostname.interface` para la primera interfaz que se encuentra durante el proceso de instalación. Esta interfaz normalmente tiene el número de dispositivo menor, por ejemplo, `eri0`, y se hace referencia a ella como la *interfaz de red principal*. Si el programa de instalación encuentra interfaces adicionales, puede configurarlas de modo opcional, como parte del proceso de instalación.

Nota – Si crea archivos alternativos de host para la misma interfaz, también deben seguir el formato de asignación de nombres `hostname.[0-9]*`, como, por ejemplo, `hostname.qfe0.a123`. Nombres como `hostname.qfe0.bak` o `hostname.qfe0.old` no son válidos y serán ignorados por las secuencias durante el inicio del sistema.

Tenga en cuenta también que sólo puede haber un archivo de nombre de host para una interfaz determinada. Si crea archivos alternativos de host para una interfaz con un nombre de archivo válido como, por ejemplo, `/etc/hostname.qfe` y `/etc/hostname.qfe.a123`, las secuencias de comandos de inicio intentarán la configuración mediante la referencia a los contenidos de ambos archivos de host, y se generarán errores. Para evitar esos errores, proporcione un nombre de archivo no válido para el sistema host que no desea utilizar en una configuración concreta.

Si agrega una interfaz de red nueva al sistema tras la instalación, debe crear un archivo `/etc/hostname.interface` para dicha interfaz, tal como se explica en “[Cómo configurar una interfaz física tras la instalación del sistema](#)” en la [página 148](#). Asimismo, para que el software Oracle Solaris reconozca y utilice la nueva interfaz de red, debe cargar el controlador de dispositivos de la interfaz en el directorio correspondiente. Consulte la documentación que se incluye con la nueva interfaz de red para conocer el nombre de la *interfaz* pertinente y las instrucciones relativas al controlador de dispositivos.

El archivo `/etc/hostname.interface` básico contiene una entrada: el nombre de host o dirección IPv4 asociados con la interfaz de red. La dirección IPv4 se puede expresar en el formato decimal

con punto tradicional o en la notación CIDR. Si utiliza un nombre de host como entrada para el archivo `/etc/hostname.interfaz`, dicho nombre de host también debe existir en el archivo `/etc/inet/hosts`.

Por ejemplo, supongamos que `smc0` es la interfaz de red principal para un sistema denominado `tenere`. El archivo `/etc/hostname.smc0` podría tener como entrada una dirección IPv4 en notación decimal con punto o CIDR, o el nombre de host `tenere`.

Nota – IPv6 utiliza el archivo `/etc/hostname6.interfaz` para definir las interfaces de red. Para más información, consulte [“Archivo de configuración de interfaces de IPv6”](#) en la página 267.

Archivo `/etc/nodename`

Este archivo debe contener una entrada: el nombre de host del sistema local. Por ejemplo, en el sistema `timbuktu`, el archivo `/etc/nodename` incluiría la entrada `timbuktu`.

Archivo `/etc/defaultdomain`

Este archivo debe contener una entrada: el nombre de dominio completo del dominio administrativo al que pertenece la red del host local. Puede proporcionar este nombre en el programa de instalación de Oracle Solaris o editar el archivo posteriormente. Para más información sobre los dominios de red, consulte [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

Archivo `/etc/defaultrouter`

Este archivo puede contener una entrada para cada enrutador que esté conectado directamente a la red. La entrada debe ser el nombre de la interfaz de red que actúe como enrutador entre las redes. La presencia del archivo `/etc/defaultrouter` indica que el sistema está configurado para admitir el enrutamiento estático.

Base de datos `hosts`

La base de datos `hosts` contiene las direcciones IPv4 y los nombres de host de los sistemas de la red. Si utiliza el servicio de nombres NIS o DNS, o el servicio de directorios LDAP, la base de datos `hosts` se guarda en una base de datos designada para la información del host. Por ejemplo, en una red que ejecuta NIS, la base de datos `hosts` se guarda en el archivo `hostsbyname`.

Si utiliza los archivos locales para el servicio de nombres, la base de datos `hosts` se mantiene en el archivo `/etc/inet/hosts`. Este archivo contiene los nombres de host y las direcciones IPv4 de la interfaz de red principal, las demás interfaces de red conectadas al sistema y cualquier otra dirección de red que deba comprobar el sistema.

Nota – Para fines de compatibilidad con los sistemas operativos basados en BSD, el archivo `/etc/hosts` es un vínculo simbólico a `/etc/inet/hosts`.

Formato de archivo `/etc/inet/hosts`

El archivo `/etc/inet/hosts` utiliza la sintaxis básica que se incluye a continuación. Consulte la página del comando `man hosts(4)` para obtener información completa acerca de la sintaxis.

nombre_host dirección_IPv4 [apodos] [#comentario]

dirección_IPv4 Contiene la dirección IPv4 de cada interfaz que debe reconocer el host local.

nombre_host Contiene el nombre de host asignado al sistema durante la instalación, además de los nombres de host asignados a interfaces de red adicionales que debe reconocer el host local.

[apodo] Es un campo opcional que contiene un apodo para el host.

[#comentario] Es un campo opcional para un comentario.

Archivo `/etc/inet/hosts` inicial

Al ejecutar el programa de instalación de Oracle Solaris en un sistema, el programa configura el archivo `/etc/inet/hosts` inicial. Este archivo contiene las entradas mínimas que requiere el host local. Las entradas incluyen la dirección en bucle, la dirección IPv4 del host y el nombre de host.

Por ejemplo, el programa de instalación de Oracle Solaris podría crear el siguiente archivo `/etc/inet/hosts` para el sistema `tenere` mostrado en la [Figura 5–1](#).

EJEMPLO 10–1 Archivo `/etc/inet/hosts` para el sistema `tenere`

```
127.0.0.1      localhost      loghost      #loopback address
192.168.200.3  tenere          #host name
```

Dirección en bucle

En el [Ejemplo 10–1](#), la dirección IPv4 `127.0.0.1` es la *dirección en bucle*. La dirección en bucle es la interfaz de red reservada que utiliza el sistema local para permitir la comunicación entre los procesos. Esta dirección permite al host enviarse paquetes a sí mismo. El comando `ifconfig` utiliza la dirección en bucle de retorno para la configuración y las pruebas, tal como se explica

en [“Supervisión de la configuración de interfaz con el comando ifconfig” en la página 205](#). Cada sistema de una red TCP/IP debe utilizar la dirección IP 127.0.0.1 para el bucle IPv4 del host local.

Nombre de host

La dirección IPv4 192.168.200.1 y el nombre tienen son la dirección y el nombre de host del sistema local. Se asignan a la interfaz de red principal del sistema.

Múltiples interfaces de red

Algunos sistemas tienen más de una interfaz de red, dado que son enrutadores o hosts múltiples. Cada interfaz de red conectada al sistema requiere su propia dirección IP y un nombre asociado. Durante la fase de instalación, debe configurar la interfaz de red principal. Si un sistema concreto tiene varias interfaces en el momento de la instalación, el programa de instalación de Oracle Solaris preguntará por estas interfaces adicionales. De modo opcional, puede configurar una o más interfaces adicionales en este punto, o puede hacerlo manualmente más adelante.

Tras la instalación de Solaris, puede configurar interfaces adicionales para un enrutador o host múltiple agregando información de la interfaz al archivo `/etc/inet/hosts` del sistema. Para más información sobre cómo configurar los enrutadores y hosts múltiples, consulte [“Configuración de un enrutador IPv4” en la página 121](#) y [“Configuración de hosts múltiples” en la página 129](#).

El [Ejemplo 10–2](#) muestra el archivo `/etc/inet/hosts` para el sistema `timbuktu` que se incluye en la [Figura 5–1](#).

EJEMPLO 10–2 Archivo `/etc/inet/hosts` para el sistema `timbuktu`

```
127.0.0.1      localhost      loghost
192.168.200.70 timbuktu      #This is the local host name
192.168.201.10 timbuktu-201  #Interface to network 192.9.201
```

Con estas dos interfaces, `timbuktu` conecta las redes 192.168.200 y 192.168.201 como enrutador.

Cómo afectan los servicios de nombres a la base de datos hosts

Los servicios de nombres NIS y DNS, así como el servicio de directorios LDAP, guardan los nombres de host y direcciones en uno o más servidores. Estos servidores mantienen las bases de datos `hosts` que contienen información de cada host y enrutador (si es pertinente) en la red del servidor. Consulte [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#) para obtener más información acerca de estos servicios.

Si los archivos locales proporcionan el servicio de nombres

En una red que utiliza los archivos locales para el servicio de nombres, los sistemas que se ejecutan en modo de archivos locales consultan sus archivos `/etc/inet/hosts` individuales para conocer las direcciones IPv4 y los nombres de host de otros sistemas de la red. Por tanto, los archivos `/etc/inet/hosts` del sistema deben contener lo siguiente:

- Dirección en bucle
- Dirección IPv4 y nombre de host del sistema local (interfaz de red principal)
- Dirección IPv4 y nombre de host de las interfaces de red adicionales conectadas a este sistema, si es preciso
- Direcciones IPv4 y nombres de host de todos los hosts de la red local
- Direcciones IPv4 y nombres de host de cualquier enrutador que deba conocer este sistema, si es preciso
- Dirección IPv4 de cualquier sistema que desee consultar el sistema por nombre de host

La [Figura 10–1](#) muestra el archivo `/etc/inet/hosts` para el sistema `tenere`. Este sistema se ejecuta en modo de archivos locales. Tenga en cuenta que el archivo contiene las direcciones IPv4 y los nombres de host de cada sistema de la red `192.9.200`. El archivo también contiene la dirección IPv4 y el nombre de interfaz `timbuktu-201`. Esta interfaz conecta la red `192.9.200` con la red `192.9.201`.

Un sistema configurado como cliente de red utiliza el archivo `/etc/inet/hosts` local para sus direcciones en bucle e IPv4.

FIGURA 10-1 Archivo /etc/inet/hosts para un sistema que se ejecuta en modo de archivos locales

	# Desert Network - Hosts File			
	#			
	# If the NIS is running, this file is only consulted			
	# when booting			
	#			
Línea de localhost	127.0.0.1	localhost		
	#			
Línea de nombre de host	192.9.200.1	tenere		#This is my machine
Línea de servidor	192.9.200.50	sahara	big	#This is the net config server
	#			
Otros hosts	192.9.200.2	libyan	libby	#This is Tom's machine
	192.9.200.3	ahaggar		#This is Bob's machine
	192.9.200.4	nubian		#This is Amina's machine
	192.9.200.5	faiyum	suz	#This is Suzanne's machine
	192.9.200.70	timbuktu	tim	#This is Kathy's machine
	192.9.201.10	timbuktu-201		#Interface to net 192.9.201 on #timbuktu

Base de datos ipnodes

Nota – La base de datos ipnodes ya no se incluye en las versiones posteriores a Solaris 10 11/06. En las versiones subsiguientes, las funciones de IPv6 de ipnodes se migran a la base de datos hosts.

El archivo /etc/inet/ipnodes almacena las direcciones IPv4 e IPv6. Además, puede guardar direcciones IPv4 en las notaciones decimal con punto o CIDR. Este archivo sirve como base de datos local que asocia los nombres de hosts con sus direcciones IPv4 e IPv6. No guarde los nombres de host y sus direcciones en archivos estáticos, como /etc/inet/ipnodes. En cambio, para fines de pruebas, debe guardar las direcciones IPv6 en un archivo del mismo modo que las direcciones IPv4 se guardan en /etc/inet/hosts. El archivo ipnodes utiliza la misma

convención de formato que el archivo `hosts`. Para más información sobre `/etc/inet/hosts`, consulte [“Base de datos hosts” en la página 235](#). Consulte la página del comando `man ipnodes(4)` para ver una descripción del archivo `ipnodes`.

Las aplicaciones habilitadas para IPv6 utilizan la base de datos `/etc/inet/ipnodes`. La base de datos `/etc/hosts` existente, que contiene sólo direcciones IPv4, permanece igual para facilitar las aplicaciones existentes. Si la base de datos `ipnodes` no existe, las aplicaciones habilitadas para IPv6 utilizan la base de datos `hosts` existente.

Nota – Si necesita agregar direcciones, debe agregar las direcciones IPv4 tanto al archivo `hosts` como al archivo `ipnodes`. Las direcciones IPv6 se agregan sólo al archivo `ipnodes`.

EJEMPLO 10-3 Archivo `/etc/inet/ipnodes`

Debe agrupar las direcciones del nombre de host por nombre de host, como se muestra en este ejemplo.

```
#
# Internet IPv6 host table
# with both IPv4 and IPv6 addresses
#
::1          localhost
2001:db8:3b4c:114:a00:20ff:fe78:f37c  farsite.com farsite farsite-v6
fe80::a00:20ff:fe78:f37c      farsite-11.com farsitell
192.168.85.87                  farsite.com farsite farsite-v4
2001:db8:86c0:32:a00:20ff:fe87:9aba  nearsite.com nearsite nearsite-v6
fe80::a00:20ff:fe87:9aba      nearsite-11.com nearsitell
10.0.0.177                     nearsite.com nearsite nearsite-v4 loghost
```

Base de datos `netmasks`

Debe editar la base de datos `netmasks` como parte de la configuración de red *sólo* si ha configurado las subredes en la red. La base de datos `netmasks` se compone de una lista de redes y sus máscaras de subred asociadas.

Nota – Al crear subredes, cada nueva red debe ser una red física independiente. No puede aplicar las subredes a una única red física.

¿Qué son las subredes?

Las *subredes* son un método para maximizar el espacio de direcciones IPv4 de 32 bits y reducir el tamaño de las tablas de enrutamiento en una interred mayor. En cualquier clase de dirección, las subredes proporcionan un medio de asignar parte del espacio de la dirección host a las

direcciones de red, lo cual permite tener más redes. La parte del espacio de dirección de host asignada a las nuevas direcciones de red se conoce como *número de subred*.

Además de hacer que el espacio de la dirección IPv4 sea mas eficaz, las subredes presentan varias ventajas administrativas. El enrutamiento puede complicarse enormemente a medida que aumenta el número de redes. Por ejemplo, una pequeña organización podría asignar a cada red local un número de clase C. A medida que la organización va aumentando, puede complicarse la administración de los diferentes números de red. Es recomendable asignar pocos números de red de clase B a cada división principal de una organización. Por ejemplo, podría asignar una red de clase B al departamento de ingeniería, otra al departamento de operaciones, etc. A continuación, podría dividir cada red de clase B en redes adicionales, utilizando los números de red adicionales obtenidos gracias a las subredes. Esta división también puede reducir la cantidad de información de enrutamiento que se debe comunicar entre enrutadores.

Creación de la máscara de red para las direcciones IPv4

Como parte del proceso de subredes, debe seleccionar una *máscara de red* para toda la red. La máscara de red determina cuántos y qué bits del espacio de la dirección host representan el número de subred y cuántos y cuáles representan el número de host. Recuerde que la dirección IPv4 completa se compone de 32 bits. En función de la clase de dirección, puede haber como máximo 24 bits y como mínimo 8 disponibles para representar el espacio de la dirección host. La máscara de red se especifica en la base de datos `netmasks`.

Si tiene previsto utilizar subredes, debe determinar la máscara de red antes de configurar TCP/IP. Si tiene previsto instalar el sistema operativo como parte de la configuración de red, el programa de instalación de Oracle Solaris solicita la máscara de red para la red.

Tal como se describe en [“Cómo diseñar un esquema de direcciones IPv4” en la página 58](#), las direcciones IP de 32 bits se componen de una parte de red y una parte de host. Los 32 bits se dividen en 4 bytes. Cada byte se asigna al número de red o al número de host, según la clase de red.

Por ejemplo, en una dirección IPv4 de clase B, los 2 bytes de la izquierda se asignan al número de red, y los 2 de la derecha al número de host. En la dirección IPv4 de clase B 172.16.10, puede asignar los 2 bytes de la derecha a hosts.

Si desea implementar subredes, debe utilizar algunos de los bits de los bytes asignados al número de host para aplicar a las direcciones de subred. Por ejemplo, un espacio de dirección host de 16 bits proporciona direcciones para 65.534 hosts. Si aplica el tercer byte a las direcciones de subred y el cuarto a las direcciones de host, puede asignar direcciones a 254 redes, con un máximo de 254 hosts en cada red.

Los bits de los bytes de direcciones host que se aplican a las direcciones de subredes y los que se aplican a direcciones host están determinados por una *máscara de subred*. Las máscaras de

subred se utilizan para seleccionar bits de cualquiera de los bytes para utilizar como direcciones de subred. Aunque los bits de máscara de red deben ser contiguos, no es necesario que estén alineados con los límites del byte.

La máscara de red puede aplicarse a una dirección IPv4 utilizando el operador lógico AND en el nivel de bits. Esta operación selecciona las posiciones del número de red y el número de subred de la dirección.

Las máscaras de red se pueden explicar en términos de su representación binaria. Puede utilizar una calculadora para la conversión de binario a decimal. Los ejemplos siguientes muestran los formatos binario y decimal de la máscara de red.

Si se aplica una máscara de red 255 . 255 . 255 . 0 a la dirección IPv4 172 . 16 . 41 . 101, el resultado es la dirección IPv4 de 172 . 16 . 41 . 0 .

172 . 16 . 41 . 101 & 255 . 255 . 255 . 0 = 172 . 16 . 41 . 0

En formato binario, la operación es:

10000001.10010000.00101001.01100101 (dirección IPv4)

y el operador AND con

11111111.11111111.11111111.00000000 (máscara de red)

Ahora el sistema busca un número de red de 172 . 16 . 41 en lugar de 172 . 16. Si la red tiene el número 172 . 16 . 41, dicho número es lo que comprueba y busca el sistema. Dado que puede asignar hasta 254 valores al tercer byte del espacio de dirección IPv4, las subredes permiten crear espacio de dirección para 254 redes, mientras que anteriormente el espacio sólo estaba disponible para una.

Si va a proporcionar espacio de dirección sólo para dos redes adicionales, puede utilizar la siguiente máscara de subred:

255 . 255 . 192 . 0

Esta máscara de red genera el resultado siguiente:

11111111.11111111.11000000.00000000

Este resultado deja 14 bits disponibles para las direcciones host. Dado que todos los 0 y 1 están reservados, deben reservarse como mínimo 2 bits para el número host.

Archivo `/etc/inet/netmasks`

Si la red ejecuta NIS o LDAP, los servidores de estos servicios de nombres guardan las bases de datos `netmasks`. En el caso de las redes que utilizan archivos locales para el servicio de nombres, esta información se guarda en el archivo `/etc/inet/netmasks`.

Nota – Para fines de compatibilidad con los sistemas operativos basados en BSD, el archivo `/etc/netmasks` es un vínculo simbólico a `/etc/inet/netmasks`.

El ejemplo siguiente muestra el archivo `/etc/inet/netmasks` para una red de clase B.

EJEMPLO 10-4 Archivo `/etc/inet/netmasks` para una red de clase B

```
# The netmasks file associates Internet Protocol (IPv4) address
# masks with IPv4 network numbers.
#
#      network-number      netmask
#
# Both the network-number and the netmasks are specified in
# "decimal dot" notation, e.g:
#
#      128.32.0.0      255.255.255.0
192.168.0.0      255.255.255.0
```

Si el archivo `/etc/netmasks` no existe, créelo con un editor de texto. Use la sintaxis siguiente:

network-number netmask-number

Consulte la página del comando `man netmasks(4)` para obtener más información.

Cuando cree números de máscara de red, escriba el número de red asignado por el ISP o el registro de Internet (no el número de subred) y el número de máscara de red en `/etc/inet/netmasks`. Cada máscara de subred debe encontrarse en una línea distinta.

Por ejemplo:

```
128.78.0.0      255.255.248.0
```

También puede escribir nombres simbólicos para los números de red en el archivo `/etc/inet/hosts`. Estos nombres de red pueden utilizarse en lugar de los números de red como parámetros para los comandos.

Daemon de servicios de Internet inetd

El daemon `inetd` inicia los servicios de Internet cuando se inicia un sistema, y puede reiniciar un servicio mientras el sistema está en ejecución. Con la Utilidad de gestión de servicios (SMF), podrá modificar los servicios de Internet estándar o hacer que el daemon `inetd` inicie servicios adicionales.

Utilice los comandos SMF siguientes para administrar los servicios iniciados por el comando `inetd`:

<code>svcadm</code>	Para las acciones de un servicio, como activar, desactivar o reiniciar. Para ver más detalles, consulte la página del comando <code>man svcadm(1M)</code> .
<code>svcs</code>	Para consultar el estado de un servicio. Para ver más detalles, consulte la página del comando <code>man svcs(1)</code> .
<code>inetadm</code>	Para ver y modificar las propiedades de un servicio. Si desea más información, consulte la página del comando <code>man inetadm(1M)</code> .

El valor de campo `proto` del perfil `inetadm` de un servicio específico indica el protocolo de capa de transporte en el que se ejecuta el servicio. Si el servicio está habilitado sólo para IPv4, el campo `proto` debe especificarse como `tcp`, `udp` o `sctp`.

- Para obtener instrucciones sobre el uso de los comandos de SMF, consulte [“Utilidades administrativas de la línea de comandos de la SMF” de Guía de administración del sistema: administración básica](#).
- Para ver una tarea que utilice comandos SMF para agregar un servicio que se ejecute con SCTP, consulte [“Cómo agregar servicios que utilicen el protocolo SCTP” en la página 138](#).
- Para obtener información sobre cómo agregar servicios que manejen solicitudes IPv4 e IPv6, consulte [“Daemon de servicios de Internet inetd” en la página 244](#).

Bases de datos de red y el archivo `nsswitch.conf`

Las bases de datos de red son archivos que proporcionan información necesaria para configurar la red. Son las siguientes:

- `hosts`
- `netmasks`
- Base de datos `ethers`
- `bootparams`
- `protocols`
- `services`
- `networks`

Como parte del proceso de configuración, puede editar las bases de datos `hosts` y `netmasks`, si la red cuenta con subredes. Se utilizan dos bases de datos de red, `bootparams` y `ethers`, para configurar los sistemas como clientes de red. El sistema operativo utiliza las bases de datos restantes, que raramente requieren edición.

Aunque el archivo `nsswitch.conf` no es una base de datos de red, debe configurar este archivo junto con las bases de datos de red pertinentes. El archivo `nsswitch.conf` especifica qué servicio de nombre utilizar para un sistema concreto: archivos locales, NIS, DNS o LDAP.

Cómo afectan los servicios de nombres a las bases de datos de red

El formato de la base de datos de red depende del tipo de servicio de nombres que seleccione para la red. Por ejemplo, la base de datos `hosts` contiene como mínimo el nombre de host y la dirección IPv4 del sistema local, así como cualquier interfaz de red que esté conectada directamente al sistema local. Sin embargo, la base de datos `hosts` puede contener otras direcciones IPv4 y nombres de host, según el tipo de servicio de nombres de la red.

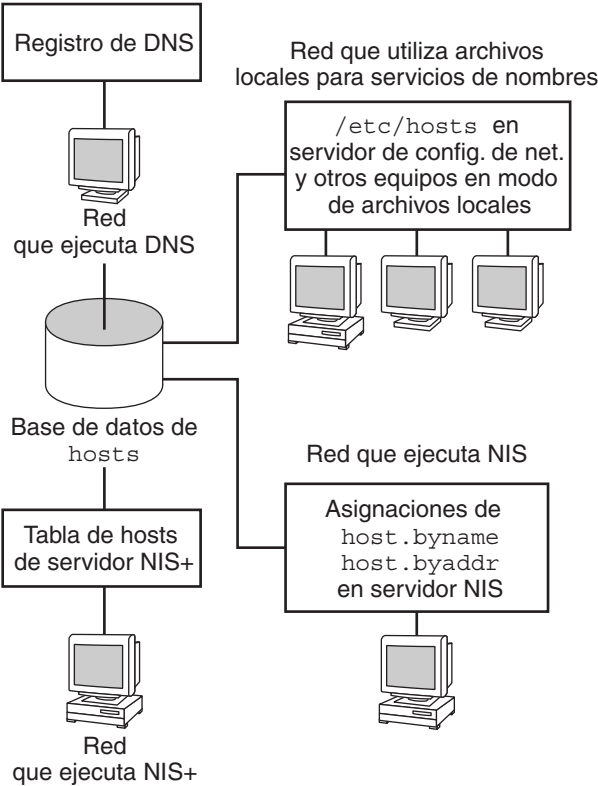
El uso de las bases de datos de red es el siguiente:

- Las redes que utilizan archivos locales para su servicio de nombres dependen de los archivos de los directorios `/etc/inet` y `/etc`.
- NIS utiliza las bases de datos denominadas asignaciones NIS.
- DNS utiliza los registros con la información de host.

Nota – El inicio DNS y los archivos de datos no se corresponden directamente con las bases de datos de red.

La figura siguiente muestra los formatos de la base de datos `hosts` que utilizan estos servicios de nombres.

FIGURA 10-2 Formatos de la base de datos hosts que utilizan los servicios de nombres



La tabla siguiente muestra las bases de datos de red y sus asignaciones NIS y archivos locales correspondientes.

Nota – La base de datos ipnodes se elimina de las versiones de Oracle Solaris a partir de Solaris 10 11/06.

TABLA 10-1 Bases de datos de red y archivos del servicio de nombres correspondiente

Base de datos de red	Archivos locales	Asignaciones NIS
hosts	/etc/inet/hosts	hosts.byaddr hosts.byname
ipnodes	/etc/inet/ipnodes	ipnodes.byaddr ipnodes.byname
netmasks	/etc/inet/netmasks	netmasks.byaddr
ethers	/etc/ethers	ethers.byname ethers.byaddr

TABLA 10-1 Bases de datos de red y archivos del servicio de nombres correspondiente (Continuación)

Base de datos de red	Archivos locales	Asignaciones NIS
bootparams	/etc/bootparams	bootparams
protocols	/etc/inet/protocols	protocols.byname protocols.bynumber
services	/etc/inet/services	services.byname
networks	/etc/inet/networks	networks.byaddr networks.byname

En este manual se describen las bases de datos de red tal como las ven las redes que utilizan archivos locales para los servicios de nombres.

- Encontrará información sobre la base de datos hosts en “[Base de datos hosts](#)” en la [página 235](#).
- Para obtener información sobre la base de datos netmasks, consulte “[Base de datos netmasks](#)” en la [página 240](#).
- En el caso de Solaris 10 11/06 y versiones anteriores, encontrará información sobre la base de datos ipnodes en “[Base de datos ipnodes](#)” en la [página 239](#).

Consulte *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)* para obtener información sobre las correspondencias de bases de datos de red en NIS, DNS y LDAP.

Archivo nsswitch.conf

El archivo /etc/nsswitch.conf define el orden de búsqueda de las bases de datos de red. El programa de instalación de Oracle Solaris crea un archivo /etc/nsswitch.conf predeterminado para el sistema local, basándose en el servicio de nombres que indique durante el proceso de instalación. Si ha seleccionado la opción "None" que indica los archivos locales para el servicio de nombres, el archivo nsswitch.conf resultante será similar al del ejemplo siguiente.

EJEMPLO 10-5 nsswitch.conf para redes utilizando archivos para el servicio de nombres

```
# /etc/nsswitch.files:
#
# An example file that could be copied over to /etc/nsswitch.conf;
# it does not use any naming service.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file contains "switch.so" as a
# nametoaddr library for "inet" transports.

passwd:      files
group:       files
hosts:       files
networks:    files
```

EJEMPLO 10-5 `nsswitch.conf` para redes utilizando archivos para el servicio de nombres
(Continuación)

```
protocols:      files
rpc:            files
ethers:         files
netmasks:      files
bootparams:     files
publickey:      files
# At present there isn't a 'files' backend for netgroup; the
# system will figure it out pretty quickly,
# and won't use netgroups at all.
netgroup:       files
automount:      files
aliases:        files
services:       files
sendmailvars:   files
```

La página del comando `man nsswitch.conf(4)` describe el archivo de manera pormenorizada. A continuación se muestra la sintaxis básica:

base_datos servicio_nombres_para_buscar

El campo *base_datos* puede incluir uno de múltiples tipos de bases de datos en las que busca el sistema operativo. Por ejemplo, el campo puede indicar una base de datos que afecta a los usuarios, como `passwd` o `aliases`, o una base de datos de red. El parámetro *servicio_nombres_para_buscar* puede tener los valores `files`, `nis` o `nis+` para las bases de datos de redes. La base de datos `hosts` también puede tener `dns` como servicio de nombres para buscar. Además, puede enumerar más de un servicio de nombres, como `nis+` y `files`.

En el [Ejemplo 10-5](#), la única opción de búsqueda que se indica es `files`. Por tanto, el sistema local obtiene información de seguridad y montaje automático, además de información de la base de datos de red, a partir de los archivos ubicados en los directorios `/etc` y `/etc/inet`.

Cambio de `nsswitch.conf`

El directorio `/etc` contiene el archivo `nsswitch.conf`, creado por el programa de instalación de Oracle Solaris. Este directorio también contiene archivos de plantilla para los siguientes servicios de nombres:

- `nsswitch.files`
- `nsswitch.nis`

Si desea cambiar de un servicio de nombres a otro, puede copiar la plantilla pertinente en `nsswitch.conf`. También puede editar de forma selectiva el archivo `nsswitch.conf` y cambiar el servicio de nombres predeterminado para buscar bases de datos individuales.

Por ejemplo, en una red que ejecuta NIS, es posible que tenga que cambiar el archivo `nsswitch.conf` en los clientes de red. La ruta de búsqueda de las bases de datos `bootparams` y `ethers` debe enumerar `files` como primera opción, y después `nis`. El ejemplo siguiente muestra las rutas de búsqueda correctas.

EJEMPLO 10-6 nsswitch.conf para un cliente en una red en la que se ejecuta NIS

```
# /etc/nsswitch.conf:#
.
.
passwd:      files nis
group:       files nis

# consult /etc "files" only if nis is down.
hosts:       nis      [NOTFOUND=return] files
networks:    nis      [NOTFOUND=return] files
protocols:   nis      [NOTFOUND=return] files
rpc:         nis      [NOTFOUND=return] files
ethers:       files    [NOTFOUND=return] nis
netmasks:    nis      [NOTFOUND=return] files
bootparams:   files    [NOTFOUND=return] nis
publickey:    nis
netgroup:     nis

automount:    files nis
aliases:      files nis

# for efficient getservbyname() avoid nis
services:     files nis
sendmailvars: files
```

Para más información sobre el cambio de servicio de nombres, consulte [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

Base de datos bootparams

La base de datos bootparams contiene información que utilizan los sistemas configurados para iniciarse en modo de cliente de red. Debe editar esta base de datos si la red tiene clientes de red. Consulte “[Configuración de clientes de red](#)” en la [página 109](#) para conocer los procedimientos. La base de datos se genera a partir de la información que se especifica en el archivo /etc/bootparams.

La página del comando man [bootparams\(4\)](#) contiene la sintaxis completa para esta base de datos. A continuación se muestra la sintaxis básica:

```
nombre_sistema nombre_servidor_claves_archivo:nombre_ruta
```

Para cada sistema cliente de red, la entrada puede contener la información siguiente: el nombre del cliente, una lista de claves, los nombres de los servidores y los nombres de la ruta. El primer elemento de cada entrada es el nombre del sistema cliente. Todos los elementos son opcionales, a excepción del primero. A continuación se muestra un ejemplo.

EJEMPLO 10-7 Base de datos bootparams

```
myclient  root=myserver : /nfsroot/myclient \
swap=myserver : /nfsswap//myclient \
dump=myserver : /nfsdump/myclient
```

En este ejemplo, el término `dump=` indica a los hosts cliente que no deben buscar un archivo de volcado.

Entrada comodín de `bootparams`

En la mayoría de los casos, la entrada comodín se utiliza durante la edición de la base de datos `bootparams` para la compatibilidad con clientes. A continuación, se incluye esta entrada:

```
* root=server:/path dump=:
```

El comodín de asterisco (*) indica que esta entrada se aplica a todos los clientes que no tengan un nombre específico en la base de datos `bootparams`.

Base de datos `ethers`

La base de datos `ethers` se genera a partir de la información que se especifica en el archivo `/etc/ethers`. Esta base de datos asocia los nombres de host a sus direcciones de *control de acceso de soportes* (MAC). Sólo debe crear una base de datos `ethers` si está ejecutando el daemon RARP. En otros términos, esta base de datos debe crearse si está configurando clientes de red.

RARP utiliza el archivo para asignar direcciones MAC a direcciones IP. Si está ejecutando el daemon RARP `in.rarpd`, debe configurar el archivo `ethers` y guardarlo en todos los hosts que estén ejecutando el daemon para que los cambios se reflejen en la red.

La página del comando `man ethers(4)` contiene la sintaxis completa para esta base de datos. A continuación se muestra la sintaxis básica:

MAC-address hostname #comment

dirección_MAC Dirección MAC del host

nombre_host Nombre oficial del host

#comentario Cualquier nota que desee anexas a una entrada del archivo

El fabricante del equipo proporciona la dirección MAC. Si un sistema no muestra la dirección MAC durante el proceso de inicio, consulte los manuales de hardware para obtener información al respecto.

Cuando añada entradas a la base de datos `ethers`, asegúrese de que los nombres de host correspondan a los nombres principales de la base de datos `hosts` y, para Solaris 10 11/06 y versiones anteriores, a los de la base de datos `ipnodes`, no a los apodos, tal como se indica a continuación.

EJEMPLO 10-8 Entradas de la base de datos ethers

```
8:0:20:1:40:16 fayoum
8:0:20:1:40:15 nubian
8:0:20:1:40:7  sahara   # This is a comment
8:0:20:1:40:14 tenere
```

Otras bases de datos de red

Las bases de datos de red restantes raramente deben editarse.

Base de datos networks

La base de datos networks asocia los nombres de red con los números de red, lo cual permite a algunas aplicaciones utilizar y visualizar los nombres en lugar de los números. La base de datos networks se basa en la información del archivo `/etc/inet/networks`. Este archivo contiene los nombres de todas las redes a las que se conecta la red mediante enrutadores.

El programa de instalación de Oracle Solaris configura la base de datos networks inicial. Sin embargo, esta base de datos debe actualizarse si agrega una red nueva a la topología de red existente.

La página del comando `man networks(4)` contiene la sintaxis completa de `/etc/inet/networks`. A continuación se muestra el formato básico:

```
network-name network-number nickname(s) #comment
```

nombre_red Nombre oficial de la red

número_red Número asignado por el ISP o el registro de Internet

apodo Cualquier otro nombre por el que se conozca la red

#comentario Cualquier nota que desee anexar a una entrada del archivo

Debe guardar el archivo `networks`. El programa `netstat` utiliza la información de esta base de datos para producir tablas de estado.

A continuación se incluye un archivo `/etc/networks` de ejemplo.

EJEMPLO 10-9 Archivo `/etc/networks`

```
#ident    "@(#)networks    1.4    92/07/14 SMI"    /* SVr4.0 1.1    */
#
# The networks file associates Internet Protocol (IP) network
# numbers with network names. The format of this file is:
#
#    network-name            network-number            nicnames . . .
#
# The loopback network is used only for intra-machine communication
```

EJEMPLO 10-9 Archivo `/etc/networks` (Continuación)

```
loopback          127

#
# Internet networks
#
arpanet    10      arpa  # Historical
#
# local networks

eng    192.168.9 #engineering
acc    192.168.5 #accounting
prog   192.168.2 #programming
```

Base de datos `protocols`

La base de datos `protocols` enumera los protocolos TCP/IP que están instalados en el sistema y sus números de protocolo. El programa de instalación de Oracle Solaris crea automáticamente la base de datos. Este archivo rara vez requiere administración.

La página del comando `man protocols(4)` describe la sintaxis de esta base de datos. A continuación se incluye un ejemplo del archivo `/etc/inet/protocols`.

EJEMPLO 10-10 Archivo `/etc/inet/protocols`

```
#
# Internet (IP) protocols
#
ip      0   IP      # internet protocol, pseudo protocol number
icmp    1   ICMP    # internet control message protocol
tcp     6   TCP     # transmission control protocol
udp    17   UDP     # user datagram protocol
```

Base de datos `services`

La base de datos `services` enumera los nombres de los servicios TCP y UDP y sus números de puerto conocidos. Los programas que llaman a los servicios de red utilizan esta base de datos. El programa de instalación de Oracle Solaris crea automáticamente la base de datos `services`. Normalmente, esta base de datos no requiere ninguna administración.

La página del comando `man services(4)` contiene información sobre la sintaxis completa. A continuación se incluye un segmento de un archivo `/etc/inet/services` típico.

EJEMPLO 10-11 Archivo `/etc/inet/services`

```
#
# Network services
```

EJEMPLO 10-11 Archivo /etc/inet/services (Continuación)

```
#
echo      7/udp
echo      7/tcp
echo      7/sctp6
discard   9/udp      sink null
discard   11/tcp
daytime   13/udp
daytime   13/tcp
netstat   15/tcp
ftp-data  20/tcp
ftp       21/tcp
telnet    23/tcp
time      37/tcp      timeserver
time      37/udp      timeserver
name      42/udp      nameserver
whois     43/tcp      nickname
```

Protocolos de enrutamiento en Oracle Solaris

Esta sección describe dos protocolos de enrutamiento que admite Oracle Solaris: el Routing Information Protocol (RIP) y el ICMP Router Discovery (RDISC). RIP y RDISC son protocolos TCP/IP estándar. Para ver una lista completa de los protocolos de enrutamiento disponibles para Oracle Solaris, consulte la [Tabla 5-1](#) y la [Tabla 5-2](#).

Protocolo Routing Information Protocol (RIP)

RIP se implementa mediante el daemon de enrutamiento `in.routed`, que se inicia automáticamente al iniciar el sistema. Cuando se ejecuta en un enrutador con la opción `s` especificada, el comando `in.routed` rellena la tabla de enrutamiento del núcleo con una ruta a cada red accesible y comunica la posibilidad de acceso mediante todas las interfaces de red.

Cuando se ejecuta en un host con la opción `q` especificada, `in.routed` extrae la información de enrutamiento pero no comunica las posibilidades de acceso. En los hosts, la información de enrutamiento se puede extraer de dos modos:

- No se especifica el indicador `S` ("`S`" mayúscula: "Modo de ahorro de espacio"). El comando `in.routed` genera una tabla de enrutamiento completa, al igual que en un enrutador.
- Se especifica el indicador `S`. El comando `in.routed` crea una tabla de núcleo mínima, que contiene una única ruta predeterminada para cada enrutador disponible.

Protocolo ICMP Router Discovery (RDISC)

Los hosts utilizan RDISC para obtener información de enrutamiento de los enrutadores. De este modo, cuando los hosts ejecutan RDISC, los enrutadores también deben ejecutar otro protocolo, como RIP, para poder intercambiar información de enrutadores.

RDISC se implementa mediante el comando `in . routed`, que debe ejecutarse tanto en los enrutadores como en los hosts. En los hosts, `in . routed` utiliza RDISC para descubrir las rutas predeterminadas de los enrutadores que se dan a conocer a través de RDISC. En los enrutadores, `in . routed` utiliza RDISC para dar a conocer las rutas predeterminadas a los hosts en las redes conectadas directamente. Consulte las página del comando `man in . routed(1M)` y `gateways(4)`.

Clases de red

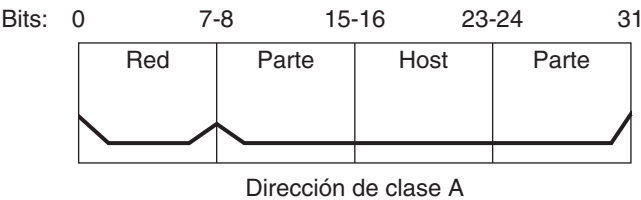
Nota – La IANA ya no pone a disposición los números de red basados en clases, aunque hay muchas redes antiguas que siguen estando basadas en clases.

En esta sección se describen las clases de red IPv4. Cada clase utiliza el espacio de dirección IPv4 de 32 bits de un modo distinto, y proporciona más o menos bits para la parte de red de la dirección. Estas clases son las clases A, B y C.

Números de red de clase A

Un número de red de clase A utiliza los 8 primeros bits de la dirección IPv4 como "parte de red". Los 24 bits restantes contienen la parte de host de la dirección IPv4, tal como muestra la figura siguiente.

FIGURA 10-3 Asignación de bytes en una dirección de clase A

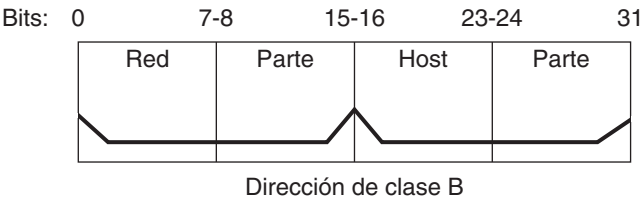


Los valores asignados al primer byte de los números de red de clase A van del 0 al 127. Pongamos como ejemplo la dirección IPv4 75 . 4 . 10 . 4. El valor 75 del primer byte indica que el host se encuentra en una red de clase A. Los bytes restantes, 4 . 10 . 4, establecen la dirección del host. Sólo el primer byte de un número de clase A se registra con la IANA. El uso de los tres bytes restantes se deja a criterio del propietario del número de red. Sólo existen 127 redes de clase A. Cada uno de estos números puede incluir un máximo de 16.777.214 de hosts.

Números de red de clase B

Un número de red de clase B utiliza 16 bits para el número de red y 16 bits para los números de host. El primer byte de un número de red de clase B va del 128 al 191. En el número 172 . 16 . 50 . 56, los dos primeros bytes, 172 . 16, se registran con la IANA, y componen la dirección de red. Los dos últimos bytes, 50 . 56, contienen la dirección de host, y se asignan según el criterio del propietario del número de red. La figura siguiente ilustra una dirección de clase B.

FIGURA 10-4 Asignación de bytes en una dirección de clase B

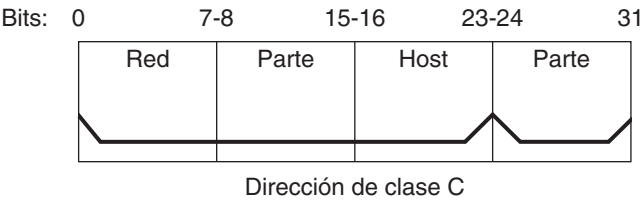


La clase B se asigna típicamente a las organizaciones que tienen varios hosts en sus redes.

Números de red de clase C

Los números de red de clase C utilizan 24 bits para el número de red y 8 bits para los números de host. Los números de red de clase C son adecuados para las redes con pocos hosts, con un máximo de 254 hosts. Un número de red de clase C ocupa los tres primeros bytes de una dirección IPv4. Sólo el cuarto byte se asigna según el criterio de los propietarios de la red. La figura siguiente representa gráficamente los bytes de una dirección de clase C.

FIGURA 10-5 Asignación de bytes en una dirección de clase C



El primer byte de un número de red de clase C va de 192 a 223. El segundo y el tercer byte van de 1 a 255. Una dirección de clase C típica podría ser 192 . 168 . 2 . 5. Los tres primeros bytes, 192 . 168 . 2, forman el número de red. El último byte de este ejemplo, 5, es el número de host.

IPv6 en profundidad (referencia)

Este capítulo proporciona la siguiente información de referencia relativa a la implementación de IPv6 en Oracle Solaris.

- “Formatos de direcciones IPv6 que no son los básicos” en la página 258
- “Formato del encabezado de los paquetes de IPv6” en la página 261
- “Protocolos de pila doble” en la página 263
- “Oracle Solaris implementación de IPv6” en la página 263
- “Protocolo ND de IPv6” en la página 278
- “Encaminamiento de IPv6” en la página 284
- “Túneles de IPv6” en la página 286
- “Extensiones de IPv6 para servicios de nombres de Oracle Solaris” en la página 295
- “Admisión de NFS y RPC IPv6” en la página 297
- “Admisión de IPv6 en ATM” en la página 298

Para obtener una descripción general de IPv6, consulte el [Capítulo 3, “Introducción a IPv6 \(descripción general\)”](#). Para obtener información sobre tareas relativas a la configuración de redes habilitadas para IPv6, consulte el [Capítulo 7, “Configuración de una red IPv6 \(tareas\)”](#).

Novedades de IPv6 en profundidad

En Solaris 10 7/07, el archivo `/etc/inet/ipnodes` pasa a estar obsoleto. Utilice `/etc/inet/ipnodes` únicamente para las versiones anteriores de Oracle Solaris 10, tal como se explica en los procedimientos individuales.

Formatos de direcciones IPv6 que no son los básicos

El [Capítulo 3, “Introducción a IPv6 \(descripción general\)”](#) presenta los formatos más comunes de direcciones IPv6: direcciones de sitios unidifusión y direcciones locales de enlace. Esta sección proporciona descripciones pormenorizadas de formatos de direcciones que se tratan de manera general en el [Capítulo 3, “Introducción a IPv6 \(descripción general\)”](#):

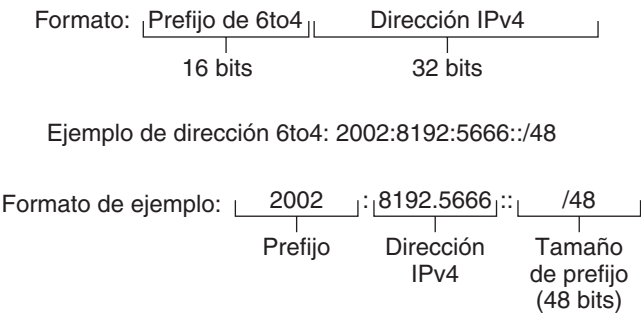
- “Direcciones 6to4 derivadas” en la página 258
- “Direcciones multidifusión IPv6 en profundidad” en la página 260

Direcciones 6to4 derivadas

Si tiene previsto configurar un túnel de 6to4 desde un punto final de enrutador o host, el prefijo de sitio de 6to4 se debe anunciar en el archivo `/etc/inet/ndpd.conf` del sistema de puntos finales. Para obtener una introducción e información sobre tareas relativas a la configuración de túneles de 6to4, consulte [“Cómo configurar un túnel 6to4” en la página 192](#).

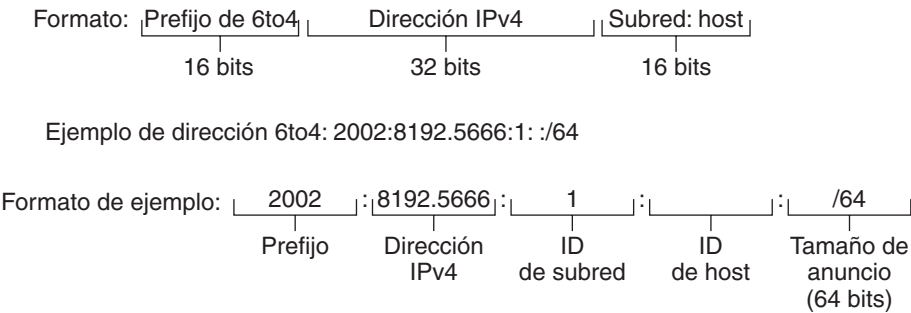
La figura siguiente ilustra las partes que conforman un prefijo de sitio de 6to4.

FIGURA 11-1 Partes de un prefijo de sitio de 6to4



La figura siguiente ilustra las distintas partes de un prefijo de subred de un sitio de 6to4, de la forma que se incluiría en el archivo `ndpd.conf`.

FIGURA 11-2 Partes de un prefijo de subred de 6to4



Esta tabla explica las partes que componen un prefijo de subred de 6to4 y sus respectivas longitudes y definiciones.

Parte	Tamaño	Definición
Prefijo	16 bits	Etiqueta 2002 de prefijo de 6to4 (0x2002).
Dirección IPv4	32 bits	Dirección IPv4 exclusiva que ya se ha configurado en la interfaz de 6to4. En el anuncio, se especifica la representación hexadecimal de la dirección IPv4, en lugar de la representación decimal con punto de IPv4.
ID de subred	16 bits	ID de subred; debe ser un valor exclusivo del vínculo en el sitio de 6to4.

Direcciones 6to4 derivadas en un host

Cuando un host de IPv6 recibe el prefijo de 6to4 derivado mediante un anuncio de enrutador, de forma automática el host vuelve a configurar una dirección 6to4 derivada en una interfaz. La dirección tiene el formato siguiente:

prefix:IPv4-address:subnet-ID:interface-ID/64

La salida del comando `ifconfig -a` en un host con una interfaz de 6to4 tiene un aspecto similar al siguiente:

```
qfe1:3: flags=2180841<UP, RUNNING, MULTICAST, ADDRCONF, ROUTER, IPv6>
    mtu 1500 index 7
        inet6 2002:8192:56bb:9258:a00:20ff:fea9:4521/64
```

En esta salida, la dirección 6to4 derivada sigue a `inet6`.

Esta tabla explica las partes de la dirección derivada 6to4, sus longitudes y la información que proporcionan.

Parte de la dirección	Tamaño	Definición
<i>prefix</i>	16 bits	2002, prefijo de 6to4
<i>dirección_IPv4</i>	32 bits	8192:56bb, dirección IPv4 en notación hexadecimal para la pseudointerfaz de 6to4 que se configura en el enrutador de 6to4
<i>ID de subred</i>	16 bits	9258, dirección de la subred a la que pertenece el host
<i>ID de interfaz</i>	64 bits	a00:20ff:fea9:4521, ID de interfaz de la interfaz de host que se configura para 6to4

Direcciones multidifusión IPv6 en profundidad

La dirección multidifusión IPv6 brinda un método para distribuir los mismos servicios o información a un grupo de interfaces establecido, denominado *grupo de multidifusión*. En general, las interfaces del grupo de multidifusión se encuentran en distintos nodos. Una interfaz puede pertenecer a cualquier cantidad de grupos de multidifusión. Los paquetes que se envían al grupo de multidifusión van a parar a todos los miembros del grupo. Uno de los usos de las direcciones multidifusión consiste en transmitir información, equivalente a la capacidad de la dirección de transmisión IPv4.

En la tabla siguiente se muestra el formato de la dirección multidifusión.

TABLA 11-1 Formato de dirección multidifusión IPv6

8 bits	4 bits	4 bits	8 bits	8 bits	64 bits	32 bits
11111111	<i>INDICS</i>	<i>SCOP</i>	<i>Reservado</i>	<i>Plen</i>	<i>Prefijo de red</i>	<i>ID de grupo</i>

A continuación se resume el contenido de cada campo.

- 11111111: identifica la dirección como dirección multidifusión.
- *FLGS*: conjunto de los cuatro indicadores 0,0,P,T. Los dos primeros deben ser cero. El campo P tiene uno de los valores siguientes:
 - 0 = Dirección multidifusión que no se asigna en función del prefijo de red
 - 1 = Dirección multidifusión que se asigna en función del prefijo de red

Si P se establece en 1, T debe ser también 1.

- *Reservado*: valor reservado de cero.
- *Plen*: cantidad de bits del prefijo de sitio que identifican la subred, para una dirección multidifusión que se asigna a partir de un prefijo de sitio.
- *ID de grupo*: identificador del grupo de multidifusión, ya sea permanente o dinámico.

Para obtener información detallada sobre el formato multidifusión, consulte [RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses \(ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt\)](ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt).

Determinadas direcciones multidifusión IPv6 son asignadas permanentemente por la IANA (Internet Assigned Numbers Authority). Ejemplos son las direcciones multidifusión de todos los nodos y todos los enrutadores multidifusión que necesitan todos los hosts y enrutadores de IPv6. Las direcciones multidifusión IPv6 también se pueden asignar dinámicamente. Para obtener más información sobre el uso adecuado de grupos y direcciones multidifusión, consulte [RFC 3307, Allocation Guidelines for IPv6 Multicast Addresses](#).

Formato del encabezado de los paquetes de IPv6

El protocolo IPv6 define un conjunto de encabezados, que se dividen en básicos y de extensión. La figura siguiente ilustra los campos que tiene un encabezado de IPv6 y el orden en que aparecen.

FIGURA 11-3 Formato de encabezado básico de IPv6

Versión	Clase de tráfico	Etiqueta de flujo	
Tamaño de carga útil		Siguiente encabezado	Límite de salto
Dirección de origen			
Dirección de destino			

En la lista siguiente se describe la función de cada campo de encabezado.

- **Versión:** número de versión de 4 bits del protocolo de Internet = 6.
- **Clase de tráfico:** campo de clase de tráfico de 8 bits.
- **Etiqueta de flujo:** campo de 20 bits.
- **Tamaño de carga útil:** entero sin signo de 16 bits, que representa el resto del paquete que sigue al encabezado de IPv6, en octetos.

- **Encabezado siguiente:** selector de 8 bits. Identifica el tipo de encabezado que va inmediatamente después del encabezado de IPv6. Emplea los mismos valores que el campo de protocolo IPv4.
- **Límite de salto:** entero sin signo de 8 bits. Disminuye en uno cada nodo que reenvía el paquete. El paquete se desecha si el límite de salto se reduce a cero.
- **Dirección de origen:** 128 bits. Dirección del remitente inicial del paquete.
- **Dirección de destino:** 128 bits. Dirección del destinatario previsto del paquete. El destinatario previsto no es necesariamente el destinatario si existe un encabezado de enrutamiento opcional.

Encabezados de extensión de IPv6

Las opciones de IPv6 se colocan en encabezados de extensión independientes que se ubican entre el encabezado de IPv6 y el encabezado de capa de transporte de un paquete. Ningún enrutador procesa ni examina la mayoría de los encabezados de extensión de IPv6 durante el recorrido de distribución del paquete hasta que éste llega a su destino. Esta función supone una mejora importante en el rendimiento de los enrutadores en paquetes que contienen opciones. En IPv4, la presencia de cualquier opción hace que el enrutador examine todas las opciones.

A diferencia de las opciones de IPv4, los encabezados de extensión de IPv6 pueden tener un tamaño arbitrario. Asimismo, la cantidad de opciones que lleva un paquete no se limita a 40 bytes. Aparte de la forma de procesar las opciones de IPv6, esta función permite que las opciones de IPv6 se apliquen a funciones que no resultan viables en IPv4.

Para mejorar el rendimiento al controlar los encabezados de opciones subsiguientes, así como el protocolo de transporte que va después, las opciones de IPv6 siempre son un múltiplo entero de 8 octetos. El múltiplo entero de 8 octetos mantiene la alineación de los encabezados subsiguientes.

Hay definidos los siguientes encabezados de extensión de IPv6:

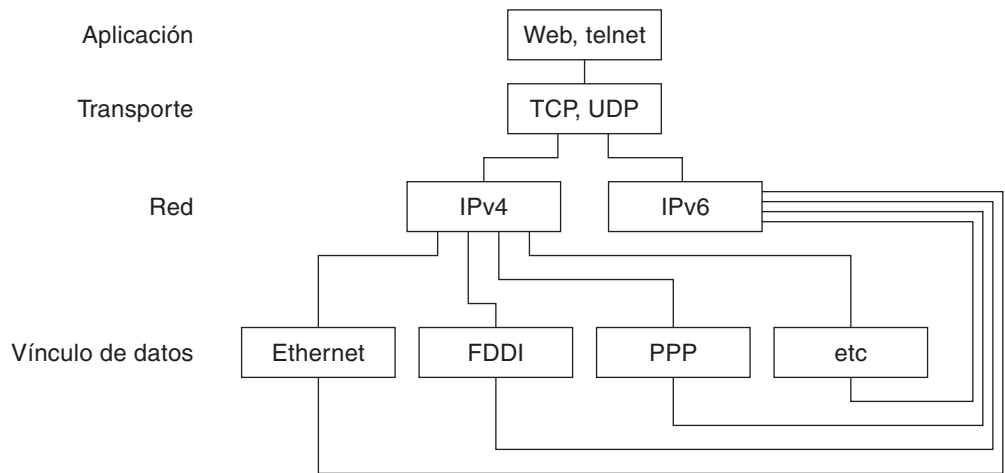
- **Encaminamiento:** enrutamiento extendido, por ejemplo ruta holgada fijada en origen de IPv4
- **Fragmentación:** fragmentación y montaje
- **Autenticación:** integridad y autenticación, y seguridad
- **Encapsulado de carga útil:** confidencialidad
- **Opciones de salto a salto:** opciones especiales que necesitan procesamiento salto a salto
- **Opciones de destino:** información opcional que el nodo de destino debe examinar

Protocolos de pila doble

En general, el término *pila doble* se refiere a una duplicación completa de todos los niveles de la pila de protocolos de aplicaciones en la capa de red. Un ejemplo de duplicación completa es un sistema que ejecuta los protocolos OSI y TCP/IP.

Oracle Solaris es un entorno de *doble pila*: implementa tanto el protocolo IPv4 como el IPv6. Al instalar el sistema operativo, se elige entre habilitar los protocolos IPv6 en la capa de IP o utilizar únicamente los protocolos IPv4 predeterminados. El resto de la pila TCP/IP es idéntica. Por lo tanto, en IPv4 e IPv6 pueden ejecutarse los mismos protocolos de transporte, TCP UDP y SCTP. Además, se pueden ejecutar las mismas aplicaciones. La [Figura 11-4](#) ilustra el funcionamiento de los protocolos IPv4 e IPv6 como pila doble en las distintas capas del conjunto de protocolos de Internet.

FIGURA 11-4 Arquitectura de protocolos de pila doble



En el caso hipotético de pila doble, los subconjuntos de enrutadores y hosts se actualizan para admitir IPv6, además de IPv4. Con este planteamiento de pila doble, los nodos actualizados siempre pueden interoperar con nodos que son sólo de IPv4 mediante IPv4.

Oracle Solaris implementación de IPv6

Esta sección describe los archivos, comandos y daemons que habilitan IPv6 en Oracle Solaris.

Archivos de configuración de IPv6

Esta sección describe los archivos de configuración que forman parte de una implementación de IPv6:

- “Archivo de configuración `ndpd.conf`” en la página 264
- “Archivo de configuración de interfaces de IPv6” en la página 267
- “Archivo de configuración `/etc/inet/ipaddrsel.conf`” en la página 268

Archivo de configuración `ndpd.conf`

El archivo `/etc/inet/ndpd.conf` se utiliza para configurar opciones empleadas por el daemon del protocolo ND in `ndpd`. En el caso de un enrutador, `ndpd.conf` se utiliza sobre todo para configurar el prefijo de sitio que se debe anunciar en el vínculo. En lo que respecta a un host, `ndpd.conf` se usa para desactivar la configuración automática de redes o para configurar direcciones temporales.

La tabla siguiente muestra las palabras clave que se utilizan en el archivo `ndpd.conf`.

TABLA 11-2 Palabras clave de `/etc/inet/ndpd.conf`

Variable	Descripción
<code>ifdefault</code>	Especifica el comportamiento de enrutador en todas las interfaces. Utilice la sintaxis siguiente para establecer los parámetros de enrutador y los valores correspondientes: <code>ifdefault [valor_variable]</code>
<code>prefixdefault</code>	Especifica el comportamiento predeterminado para los anuncios de prefijo. Utilice la sintaxis siguiente para establecer los parámetros de enrutador y los valores correspondientes: <code>prefixdefault [valor_variable]</code>
<code>if</code>	Establece los parámetros según la interfaz. Use la sintaxis siguiente: <code>if interfaz [valor_variable]</code>
<code>prefix</code>	Anuncia información de prefijo según la interfaz. Use la sintaxis siguiente: <code>prefijo prefijo/tamaño interfaz [valor_variable]</code>

En el archivo `ndpd.conf`, las palabras clave de esta tabla se usan con un conjunto de variables de configuración de enrutador. Puede encontrar una definición detallada de estas variables en [RFC 2461, Neighbor Discovery for IP Version 6 \(IPv6\)](http://www.ietf.org/rfc/rfc2461.txt?number=2461) (<http://www.ietf.org/rfc/rfc2461.txt?number=2461>).

En la siguiente tabla aparecen las variables necesarias para configurar una interfaz, junto con breves definiciones.

TABLA 11-3 Variables de configuración de interfaz de `/etc/inet/ndpd.conf`

Variable	Predeterminado	Definición
AdvRetransTimer	0	Especifica el valor del campo RetransTimer en los mensajes de anuncio que envía el enrutador.
AdvCurHopLimit	Diámetro actual de Internet	Especifica el valor que se debe colocar en el límite de salto actual de los mensajes de anuncio que envía el enrutador.
AdvDefaultLifetime	3 + MaxRtrAdvInterval	Especifica la vida útil predeterminada de los anuncios de enrutador.
AdvLinkMTU	0	Especifica el valor de MTU (Maximum Transmission Unit, unidad de transmisión máxima) que debe enviar el enrutador. El cero indica que el enrutador no especifica opciones de MTU.
AdvManaged Flag	Falso	Indica el valor que se debe colocar en el indicador Manage Address Configuration del anuncio de enrutador.
AdvOtherConfigFlag	Falso	Indica el valor que se debe colocar en el indicador Other Stateful Configuration del anuncio de enrutador.
AdvReachableTime	0	Especifica el valor del campo ReachableTime en los mensajes de anuncio que envía el enrutador.
AdvSendAdvertisements	Falso	Indica si el nodo debe enviar anuncios y responder a solicitudes de enrutador. Esta variable se debe establecer en "TRUE" en el archivo <code>ndpd.conf</code> para activar funciones de anuncio de enrutador. Para obtener más información, consulte “Cómo configurar un enrutador habilitado para IPv6” en la página 178 .
DupAddrDetect Transmits	1	Define la cantidad de mensajes consecutivos de solicitudes de vecino que el protocolo ND debe enviar durante la detección de direcciones duplicadas de la dirección del nodo local.
MaxRtrAdvInterval	600 segundos	Especifica el intervalo máximo de tiempo de espera entre el envío de anuncios multidifusión no solicitados.
MinRtrAdvInterval	200 segundos	Especifica el intervalo mínimo de espera entre el envío de anuncios multidifusión no solicitados.
StatelessAddrConf	Verdadero	Controla si el nodo configura su dirección IPv6 mediante la configuración automática de direcciones sin estado. Si en el archivo <code>ndpd.conf</code> se declara False, la dirección se debe configurar manualmente. Para obtener más información, consulte “Cómo configurar un token IPv6 especificado por el usuario” en la página 186 .
TmpAddrsEnabled	Falso	Indica si se debe crear una dirección temporal para todas las interfaces o para una determinada interfaz de un nodo. Para obtener más información, consulte “Cómo configurar una dirección temporal” en la página 183 .

TABLA 11-3 Variables de configuración de interfaz de /etc/inet/ndpd.conf (Continuación)

Variable	Predeterminado	Definición
TmpMaxDesyncFactor	600 segundos	Especifica un valor aleatorio que se debe sustraer de la variable de vida útil preferente TmpPreferredLifetime al iniciarse in.ndpd. La finalidad de la variable TmpMaxDesyncFactor es impedir que todos los sistemas de la red vuelvan a generar sus direcciones temporales al mismo tiempo. TmpMaxDesyncFactor permite modificar el límite superior de ese valor aleatorio.
TmpPreferredLifetime	Falso	Establece la vida útil preferente de una dirección temporal. Para obtener más información, consulte “Cómo configurar una dirección temporal” en la página 183 .
TmpRegenAdvance	Falso	Especifica el tiempo de demora antes de descartar una dirección temporal. Para obtener más información, consulte “Cómo configurar una dirección temporal” en la página 183 .
TmpValidLifetime	Falso	Establece la vida útil válida de una dirección temporal. Para obtener más información, consulte “Cómo configurar una dirección temporal” en la página 183 .

En la siguiente tabla se muestran las variables que se utilizan para configurar prefijos IPv6.

TABLA 11-4 Variables de configuración de prefijo de /etc/inet/ndpd.conf

Variable	Predeterminado	Definición
AdvAutonomousFlag	Verdadero	Especifica el valor que se debe colocar en el campo AutonomousFlag en la opción de información de prefijo.
AdvOnLinkFlag	Verdadero	Especifica el valor que se debe colocar en el campo OnLink ("L-bit") en la opción de información de prefijo.
AdvPreferredExpiration	No establecido	Especifica la fecha de caducidad preferente del prefijo.
AdvPreferredLifetime	604800 segundos	Especifica el valor que se debe colocar en el campo PreferredLifetime en la opción de información de prefijo.
AdvValidExpiration	No establecido	Especifica la fecha de caducidad válida del prefijo.
AdvValidLifetime	2592000 segundos	Especifica la vida útil válida del prefijo que se configura.

EJEMPLO 11-1 Archivo /etc/inet/ndpd.conf

En el ejemplo siguiente se muestra el modo de utilizar las palabras clave y las variables de configuración en el archivo ndpd.conf. Elimine el comentario (#) para activar la variable.

```
# ifdefault      [variable-value ]*
# prefixdefault [variable-value ]*
# if ifname      [variable-value ]*
# prefix prefix/length ifname
```

EJEMPLO 11-1 Archivo `/etc/inet/ndpd.conf` (Continuación)

```
#
# Per interface configuration variables
#
#DupAddrDetectTransmits
#AdvSendAdvertisements
#MaxRtrAdvInterval
#MinRtrAdvInterval
#AdvManagedFlag
#AdvOtherConfigFlag
#AdvLinkMTU
#AdvReachableTime
#AdvRetransTimer
#AdvCurHopLimit
#AdvDefaultLifetime
#
# Per Prefix: AdvPrefixList configuration variables
#
#
#AdvValidLifetime
#AdvOnLinkFlag
#AdvPreferredLifetime
#AdvAutonomousFlag
#AdvValidExpiration
#AdvPreferredExpiration

ifdefault AdvReachableTime 30000 AdvRetransTimer 2000
prefixdefault AdvValidLifetime 240m AdvPreferredLifetime 120m

if qe0 AdvSendAdvertisements 1
prefix 2:0:0:56::/64 qe0
prefix fec0:0:0:56::/64 qe0

if qe1 AdvSendAdvertisements 1
prefix 2:0:0:55::/64 qe1
prefix fec0:0:0:56::/64 qe1

if hme1 AdvSendAdvertisements 1
prefix 2002:8192:56bb:1::/64 qfe0

if hme1 AdvSendAdvertisements 1
prefix 2002:8192:56bb:2::/64 hme1
```

Archivo de configuración de interfaces de IPv6

IPv6 utiliza el archivo `/etc/hostname6.interfaz` al inicio para definir interfaces lógicas de IPv6 de manera automática. Si al instalar Oracle Solaris se elige la opción de habilitar para IPv6, el programa de instalación crea un archivo `/etc/hostname6.interfaz` para la interfaz de red principal, además del archivo `/etc/hostname.interfaz`.

Si durante la instalación se detecta más de una interfaz física, se pregunta al usuario si desea configurar dichas interfaces. El programa de instalación crea archivos de configuración de interfaces físicas de IPv4 e interfaces lógicas de IPv6 para cada interfaz adicional que se especifique.

Al igual que las interfaces de IPv4, las de IPv6 se pueden configurar manualmente, tras instalar Oracle Solaris. El usuario crea archivos `/etc/hostname6.interface` para las nuevas interfaces. Para obtener instrucciones sobre la configuración manual de interfaces, consulte [Capítulo 6, “Administración de interfaces de red \(tarear\)”](#).

Los nombres de archivos de configuración de interfaz de red presentan la sintaxis siguiente:

```
hostname.interface
hostname6.interface
```

La variable *interfaz* presenta la sintaxis siguiente:

```
dev[.module[.module...]]PPA
```

dis Indica un dispositivo de interfaz de red. El dispositivo puede ser una interfaz física de red, por ejemplo `eri` o `qfe`, o una interfaz lógica, por ejemplo un túnel. Para obtener más información, consulte [“Archivo de configuración de interfaces de IPv6” en la página 267](#).

Módulo Presenta uno o varios módulos STREAMS para insertar en el dispositivo cuando dicho dispositivo esté conectado.

PPC Indica el punto físico de conexión.

La sintaxis `[.]` también se acepta.

EJEMPLO 11-2 Archivos de configuración de interfaz de IPv6

A continuación se presentan ejemplos de nombres válidos de archivos de configuración de IPv6:

```
hostname6.qfe0
hostname.ip.tun0
hostname.ip6.tun0
hostname6.ip6to4tun0
hostname6.ip.tun0
hostname6.ip6.tun0
```

Archivo de configuración `/etc/inet/ipaddrsel.conf`

El archivo `/etc/inet/ipaddrsel.conf` contiene la tabla de directrices de selección de direcciones predeterminadas de IPv6. Si Oracle Solaris se instala habilitado para IPv6, este archivo tiene el contenido que se muestra en la [Tabla 11-5](#).

El contenido de `/etc/inet/ipaddrsel.conf` se puede editar. Ahora bien, en la mayoría de los casos no es conveniente modificarlo. Si hace falta realizar cambios, consulte el procedimiento [“Cómo administrar la tabla de directrices de selección de direcciones IPv6” en la página 225](#).

Para obtener más información sobre `ippaddrsel.conf`, consulte [“Motivos para modificar la tabla de directrices de selección de direcciones IPv6” en la página 270](#) y la página de comando `man ippaddrsel.conf(4)`.

Comandos relacionados con IPv6

Esta sección describe comandos que se agregan con la implementación de IPv6 en Oracle Solaris. Asimismo, se especifican las modificaciones realizadas en los comandos para poder admitir IPv6.

Comando `ippaddrsel`

El comando `ippaddrsel` permite modificar la tabla de directrices de selección de direcciones predeterminadas de IPv6.

El núcleo de Oracle Solaris utiliza la tabla de directrices de selección de direcciones predeterminadas de IPv6 para ordenar direcciones de destino y seleccionar direcciones de origen en un encabezado de paquetes de IPv6. El archivo `/etc/inet/ippaddrsel.conf` contiene la tabla de directivas.

En la tabla siguiente se enumeran los formatos de direcciones predeterminadas y las correspondientes prioridades en la tabla de directrices. En la página de comando `man inet6(7P)` hay más información referente a aspectos técnicos sobre la selección de direcciones IPv6.

TABLA 11-5 Tabla de directrices de selección de direcciones IPv6

Prefijo	Prioridad	Definición
::1/128	50	Bucle inverso
::/0	40	Predeterminado
2002::/16	30	6to4
::/96	20	Compatible con IPv4
::ffff:0:0/96	10	IPv4

En esta tabla, los prefijos de IPv6 (`::1/128` y `::/0`) tienen prioridad sobre las direcciones 6to4 (`2002::/16`) y las direcciones IPv4 (`::/96` y `::ffff:0:0/96`). Así pues, de forma predeterminada, el núcleo selecciona la dirección IPv6 global de la interfaz para paquetes que se dirigen a otro destino de IPv6. La dirección IPv4 de la interfaz tiene una prioridad inferior, sobre todo en cuanto a paquetes que se dirigen a un destino de IPv6. A partir de la dirección IPv6 de origen seleccionada, el núcleo también utiliza el formato de IPv6 para la dirección de destino.

Motivos para modificar la tabla de directrices de selección de direcciones IPv6

En la mayoría de los casos, no se necesita cambiar la tabla de directrices de selección de direcciones predeterminadas de IPv6. Para administrar la tabla de directrices, se utiliza el comando `ipaddrsel`.

La tabla de directrices podría modificarse en alguno de los supuestos siguientes:

- Si el sistema tiene una interfaz que se emplea para un túnel de 6to4, puede otorgar mayor prioridad a las direcciones 6to4.
- Si desea utilizar una determinada dirección de origen sólo para comunicarse con una determinada dirección de destino, puede agregar dichas direcciones a la tabla de directrices. A continuación, mediante el comando `ifconfig` etiqueta las direcciones en función de las preferencias.
- Si quiere otorgar más prioridad a las direcciones IPv4 respecto a las de IPv6, la prioridad de `::ffff:0:0/96` puede cambiarse por un número superior.
- Si debe asignar mayor prioridad a direcciones descartadas, tales direcciones se pueden incorporar a la tabla de directrices. Por ejemplo, las direcciones locales de sitio ahora se descartan en IPv6. Estas direcciones tienen el prefijo `fec0::/10`. La tabla de directrices se puede modificar para conceder mayor prioridad a las direcciones locales de sitio.

Para obtener más información sobre el comando `ipaddrsel`, consulte la página de comando [man `ipaddrsel`\(1M\)](#).

Comando 6to4relay

El establecimiento de túneles de 6to4 permite las comunicaciones entre sitios de 6to4 que están aislados. Sin embargo, para transferir paquetes con un sitio de IPv6 nativo que no sea de 6to4, el enrutador de 6to4 debe establecer un túnel con un enrutador de relé de 6to4. Así, el *enrutador de relé de 6to4* reenvía los paquetes de 6to4 a la red IPv6 y, en última instancia, al sitio de IPv6 nativo. Si el sitio habilitado para 6to4 debe intercambiar datos con sitio de IPv6 nativo, utilice el comando `6to4relay` para habilitar el túnel correspondiente.

Como el uso de enrutadores de relé no es seguro, en Oracle Solaris de manera predeterminada se inhabilita el establecimiento de túneles con un enrutador de relé. Antes de implementar esta situación hipotética, debe tener muy en cuenta los problemas que comporta crear un túnel con un enrutador de relé de 6to4. Para obtener más información sobre enrutadores de relé de 6to4, consulte [“Consideraciones para túneles hasta un enrutador de reenvío 6to4” en la página 293](#). Si decide habilitar la admisión de enrutadores de relé 6to4, encontrará los procedimientos en [“Cómo configurar un túnel 6to4” en la página 192](#).

Sintaxis de 6to4relay

El comando `6to4relay` presenta la sintaxis siguiente:

```
6to4relay -e [-a IPv4-address] -d -h
```

- e Habilita el uso de túneles entre el enrutador de 6to4 y un enrutador de relé de 6to4 de difusión por proximidad. Así, la dirección de punto final de túnel se establece en 192.88.99.1, que es la predeterminada para el grupo de difusión por proximidad de enrutadores de relé de 6to4.
- a *dirección_IPv4* Habilita el uso de túneles entre el enrutador de 6to4 y un enrutador de relé de 6to4 con la *dirección_IPv4* que se especifique.
- d Anula la admisión del establecimiento de túneles con el enrutador de relé de 6to4, que es el predeterminado de Oracle Solaris.
- h Muestra la ayuda del comando 6to4relay.

Para obtener más información, consulte la página de comando `man 6to4relay(1M)`.

EJEMPLO 11-3 Pantalla de estado predeterminado de admisión de enrutador de relé de 6to4

El comando `6to4relay`, sin argumentos, muestra el estado actual de la admisión de enrutadores de relé de 6to4. Este ejemplo ilustra el valor predeterminado de la implementación de IPv6 en Oracle Solaris.

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is disabled
```

EJEMPLO 11-4 Pantalla de estado con admisión habilitada de enrutadores de relé de 6to4

Si se habilita la admisión de enrutadores de relé, `6to4relay` muestra la salida siguiente:

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is enabled
IPv4 destination address of Relay Router=192.88.99.1
```

EJEMPLO 11-5 Pantalla de estado con un enrutador de relé de 6to4 especificado

Si se especifica la opción `-a` y una dirección IPv4 en el comando `6to4relay`, en lugar de `-192.88.99.1` se muestra la dirección IPv4 que se proporciona con `a`.

`6to4relay` no indica la ejecución correcta de las opciones de `-dirección_IPv4`, `-d`, `-e` y `a`. Ahora bien, `6to4relay` muestra cualquier mensaje de error que se pudiera generar durante la ejecución de dichas opciones.

Extensiones del comando `ifconfig` para admisión de IPv6

El comando `ifconfig` habilita las interfaces de IPv6 y el módulo de establecimiento de túneles que se debe conectar. `ifconfig` utiliza un conjunto de comandos `ioctl`s ampliado para configurar las interfaces de red IPv4 e IPv6. A continuación se describen las opciones de `ifconfig` que admiten operaciones de IPv6. Consulte [“Supervisión de la configuración de interfaz con el comando `ifconfig`” en la página 205](#) para obtener una serie de tareas de IPv4 e IPv6 que afectan a `ifconfig`.

<code>index</code>	Establece el índice de interfaces.
<code>tsrc/tdst</code>	Establece el origen o destino de túneles.
<code>addif</code>	Crea la siguiente interfaz lógica disponible.
<code>removeif</code>	Elimina una interfaz lógica con una determinada dirección IP.
<code>destination</code>	Establece la dirección de destino punto a punto para una interfaz.
<code>set</code>	Establece una dirección, máscara de red o ambas cosas para una interfaz.
<code>subnet</code>	Establece la dirección de subred de una interfaz.
<code>xmit/-xmit</code>	Habilita o inhabilita la transmisión de paquetes en una interfaz.

En el [Capítulo 7, “Configuración de una red IPv6 \(tareas\)”](#), encontrará procedimientos de configuración de IPv6.

EJEMPLO 11-6 Adición de una interfaz de IPv6 lógica con la opción `-addif` del comando `ifconfig`

La forma siguiente del comando `ifconfig` crea la interfaz lógica `hme0:3`:

```
# ifconfig hme0 inet6 addif up
Created new logical interface hme0:3
```

Esta forma del comando `ifconfig` verifica la creación de la interfaz:

```
# ifconfig hme0:3 inet6
hme0:3: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    inet6 inet6 fe80::203:baff:fe11:b321/10
```

EJEMPLO 11-7 Eliminación de una interfaz de IPv6 lógica con la opción `-removeif` del comando `ifconfig`

La forma siguiente del comando `ifconfig` elimina la interfaz lógica `hme0:3`:

```
# ifconfig hme0:3 inet6 down
# ifconfig hme0 inet6 removeif 1234::5678
```

EJEMPLO 11-8 Uso del comando `ifconfig` para configurar un origen de túneles de IPv6

```
# ifconfig ip.tun0 inet6 plumb index 13
```

Abre el túnel que se debe asociar con el nombre de la interfaz física.

```
# ifconfig ip.tun0 inet6
ip.tun0: flags=2200850<POINTOPOINT,RUNNING,MULTICAST,NUD,
#IPv6> mtu 1480 index 13
    inet tunnel src 0.0.0.0
    inet6 fe80::/10 --> ::
```


EJEMPLO 11-8 Uso del comando `ifconfig` para configurar un origen de túneles de IPv6
(Continuación)

Configura los correspondientes flujos de TCP/IP para utilizar el dispositivo de túneles e informar sobre el estado del dispositivo.

```
# ifconfig ip.tun0 inet6 tsrc 120.46.86.158 tdst 120.46.86.122
```

Configura la dirección de origen y de destino del túnel.

```
# ifconfig ip.tun0 inet6
ip.tun0: flags=2200850<POINTOPOINT,RUNNING,MULTICAST,NUD,
IPv6> mtu 1480 index 13
        inet tunnel src 120.46.86.158 tunnel dst 120.46.86.122
        inet6 fe80::8192:569e/10 --> fe80::8192:567a
```

Informa sobre el nuevo estado del dispositivo tras la configuración.

EJEMPLO 11-9 Configuración de un túnel de 6to4 mediante `ifconfig` (forma completa)

En este ejemplo de configuración de pseudointerfaz de 6to4 se utiliza el ID de subred de 1 y se especifica el ID de host, en forma hexadecimal.

```
# ifconfig ip.6to4tun0 inet6 plumb
# ifconfig ip.6to4tun0 inet tsrc 129.146.86.187 \
2002:8192:56bb:1::8192:56bb/64 up

# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NUD,IPv6>mtu 1480 index 11
        inet tunnel src 129.146.86.187
        tunnel hop limit 60
        inet6 2002:8192:56bb:1::8192:56bb/64
```

EJEMPLO 11-10 Configuración de un túnel de 6to4 mediante `ifconfig` (forma abreviada)

En este ejemplo se muestra la forma abreviada para la configuración de un túnel de 6to4.

```
# ifconfig ip.6to4tun0 inet6 plumb
# ifconfig ip.6to4tun0 inet tsrc 129.146.86.187 up

# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NUD,IPv6>mtu 1480 index 11
        inet tunnel src 129.146.86.187
        tunnel hop limit 60
        inet6 2002:8192:56bb::1/64
```

Modificaciones del comando `netstat` para admitir IPv6

El comando `netstat` muestra el estado de redes IPv4 e IPv6. Puede elegir la información de protocolo que se visualizará; para ello, establezca el valor de `DEFAULT_IP` en el archivo `/etc/default/inet_type` o recurra a la opción de línea de comandos `-f`. Si se aplica un valor

permanente de `DEFAULT_IP`, se garantiza que `netstat` muestre únicamente información relativa a IPv4. Este valor puede anularse mediante la opción `-f`. Para obtener más información sobre el archivo `inet_type`, consulte la página de comando man [inet_type\(4\)](#).

La opción `-p` del comando `netstat` muestra la tabla de red a soporte, que es la tabla ARP para IPv4 y la caché interna para IPv6. Consulte la página de comando man [netstat\(1M\)](#) para obtener más información. Consulte “[Cómo visualizar el estado de los sockets](#)” en la [página 212](#) para obtener descripciones de procedimientos que utilizan este comando.

Modificaciones del comando `snoop` para admitir IPv6

El comando `snoop` puede capturar paquetes de IPv4 e IPv6. Este comando puede mostrar encabezados de IPv6, encabezados de extensiones de IPv6, encabezados de ICMPv6 y datos de protocolo ND. De manera predeterminada, el comando `snoop` muestra paquetes de IPv4 e IPv6. Si especifica la palabra clave de protocolo `ip` o `ip6`, el comando `snoop` muestra sólo paquetes de IPv4 o IPv6, respectivamente. La opción para filtrar IPv6 permite filtrar en todos los paquetes, tanto de IPv4 como IPv6, y mostrar únicamente los paquetes de IPv6. Consulte la página de comando man [snoop\(1M\)](#) para obtener más información. Consulte “[Cómo supervisar tráfico de redes IPv6](#)” en la [página 224](#) para obtener información sobre procedimientos que utilizan el comando `snoop`.

Modificaciones del comando `route` para admitir IPv6

El comando `route` funciona en rutas IPv4 e IPv6; el valor predeterminado son las rutas IPv4. Si la opción `-inet6` de la línea de comandos se utiliza inmediatamente después del comando `route`, las operaciones se llevan a cabo en rutas IPv6. Consulte la página de comando man [route\(1M\)](#) para obtener más información.

Modificaciones del comando `ping` para admitir IPv6

El comando `ping` utiliza protocolos IPv4 e IPv6 para sondear hosts de destino. La selección de protocolo depende de las direcciones que devuelve el servidor de nombres en relación con el host de destino específico. De forma predeterminada, si el servidor de nombres devuelve una dirección IPv6 para el host de destino, el comando `ping` utiliza el protocolo IPv6. Si el servidor devuelve sólo una dirección IPv4, el comando `ping` emplea el protocolo IPv4. Si desea anular esta acción, utilice la opción de línea de comandos `-A` para indicar el protocolo que debe usarse.

Para obtener más información, consulte la página de comando man [ping\(1M\)](#). Para obtener información sobre procedimientos que utilicen el comando `ping`, consulte “[Sondeo de hosts remotos con el comando ping](#)” en la [página 216](#).

Modificaciones del comando `traceroute` para admitir IPv6

El comando `traceroute` efectúa el seguimiento de las rutas IPv4 e IPv6 de un determinado host. En una perspectiva de protocolos, `traceroute` utiliza el mismo algoritmo que `ping`. Si

desea anular esta selección, utilice la opción de línea de comandos `-A`. Puede efectuar el seguimiento de cada ruta en cada dirección de un host con varias direcciones permanentes mediante la opción de línea de comandos `-a`.

Para obtener más información, consulte la página de comando `man traceroute(1M)`. Para obtener información sobre procedimientos que usan el comando `traceroute`, consulte “Visualización de información de enrutamiento con el comando `traceroute`” en la página 220.

Daemons relacionados con IPv6

Esta sección trata sobre los daemons relacionados con IPv6.

Daemon `in.ndpd`, para el protocolo ND

El daemon `in.ndpd` implementa el protocolo ND de IPv6 y el descubrimiento de enrutadores. Asimismo, implementa la configuración automática de direcciones para IPv6. A continuación se muestran las opciones admitidas de `in.ndpd`.

- `-d` Activa la depuración.
- `-D` Activa la depuración para determinados eventos.
- `-f` Especifica un archivo cuyos datos de configuración deban leerse, en lugar del archivo predeterminado `/etc/inet/ndpd.conf`.
- `-I` Imprime información relativa a cada interfaz.
- `-n` No efectúa bucles de retorno de anuncios de enrutador.
- `-r` Hace caso omiso de paquetes recibidos.
- `-v` Especifica el modo detallado; informa de varios tipos de mensajes de diagnóstico.
- `-t` Activa el seguimiento de paquetes.

El daemon `in.ndpd` lo controlan parámetros que se establecen en el archivo de configuración `/etc/inet/ndpd.conf` y los pertinentes parámetros del archivo de inicio de `/var/inet/ndpd_state.interfaz`.

Si existe el archivo `/etc/inet/ndpd.conf`, se analiza y utiliza para configurar un nodo como enrutador. En la [Tabla 11–2](#) figuran las palabras clave válidas que podrían aparecer en este archivo. Si se inicia un host, podría suceder que los enrutadores no estuvieran disponibles de manera inmediata. Los paquetes anunciados por el enrutador podrían perderse. Asimismo, los paquetes anunciados quizá no se comuniquen con el host.

El archivo `/var/inet/ndpd_state.interfaz` es un archivo de estado. Cada nodo lo actualiza periódicamente. Si el nodo falla y se reinicia, el nodo puede configurar sus interfaces si no hay enrutadores. Este archivo contiene las direcciones de interfaz, la última vez que se modificó el

archivo y el tiempo que este archivo será válido. Asimismo, el archivo contiene otros parámetros que se "aprenden" a partir de anteriores anuncios de enrutador.

Nota – No es necesario modificar el contenido de archivos de estado. El daemon `in.ndpd` mantiene los archivos de estado de forma automática.

Consulte las páginas de comando `man in.ndpd(1M)` y `ndpd.conf(4)` para obtener listas de variables de configuración y valores permitidos.

Daemon `in.ripngd`, para enrutamiento de IPv6

El daemon `in.ripngd` implementa el protocolo RIPng (Routing Information Protocol) para enrutadores IPv6. RIPng define el equivalente de IPv6 de RIP. Si se configura un enrutador de IPv6 con el comando `routeadm` y se activa el enrutamiento de IPv6, el daemon `in.ripngd` implementa el protocolo RIPng en el enrutador.

A continuación se muestran las opciones admitidas del protocolo RIPng.

- p *n* *n* especifica el número de puerto alternativo que se usa para enviar o recibir paquetes de RIPng.
- q Suprime información de enrutamiento.
- s Fuerza la información de enrutamiento aun en caso de que el daemon funcione como enrutador.
- P Suprime el uso de valores negativos.
- S Si `in.ripngd` no funciona como enrutador, el daemon especifica sólo un enrutador predeterminado para cada enrutador.

Daemon `inetd` y servicios de IPv6

Una aplicación de servidores habilitada para IPv6 puede asumir solicitudes de IPv4 e IPv6, o únicamente de IPv6. El servidor controla siempre las solicitudes mediante un socket de IPv6. Además, el servidor emplea el mismo protocolo que el del cliente correspondiente. Si desea agregar o modificar un servicio de IPv6, emplee los comandos disponibles en la Utilidad de gestión de servicios (SMF).

- Para obtener información sobre los comandos de SMF, consulte [“Utilidades administrativas de la línea de comandos de la SMF” de Guía de administración del sistema: administración básica](#).
- Para ver una tarea de ejemplo que utilice SMF en la configuración de un manifiesto de servicio de IPv4 que se ejecute en SCTP, consulte [“Cómo agregar servicios que utilicen el protocolo SCTP” en la página 138](#).

Si desea configurar un servicio de IPv6, asegúrese de que el valor del campo `proto` del perfil `inetadm` relativo a ese servicio presente el valor correspondiente:

- Si necesita un servicio que controle solicitudes de IPv4 e IPv6, elija `tcp6`, `udp6` o `sctp`. Un valor de `proto` de `tcp6`, `udp6` o `sctp6` hace que `inetd` pase en un socket de IPv6 al servidor. El servidor contiene una dirección asignada a IPv4 en caso de que un cliente IPv4 tenga una solicitud.
- Si necesita un servicio que únicamente controle solicitudes de IPv6, elija `tcp6only` o `udp6only`. Si se asigna cualquiera de estos valores a `proto`, `inetd` pasa el servidor a un socket de IPv6.

Si reemplaza un comando de Oracle Solaris por otra implementación, compruebe que la implementación de ese servicio admita IPv6. Si la implementación no admite IPv6, el valor de `proto` debe especificarse como `tcp`, `udp` o `sctp`.

A continuación se muestra un perfil generado tras la ejecución de `inetadm` para un manifiesto de servicio `echo` que admite IPv4 e IPv6, y se ejecuta mediante SCTP:

```
# inetadm -l svc:/network/echo:sctp_stream
SCOPE      NAME=VALUE      name="echo"
            endpoint_type="stream"
            proto="sctp6"
            isrpc=FALSE
            wait=FALSE
            exec="/usr/lib/inet/in.echod -s"
            user="root"
default    bind_addr=""
default    bind_fail_max=-1
default    bind_fail_interval=-1
default    max_con_rate=-1
default    max_copies=-1
default    con_rate_offline=-1
default    failrate_cnt=40
default    failrate_interval=60
default    inherit_env=TRUE
default    tcp_trace=FALSE
default    tcp_wrappers=FALSE
```

Si desea cambiar el valor del campo `proto`, aplique la sintaxis siguiente:

```
# inetadm -m FMRI proto="transport-protocols"
```

Todos los servidores que se proporcionan con el software Oracle Solaris necesitan sólo una entrada de perfil que especifique `proto` como `tcp6`, `udp6` o `sctp6`. No obstante, el servidor de shell remoto (`shell`) y el servidor de ejecución remoto (`exec`) se componen en la actualidad de una sola instancia de servicio, que necesita un valor de `proto` que contenga los valores de `tcp` y `tcp6only`. Por ejemplo, para establecer el valor de `proto` para `shell`, debe ejecutarse el comando siguiente:

```
# inetadm -m network/shell:default proto="tcp,tcp6only"
```

Para obtener más información sobre la escritura en servidores habilitados para IPv6 que utilizan sockets, consulte las extensiones de IPv6 de Socket API en la [Programming Interfaces Guide](#).

Puntos que tener en cuenta al configurar un servicio para IPv6

Al agregar o modificar un servicio para IPv6, tenga en cuenta lo siguiente:

- El valor de `proto` debe establecerse en `tcp6`, `sctp6` o `udp6` para permitir conexiones IPv4 o IPv6. Si el valor de `proto` se establece en `tcp`, `sctp` o `udp`, el servicio utiliza sólo IPv4.
- Si bien puede agregar una instancia de servicio que utilice sockets SCTP de uno a varios estilos para `inetd`, no es recomendable. `inetd` no funciona con sockets SCTP de uno a varios estilos.
- Si un servicio necesita dos entradas debido a diferencias en las propiedades de `wait-status` o `exec`, debe crear dos instancias o servicios a partir del servicio original.

Protocolo ND de IPv6

IPv6 introduce el protocolo ND (Neighbor Discovery), tal como se describe en RFC 2461, [Neighbor Discovery for IP Version 6 \(IPv6\)](http://www.ietf.org/rfc/rfc2461.txt?number=2461) (<http://www.ietf.org/rfc/rfc2461.txt?number=2461>). Para obtener una descripción general de las características de este protocolo, consulte “Descripción general del protocolo ND de IPv6” en la página 82.

Esta sección trata sobre las características siguientes del protocolo ND:

- “Mensajes de ICMP del protocolo ND” en la página 278
- “Proceso de configuración automática” en la página 279
- “Solicitud e inasequibilidad de vecinos” en la página 281
- “Algoritmo de detección de direcciones duplicadas” en la página 281
- “Comparación del protocolo ND con ARP y protocolos relacionados con IPv4” en la página 283

Mensajes de ICMP del protocolo ND

El protocolo ND define cinco mensajes nuevos de ICMP (Internet Control Message Protocol). Dichos mensajes tienen los objetivos siguientes:

- **Solicitud de enrutador:** al habilitarse una interfaz, los hosts pueden enviar mensajes de solicitud de enrutador. Se solicita a los enrutadores que generen inmediatamente anuncios de enrutador, en lugar de hacerlo la próxima vez que se hubiera programado.

- **Anuncio de enrutador:** los enrutadores anuncian su presencia, así como varios parámetros de vínculos y de Internet. Los enrutadores anuncian de manera periódica o como respuesta a un mensaje de solicitud de enrutador. Los anuncios de enrutador contienen prefijos que se usan para la determinación de onlinks o configuración de direcciones, un valor de límite de salto propuesto, etcétera.
- **Solicitud de vecino:** los nodos envían mensajes de solicitud de vecino para determinar la dirección de capa de vínculo de un vecino. Los mensajes de solicitud de vecino también sirven para verificar que se pueda contactar con un vecino mediante una dirección de capa de vínculo almacenada en caché. Asimismo, las solicitudes de vecino se usan para detectar direcciones duplicadas.
- **Anuncio de vecino:** un nodo envía mensajes de anuncio de vecino como respuesta a un mensaje de solicitud de vecino. El nodo también puede enviar anuncios de vecino no solicitados para anunciar un cambio de dirección de capa de vínculo.
- **Redirección:** los enrutadores emplean mensajes de redirección para indicar a los hosts el mejor primer salto para acceder a un destino, o para indicar que el destino está en el mismo vínculo.

Proceso de configuración automática

Esta sección proporciona una descripción general de los pasos habituales que realizan las interfaces durante la configuración automática. La configuración automática se efectúa sólo en vínculos que permiten multidifusión.

1. Una interfaz que permite multidifusión se habilita, por ejemplo, al iniciar el sistema de un nodo.
2. El nodo empieza el proceso de configuración automática generando una dirección local de vínculo para la interfaz.

La dirección local de vínculo se forma a partir de la dirección MAC de la interfaz.

3. El nodo envía un mensaje de solicitud de vecino que contiene la dirección local de vínculo provisional como destino.

La finalidad del mensaje es verificar que otro nodo del vínculo no esté utilizando ya la dirección de prueba. Tras verificarla, la dirección local de vínculo puede asignarse a una interfaz.

- a. Si la dirección propuesta ya la usa otro nodo, dicho nodo genera un anuncio de vecino para informar de ello.
- b. Si otro nodo intenta utilizar la misma dirección, dicho nodo también envía una solicitud de vecino para el destino.

La cantidad de transmisiones y retransmisiones de solicitudes de vecino, así como el retraso entre solicitudes consecutivas, dependen de cada vínculo. Si es preciso, establezca estos parámetros.

4. Si un nodo determina que la dirección local de vínculo de prueba no es exclusiva, se detiene el proceso de configuración automática. De ser así, la dirección local de vínculo de la interfaz se debe configurar manualmente.

Para simplificar la recuperación, puede especificar otro ID de interfaz que anule el predeterminado. De este modo, el mecanismo de configuración automática puede reanudar su funcionamiento con el nuevo ID de interfaz, que en principio es exclusivo.

5. Si un nodo determina que la dirección local de vínculo de prueba es exclusiva, el nodo la asigna a la interfaz.

En ese momento, el nodo dispone de conectividad IP con nodos vecinos. Los demás pasos de la configuración automática los efectúan solamente hosts.

Obtención de un anuncio de enrutador

La fase siguiente de la configuración automática consiste en obtener un anuncio de enrutador o determinar que no hay enrutadores. Si hay enrutadores, éstos envían anuncios de enrutador para indicar la clase de configuración automática que debe ejecutar un host.

Los enrutadores envían periódicamente solicitudes de enrutador. No obstante, el retraso entre los sucesivos anuncios suele ser superior a lo que puede esperar un host que efectúa la configuración automática. Para obtener rápidamente un anuncio, el host envía una o varias solicitudes de enrutador al grupo multidifusión de todos los enrutadores.

Variables en la configuración de prefijos

Los anuncios de enrutador pueden contener también variables de prefijo con información que la configuración automática de direcciones emplea en la generación de prefijos. El campo de configuración automática de direcciones sin estado de los anuncios de enrutador se procesa de manera independiente. El indicador de configuración de direcciones, un campo de opción que contiene información de prefijo, indica si la opción se aplica también a la configuración automática sin estado. Si se aplica el campo de opción, otros campos de opciones contienen un prefijo de subred con valores continuamente vigentes. Estos valores indican la duración que tendrán la validez y preferencia de las direcciones creadas a partir del prefijo.

Debido a que los enrutadores generan periódicamente anuncios de enrutador, los hosts reciben anuncios nuevos de manera constante. Los hosts habilitados para IPv6 procesan la información que hay en cada anuncio. Los hosts se agregan a la información. También ponen al día la información recibida en anuncios anteriores.

Exclusividad de las direcciones

Por motivos de seguridad, antes de asignarse a la interfaz debe verificarse que todas las direcciones sean exclusivas. Es distinto en el caso de direcciones creadas con configuración automática sin estado. La exclusividad de una dirección la determina la parte de la dirección

formada por un ID de interfaz. Por eso, si un nodo ya ha comprobado la exclusividad de una dirección local de vínculo, no hace falta verificar las direcciones adicionales una a una. Las direcciones deben crearse a partir del mismo ID de interfaz. Por su parte, debe comprobarse la exclusividad de todas las direcciones que se obtengan manualmente. Los administradores de sistemas de algunos sitios consideran que el esfuerzo y los recursos dedicados a detectar direcciones duplicadas son mayores que sus ventajas. En estos sitios, la detección de direcciones duplicadas se puede inhabilitar estableciendo un indicador de configuración según la interfaz.

Para acelerar el proceso de configuración automática, un host puede generar su propia dirección local de vínculo y verificar su exclusividad, mientras el host espera un anuncio de enrutador. Un enrutador podría retrasar durante unos segundos la respuesta a una solicitud de enrutador. Por lo tanto, el tiempo total que se necesita para completar la configuración automática puede ser considerablemente superior si los dos pasos se realizan en serie.

Solicitud e inasequibilidad de vecinos

El protocolo ND utiliza mensajes de *solicitud de vecino* para determinar si la misma dirección unidifusión tiene asignado más de un nodo. La *detección de inasequibilidad de vecinos* descubre el error de un vecino o de la ruta de reenvío del vecino. Esta clase de detección precisa la confirmación positiva de que los paquetes que se envían a un vecino lleguen realmente a su destino. Asimismo, la detección de inasequibilidad de vecinos determina que la capa IP del nodo procese correctamente los paquetes.

La detección de inasequibilidad de vecinos utiliza la confirmación a partir de dos puntos de referencia: los protocolos de capa superior y los mensajes de solicitud de vecino. Si es posible, los protocolos de capa superior brindan la confirmación positiva de que una conexión *avanza en el reenvío*. Por ejemplo, si se reciben reconocimientos de TCP, se confirma la correcta entrega de los datos enviados con anterioridad.

Si un nodo no obtiene una confirmación positiva de los protocolos de capa superior, dicho nodo envía mensajes de solicitud de vecino unidifusión. Estos mensajes solicitan anuncios de vecino como confirmación de asequibilidad a partir del próximo salto. Para reducir el tráfico redundante en la red, los mensajes sonda se envían sólo a los vecinos a los que el nodo esté enviando paquetes.

Algoritmo de detección de direcciones duplicadas

Para asegurarse de que todas las direcciones configuradas puedan ser exclusivas en un determinado vínculo, los nodos ejecutan en las direcciones un algoritmo de *detección de direcciones duplicadas*. Los nodos deben ejecutar el algoritmo antes de asignar las direcciones a una interfaz. El algoritmo de detección de direcciones duplicadas se ejecuta en todas las direcciones.

El proceso de configuración automática que se describe en esta sección de detección de direcciones duplicadas sólo es válido para hosts, no para enrutadores. Debido a que la configuración automática de hosts emplea información anunciada por enrutadores, éstos se deben configurar por otros medios. Sin embargo, los enrutadores generan direcciones locales de vínculo mediante el mecanismo que se explica en este capítulo. Además, en principio los enrutadores deben superar correctamente el algoritmo de detección de direcciones duplicadas en todas las direcciones antes de asignar la dirección a una interfaz.

Anuncios de proxy

Un enrutador que acepta paquetes de parte de una dirección de destino puede ejecutar anuncios que no se anulan. El enrutador puede aceptar paquetes de parte de una dirección de destino que sea incapaz de responder a solicitudes de destino. En la actualidad no se especifica el uso de proxy. Ahora bien, el anuncio de proxy se puede utilizar para ocuparse de casos como nodos móviles que se han desplazado fuera del vínculo. El uso de proxy no se ha concebido como mecanismo general para controlador nodos que no implementen este protocolo.

Equilibrio de la carga entrante

Los nodos con interfaces duplicadas quizá deban equilibrar la carga de la recepción de paquetes entrantes en las distintas interfaces de red del mismo vínculo. Estos nodos disponen de varias direcciones locales de vínculo asignadas a la misma interfaz. Por ejemplo, un solo controlador de red puede representar a varias tarjetas de interfaz de red como una única interfaz lógica que dispone de varias direcciones locales de vínculo.

El equilibrio de carga se controla permitiendo que los enrutadores omitan la dirección local de vínculo de origen de los paquetes de anuncio de enrutador. Por consiguiente, los vecinos deben emplear mensajes de solicitud de vecino para aprender las direcciones locales de vínculo de los enrutadores. Los mensajes de anuncio de vecino devueltos pueden contener direcciones locales de vínculo diferentes, en función del que haya emitido la solicitud.

Cambio de dirección local de vínculo

Un nodo que sepa que se ha modificado su dirección local de vínculo puede enviar paquetes de anuncios de vecinos multidifusión no solicitados. El nodo puede enviar paquetes multidifusión a todos los nodos para actualizar las direcciones locales de vínculo almacenadas en caché que ya no sean válidas. El envío de anuncios no solicitados es una simple mejora del rendimiento. El algoritmo de detección de inasequibilidad de vecinos se asegura de que todos los nodos descubran la nueva dirección de manera fiable, aunque ello comporte un retraso algo mayor.

Comparación del protocolo ND con ARP y protocolos relacionados con IPv4

El funcionamiento del protocolo ND de IPv6 equivale a combinar los siguientes protocolos de IPv4: ARP (Address Resolution Protocol), ICMP (Internet Control Message Protocol, Router Discovery e ICMP Redirect. IPv4 carece de un protocolo general establecido y de un mecanismo para detectar la inasequibilidad de vecinos. Sin embargo, los requisitos de host especifican determinados algoritmos para la detección de portales inactivos. La detección de portales inactivos es un subconjunto de los problemas que soluciona la detección de inasequibilidad de vecinos.

En la lista siguiente se comparan el protocolo ND con el conjunto correspondiente de protocolos de IPv4.

- El descubrimiento de enrutador forma parte del conjunto básico de protocolos de IPv6. Los hosts de IPv6 no necesitan aplicar el comando snoop a los protocolos de enrutamiento para buscar un enrutador. IPv4 utiliza ARP, descubrimiento de enrutadores ICMP y redirección de ICMP para el descubrimiento de enrutador.
- Los anuncios de enrutador de IPv6 llevan direcciones locales de vínculo. Para resolver la dirección local de vínculo no hace falta un intercambio adicional de paquetes.
- Los anuncios de enrutador llevan los prefijos de sitio para un vínculo. No hace falta un mecanismo aparte para configurar la máscara de red, como sucede con IPv4.
- Los anuncios de enrutador permiten la configuración automática de direcciones. En IPv4 no se implementa la configuración automática.
- El protocolo ND permite que los enrutadores de IPv6 anuncien una MTU (Maximum Transmission Unit, unidad de transmisión máxima) para hosts para utilizarse en el vínculo. Por lo tanto, todos los nodos emplean el mismo valor de MTU en los vínculos que carecen de una MTU bien definida. Podría ser que los hosts de IPv4 de una misma red tuvieran distintas MTU.
- A diferencia de las direcciones de emisión IPv4, las multidifusiones de resolución de direcciones IPv6 se distribuyen en cuatro mil millones (2^{32}) de direcciones multidifusión, lo cual reduce significativamente las interrupciones por resolución de direcciones en nodos que no sean el de destino. Además, no es recomendable interrumpir sistemas que no sean IPv6.
- Las redirecciones de IPv6 contienen la dirección local de vínculo del primer salto nuevo. Al recibir una redirección no hace falta una resolución de direcciones aparte.
- Una misma red IPv6 puede tener asociados varios prefijos de sitio. De forma predeterminada, los hosts aprenden todos los prefijos de sitio locales a partir de anuncios de enrutador. Sin embargo, es posible configurar los enrutadores para que omitan todos o algunos prefijos de anuncios de enrutador. En esos casos, los hosts dan por sentado que los

destinos se encuentran en redes remotas. Por lo tanto, los hosts envían el tráfico a enrutadores. Así pues, un enrutador puede ejecutar redirecciones si es preciso.

- A diferencia de IPv4, el destinatario de un mensaje de redirección de IPv6 da por sentado que el próximo salto nuevo se da en la red local. En IPv4, un host hace caso omiso de los mensajes de redirección que especifiquen un próximo salto que no se ubique en la red local, conforme a la máscara de red. El mecanismo de redirección de IPv6 es análogo a la función XRedirect de IPv4. El mecanismo de redirección es útil en vínculos de soportes compartidos y de no emisión. En esta clase de redes, los nodos no deben comprobar todos los prefijos de destinos de vínculo local.
- La detección de inasequibilidad de vecinos de IPv6 mejora la distribución de paquetes si hay enrutadores que funcionan mal. Esta capacidad mejora la distribución de paquetes en vínculos con particiones o que funcionan parcialmente mal. Asimismo, mejora la distribución de paquetes en nodos que modifican sus direcciones locales de vínculo. Por ejemplo, los nodos móviles pueden salir de la red local sin perder ninguna clase de conectividad debido a memorias caché de ARP que hayan quedado obsoletas. IPv4 carece de método equivalente para la detección de inasequibilidad de vecinos.
- A diferencia de ARP, el protocolo ND detecta errores parciales en vínculos mediante la detección de inasequibilidad de vecinos. El protocolo ND evita el envío de tráfico a vecinos si no existe conectividad bidireccional.
- Las direcciones locales de vínculo permiten la identificación exclusiva de enrutadores y los hosts de IPv6 mantienen las asociaciones de enrutador. La capacidad de identificar enrutadores es necesaria en anuncios de enrutador y mensajes de redirección. Los hosts deben mantener asociaciones de enrutador si el sitio emplea prefijos globales nuevos. IPv4 carece de un método equiparable para la identificación de enrutadores.
- Debido a que los mensajes de protocolo ND tienen un límite de salto de 255 en la recepción, dicho protocolo es inmune a ataques de spoofing provenientes de nodos que no están en el vínculo. Por el contrario, los nodos que no están en vínculos de IPv4 pueden enviar mensajes de redirección de ICMP. Asimismo, los nodos que no están en vínculos de IPv4 pueden enviar mensajes de anuncio de enrutador.
- La colocación de resolución de direcciones en la capa de ICMP hace que el protocolo ND sea más independiente en cuanto a soportes que ARP. por consiguiente, se pueden utilizar la autenticación IP y los mecanismos de seguridad estándar.

Encaminamiento de IPv6

El enrutamiento de IPv6 es casi idéntico al de IPv4 en la dirección de enrutamiento entre dominios sin clase (CIDR). La única diferencia estriba en que las direcciones son IPv6 de 128 bits, en lugar de IPv4 de 32 bits. Con extensiones sumamente sencillas, todos los algoritmos de enrutamiento de IPv4, por ejemplo OSPF, RIP, IDRP e IS-IS, son válidos para enrutar IPv6.

Asimismo, IPv6 incluye extensiones sencillas de enrutamiento que admiten nuevas y potentes posibilidades de enrutamiento. A continuación se describen las nuevas funciones de enrutamiento:

- La selección del proveedor se basa en las directrices, el rendimiento, los costes, etcétera
- Movilidad de los hosts, enrutamiento a la ubicación actual
- Redireccionamiento automático, enrutamiento a la dirección nueva

Para acceder a las nuevas funciones de enrutamiento, debe crear secuencias de direcciones IPv6 que utilicen la opción de enrutamiento de IPv6. Un origen de IPv6 utiliza la opción de enrutamiento para obtener uno o varios nodos intermedios, o un grupo topológico, que debe visitarse en dirección al destino del paquete. Es una función muy parecida a las opciones de ruta de registro y ruta holgada fija en origen de IPv4.

Para que las secuencias de direcciones sean una función general, los hosts de IPv6 deben, en la mayoría de los casos, invertir las rutas de un paquete que reciba un host. El paquete se debe autenticar correctamente mediante el encabezado de autenticación de IPv6. El paquete debe contener secuencias de direcciones para devolver el paquete al emisor. Esta técnica obliga a que las implementaciones de hosts de IPv6 admitan el control y la inversión de las rutas de origen. El control y la inversión de las rutas de origen es la clave que permite a los proveedores trabajar con los hosts que implementan las nuevas funciones de IPv6 como la selección de proveedor y las direcciones extendidas.

Anuncio de enrutador

En vínculos con capacidad multidifusión y punto a punto, cada enrutador envía, de forma periódica, al grupo multidifusión un paquete de anuncios de enrutador que informa de su disponibilidad. Un host recibe anuncios de enrutador de todos los enrutadores, y confecciona una lista de enrutadores predeterminados. Los enrutadores generan anuncios de enrutador con la suficiente frecuencia para que los hosts aprendan su presencia en pocos minutos. Sin embargo, los enrutadores no anuncian con suficiente frecuencia como para que una falta de anuncios permita detectar un error de enrutador. La detección de errores es factible mediante un algoritmo de detección independiente que determina la inasequibilidad de vecinos.

Prefijos de anuncio de enrutador

Los anuncios de enrutador contienen una lista de prefijos de subred que se usan para determinar si un host se encuentra en el mismo vínculo que el enrutador. La lista de prefijos también se utiliza en la configuración de direcciones autónomas. Los indicadores que se asocian con los prefijos especifican el uso concreto de un determinado prefijo. Los hosts utilizan los prefijos del vínculo anunciados para configurar y mantener una lista que se emplea para decidir si el destino de un paquete se encuentra en el vínculo o fuera de un enrutador. Un destino puede

encontrarse en un vínculo aunque dicho destino no aparezca en ningún prefijo del vínculo que esté anunciado. En esos casos, un enrutador puede enviar una redirección. La redirección indica al remitente que el destino es un vecino.

Los anuncios de enrutador, y los indicadores de prefijo, permiten a los enrutadores informar a los hosts sobre cómo efectuar la configuración automática de direcciones sin estado.

Mensajes de anuncio de enrutador

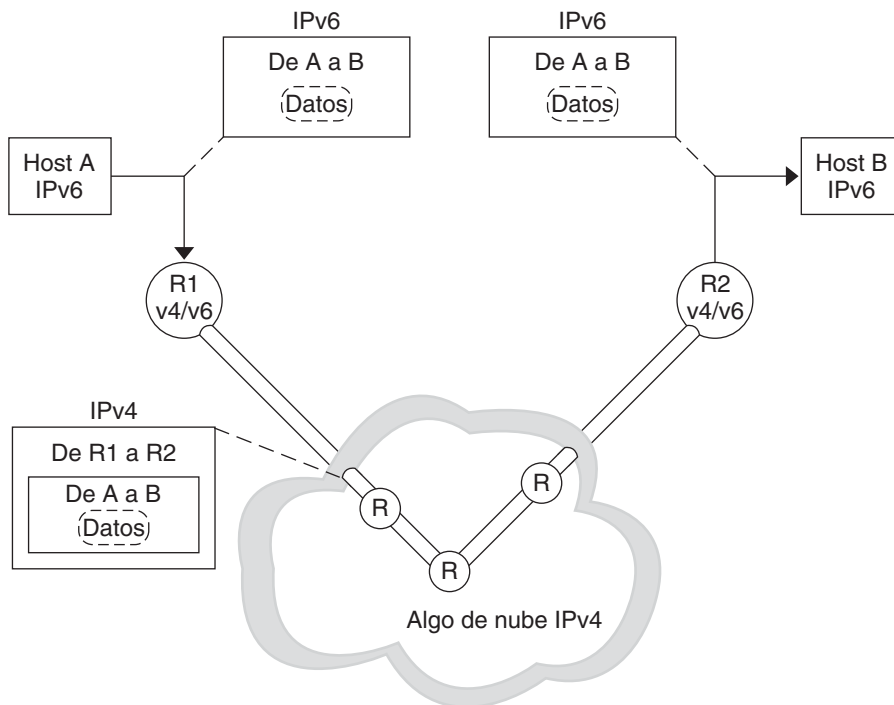
Los mensajes de anuncio de enrutador contienen también parámetros de Internet, por ejemplo el límite de salto que los hosts deben emplear en los paquetes salientes. También es posible que los mensajes de anuncio de enrutador contengan parámetros de vínculo, por ejemplo la MTU de vínculo. Esta función permite la administración centralizada de los parámetros importantes. Los parámetros se pueden establecer en enrutadores y propagarse automáticamente a todos los hosts que estén conectados.

Los nodos llevan a cabo la resolución de direcciones enviando al grupo de multidifusión una solicitud de vecino que pide al nodo de destino que devuelva su dirección de capa de vínculo. Los mensajes de solicitud de vecino multidifusión se envían a la dirección multidifusión de nodo solicitado de la dirección de destino. El destino devuelve su dirección de capa de vínculo en un mensaje de anuncio de vecino unidifusión. Para que el iniciador y el destino resuelvan sus respectivas direcciones de capa de vínculo basta con un solo par de paquetes de solicitud-respuesta. El iniciador incluye su dirección de capa de vínculo en la solicitud de vecino.

Túneles de IPv6

Para minimizar las dependencias en una sitio de IPv4/IPv6 de doble pila, todos los enrutadores de la ruta entre dos nodos IPv6 no necesitan ser compatibles con IPv6. El mecanismo que admite esta clase de configuración en red se denomina *colocación en túneles*. Básicamente, los paquetes de IPv6 se colocan en paquetes de IPv4, que luego se enrutan a través de enrutadores de IPv4. La figura siguiente ilustra el mecanismo de colocación en túneles mediante enrutadores de IPv4, cosa que en la figura se señala mediante una R.

FIGURA 11-5 Mecanismo de colocación en túneles de IPv6



La implementación de IPv6 en Oracle Solaris incluye dos clases de mecanismos de colocación en túneles:

- Túneles configurados entre dos enrutadores, como en la [Figura 11-5](#)
- Túneles automáticos que terminan en los hosts de punto final

Un túnel configurado se utiliza actualmente en Internet para otras finalidades, por ejemplo en MBONE, el núcleo multidifusión de IPv4. Desde un punto de vista operativo, el túnel se compone de dos enrutadores que se configuran para tener un vínculo punto a punto virtual entre los dos enrutadores en la red IPv4. Es probable que esta clase de túnel se utilice en Internet en un futuro previsible.

Los túneles automáticos necesitan direcciones compatibles con IPv4. Los túneles automáticos se pueden utilizar para conectar con IPv6 cuando no estén disponibles los enrutadores de IPv6. Estos túneles se pueden originar en un host de pila doble o un enrutador de pila doble configurando una interfaz de red de colocación automática en túneles. Los túneles siempre terminan en el host de pila doble. Estos túneles funcionan determinando dinámicamente la dirección IPv4 de destino, que es el punto final del túnel, extrayendo la dirección de la dirección de destino compatible con IPv4.

Túneles configurados

Las interfaces colocadas en túneles tienen el siguiente formato:

```
ip.tun ppa
```

ppa es el punto físico de conexión.

Al iniciar el sistema, se conecta remotamente con el módulo de colocación en túneles (tun) mediante el comando `ifconfig`, en la parte superior de IP para crear una interfaz virtual. La conexión remota se lleva a cabo creando el correspondiente archivo `hostname6.*`.

Por ejemplo, para crear un túnel con el fin de encapsular paquetes de IPv6 en una red IPv4, IPv6 sobre IPv4, debe crear el siguiente nombre de archivo:

```
/etc/hostname6.ip.tun0
```

El contenido de este archivo se pasa a `ifconfig` tras la conexión de las interfaces. El contenido se convierte en los parámetros que se necesitan para configurar un túnel de extremo a extremo.

EJEMPLO 11-11 Archivo `hostname6.ip.tun0` para un túnel IPv6 sobre IPv4

A continuación se muestra un ejemplo de entradas para el archivo `hostname6.ip.tun0`:

```
tsrc 10.10.10.23 tdst 172.16.7.19 up
addif 2001:db8:3b4c:1:5678:5678::2 up
```

En este ejemplo, las direcciones IPv4 de origen y destino se usan como tokens para configurar automáticamente direcciones IPv6 locales de vínculo. Estas direcciones son el origen y destino de la interfaz `ip.tun0`. Se configuran dos interfaces. Se configura la interfaz `ip.tun0`. También se configura una interfaz lógica `ip.tun0:1`. La interfaz lógica tiene las direcciones IPv6 de origen y destino especificadas mediante el comando `addif`.

El contenido de estos archivos de configuración se pasa al comando `ifconfig` sin modificarse cuando el sistema se inicia en modo multiusuario. Las entradas del [Ejemplo 11-11](#) equivalen a lo siguiente:

```
# ifconfig ip.tun0 inet6 plumb
# ifconfig ip.tun0 inet6 tsrc 10.0.0.23 tdst 172.16.7.19 up
# ifconfig ip.tun0 inet6 addif 2001:db8:3b4c:1:5678:5678::2 up
```

A continuación se muestra la salida del comando `ifconfig -a` para este túnel.

```
ip.tun0: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,
    NONUD,IPv6> mtu 1480 index 6
    inet tunnel src 10.0.0.23 tunnel dst 172.16.7.19
    inet6 fe80::c0a8:6417/10 --> fe80::c0a8:713
ip.tun0:1: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,NONUD,IPv6> mtu 1480
```



```
index 5
    inet6 2001:db8:3b4c:1:5678:5678::2
```

Para configurar más interfaces lógicas, agregue líneas al archivo de configuración. Para ello, utilice la siguiente sintaxis:

```
addif IPv6-source IPv6-destination up
```

Nota – Si cualquiera de los extremos del túnel es un enrutador de IPv6 que anuncia uno o varios prefijos a través del túnel, los comandos `addif` no se necesitan en los archivos de configuración de túneles. Es posible que sólo hagan falta `tsrc` y `tdst` debido a que todas las demás direcciones se configuran automáticamente.

En algunas circunstancias, determinadas direcciones locales de vínculo de origen y destino se deben configurar manualmente para un túnel en concreto. Para incluir estas direcciones locales de vínculo, cambie la primera línea del archivo de configuración. La línea siguiente es a modo de ejemplo:

```
tsrc 10.0.0.23 tdst 172.16.7.19 fe80::1/10 fe80::2 up
```

Tenga en cuenta que la longitud del prefijo de la dirección local de vínculo de origen es de 10. En este ejemplo, la interfaz `ip.tun0` tiene un aspecto parecido al siguiente:

```
ip.tun0: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,NUD,IPv6> mtu 1480
index 6
    inet tunnel src 10.0.0.23 tunnel dst 172.16.7.19
    inet6 fe80::1/10 --> fe80::2
```

Para crear un túnel con el fin de encapsular paquetes de IPv6 en una red IPv6, IPv6 sobre IPv6, debe crear el siguiente nombre de archivo:

```
/etc/hostname6.ip6.tun0
```

EJEMPLO 11-12 Archivo `hostname6.ip6.tun0` para un túnel IPv6 sobre IPv6

A continuación se muestra un ejemplo de entradas del archivo `hostname6.ip6.tun0` para encapsulado de IPv6 en una red IPv6:

```
tsrc 2001:db8:3b4c:114:a00:20ff:fe72:668c
    tdst 2001:db8:15fa:25:a00:20ff:fe9b:a1c3
fe80::4 fe80::61 up
```

Para crear un túnel con el fin de encapsular paquetes de IPv4 en una red IPv6, IPv4 sobre IPv6, debe crear el siguiente nombre de archivo:

```
/etc/hostname.ip6.tun0
```

EJEMPLO 11-13 Archivo `hostname.ip6.tun0` para un túnel IPv4 sobre IPv6

A continuación se muestra un ejemplo de entradas del archivo `hostname6.ip6.tun0` para encapsulado de IPv4 en una red IPv6:

```
tsrc 2001:db8:3b4c:114:a00:20ff:fe72:668c
      tdst 2001:db8:15fa:25:a00:20ff:fe9b:a1c3
10.0.0.4 10.0.0.61 up
```

Para crear un túnel con el fin de encapsular paquetes de IPv4 en una red IPv6, IPv4 sobre IPv4, debe crear el siguiente nombre de archivo:

```
/etc/hostname.ip.tun0
```

EJEMPLO 11-14 Archivo `hostname.ip.tun0` para un túnel IPv4 sobre IPv4

A continuación se muestra un ejemplo de entradas del archivo `hostname.ip.tun0` para encapsulado de IPv4 en una red IPv4:

```
tsrc 172.16.86.158 tdst 192.168.86.122
10.0.0.4 10.0.0.61 up
```

Para obtener información sobre `tun`, consulte la página de comando `man tun(7M)`. Para obtener una descripción general sobre los conceptos de la colocación en túneles de IPv6, consulte [“Descripción general sobre los túneles de IPv6” en la página 85](#). Para obtener una descripción sobre los procedimientos que seden realizar para configurar túneles, consulte [“Tareas de configuración de túneles para compatibilidad con IPv6 \(mapa de tareas\)” en la página 189](#).

Túneles automáticos 6to4

Oracle Solaris incluye túneles 6to4 como método provisional preferido para realizar la transición de direcciones IPv4 a IPv6. Los túneles 6to4 permiten que ubicaciones IPv6 aisladas se comuniquen mediante un túnel automático a través de una red IPv4 que no admite IPv6. Para utilizar túneles 6to4 debe configurar un enrutador de límite de sistema en la red IPv6 como un punto final del túnel automático 6to4. Después, el enrutador 6to4 puede participar en un túnel hasta otra ubicación 6to4, o, si es necesario, hasta un ubicación IPv6 nativa, no 6to4.

Esta sección proporciona material de referencia sobre los siguientes temas 6to4:

- Configuración de un túnel 6to4
- Direcciones 6to4, incluido el formato del anuncio
- Descripción del flujo de paquetes a través de un túnel 6to4
- Configuración de un túnel entre un enrutador 6to4 y un enrutador de reenvío 6to4

- Puntos que considerar antes de configurar la compatibilidad con enrutador de reenvío 6to4

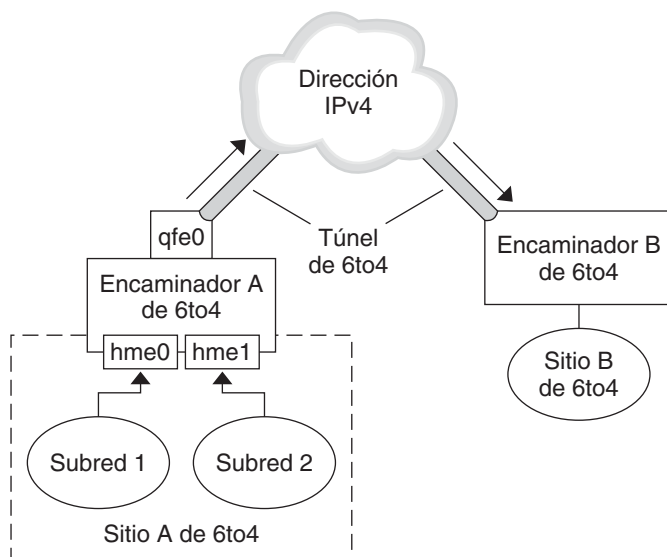
La tabla siguiente describe tareas adicionales para configurar túneles 6to4 y los recursos para obtener información adicional útil.

Tarea o detalle	Para obtener información
Tareas para configurar un túnel 6to4	“Cómo configurar un túnel 6to4” en la página 192
RCF relacionado con 6to4	RFC 3056, "Connection of IPv6 Domains via IPv4 Clouds" (http://www.ietf.org/rfc/rfc3056.txt)
Información detallada sobre el comando 6to4relay, que permite utilizar túneles hasta un enrutador de reenvío 6to4	6to4relay(1M)
Cuestiones de seguridad de 6to4	Security Considerations for 6to4 (http://www.ietf.org/rfc/rfc3964.txt)

Configuración de un túnel 6to4

Un túnel 6to4 proporciona conectividad IPv6 a todas las ubicaciones 6to4 en cualquier parte. Asimismo, el túnel ejerce como vínculo con todas las ubicaciones IPv6, incluida Internet IPv6 nativa, siempre que el enrutador se configure para reenviar a un enrutador de repetición. La figura siguiente ilustra la forma en que un túnel 6to4 proporciona esta clase de conectividad entre sitios 6to4.

FIGURA 11-6 Túnel entre dos ubicaciones 6to4



La figura muestra dos redes 6to4 independientes, Site A y Site B. Cada ubicación tiene configurado un enrutador con una conexión externa a una red IPv4. Un túnel 6to4 en la red IPv4 proporciona una conexión para vincular ubicaciones 6to4.

Antes de que una ubicación IPv6 pueda convertirse en 6to4, debe configurar al menos una interfaz de enrutador para que admite 6to4. Esta interfaz debe proporcionar la conexión externa a la red IPv4. La dirección configurada en `qfe0` debe ser única globalmente. En esta figura, la interfaz `qfe0` del enrutador de límite de sistema Router A conecta la ubicación Site A con la red IPv4. La interfaz `qfe0` ya debe estar configurada con una dirección IPv4 antes de que sea posible configurar `qfe0` como una pseudointerfaz 6to4.

En la figura, la ubicación 6to4 Site A está compuesta de dos subredes, que están conectadas a las interfaces `hme0` y `hme1` del enrutador Router A. Todos los hosts IPv6 de ambas subredes de la ubicación Site A se reconfiguran automáticamente con direcciones derivadas 6to4 al recibir el anuncio del enrutador Router A.

La ubicación Site B es otra ubicación 6to4 aislada. Para recibir correctamente tráfico de la ubicación Site A, se debe configurar un enrutador de límite en la ubicación Site B para admitir 6to4. De no ser así, los paquetes que reciba el enrutador de Site A no se reconocen y se descartan.

Flujo de paquetes a través del túnel 6to4

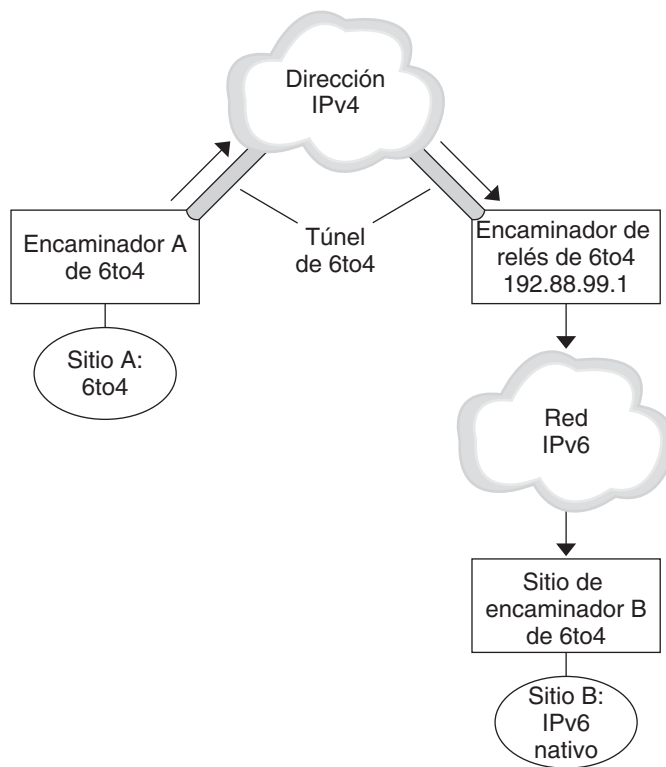
Esta sección describe el flujo de paquetes entre un hosts en una ubicación 6to4 y un host en una ubicación 6to4 remota. Esta situación hipotética utiliza la topología de la [Figura 11-6](#). En el ejemplo se considera que los enrutadores y hosts 6to4 ya están configurados.

1. Un host en la subred 1 (Subnet 1) de la ubicación 6to4 Site A envía una transmisión, con un host de la ubicación 6to4 Site B como destino. El encabezado de cada paquete tiene una dirección de origen derivada de 6to4 y una dirección de destino derivada de 6to4.
2. El enrutador de la ubicación Site A encapsula cada paquete 6to4 dentro de un encabezado IPv4. En este proceso, el enrutador establece la dirección IPv4 de destino del encabezado de encapsulado en la dirección de enrutador de la ubicación Site B. En cada paquete de IPv6 que pasa por la interfaz de túnel, la dirección de destino de IPv6 también contiene la dirección de destino de IPv4. De este modo, el enrutador puede determinar la dirección IPv4 de destino que se establece en el encabezado de encapsulado. Después, el enrutador utiliza procedimientos estándar IPv4 para reenviar los paquetes a través de la red IPv4.
3. Cualquier enrutador IPv4 que encuentren los paquetes en su camino utilizará la dirección de destino IPv4 del paquete para reenviarlo. Esta dirección es la dirección IPv4 globalmente única de la interfaz del enrutador Router B, que también funciona como pseudo-interfaz 6to4.
4. Los paquetes de Site A llegan al enrutador Router B, que desencapsula los paquetes IPv6 del encabezado IPv4.
5. A continuación, Router B utiliza la dirección de destino del paquete IPv6 para reenviar los paquetes al receptor en Site B.

Consideraciones para túneles hasta un enrutador de reenvío 6to4

Los enrutadores de reenvío 6to4 funcionan como puntos finales para túneles desde enrutadores 6to4 que necesitan comunicarse con redes IPv6 nativas, no 6to4. Los enrutadores de reenvío son básicamente puentes entre la ubicación 6to4 y ubicaciones IPv6 nativas. Debido a que esta solución puede llegar a ser muy insegura, Oracle Solaris no tiene la admisión de enrutadores 6to4 habilitada. No obstante, si es necesario establecer un túnel de este tipo en su ubicación, puede utilizar el comando `6to4relay` para activar la situación hipotética siguiente de creación de túneles.

FIGURA 11-7 Túnel desde una ubicación 6to4 hasta un enrutador de reenvío 6to4



En la [Figura 11-7](#), la ubicación 6to4 Site A necesita comunicarse con un nodo en la ubicación IPv6 nativa Site B. La figura muestra la ruta de tráfico desde Site A hasta un túnel 6to4 a través de una red IPv4. Los puntos finales del túnel son el enrutador 6to4 Router A y un enrutador de reenvío 6to4. Más allá del enrutador de reenvío 6to4 se encuentra la red IPv6, a la que está conectada la ubicación IPv6 Site B.

Flujo de paquetes entre una ubicación 6to4 y una ubicación IPv6 nativa

En esta sección se describe el flujo de paquetes desde una ubicación 6to4 hasta una ubicación IPv6 nativa. Esta situación hipotética utiliza la topología de la [Figura 11-7](#).

1. Un host en la ubicación 6to4 Site A envía una transmisión que especifica como destino un host en la ubicación IPv6 nativa Site B. El encabezado de cada paquete tiene una dirección derivada 6to4 como dirección de destino. La dirección de destino es una dirección IPv6 estándar.

2. El enrutador 6to4 de la ubicación Site A encapsula cada paquete dentro de un encabezado IPv4, que tiene la dirección IPv4 del enrutador de reenvío 6to4 como destino. El enrutador 6to4 utiliza procedimientos IPv4 estándar para reenviar el paquete a través de la red IPv4. Cualquier enrutador IPv4 que encuentren los paquetes en su camino los reenviará al enrutador de reenvío 6to4.
3. El enrutador de reenvío 6to4 de difusión por proximidad más cercano físicamente a la ubicación Site A recibe los paquetes destinados al grupo de difusión por proximidad 192 . 88 . 99 . 1.

Nota – Los enrutadores de reenvío 6to4 que forman parte del grupo de difusión por proximidad de enrutador de reenvío 6to4 tienen la dirección IP 192 . 88 . 99 . 1. Esta dirección de difusión por proximidad es la dirección predeterminada de enrutadores de reenvío 6to4. Si necesita utilizar un enrutador de reenvío 6to4 específico, puede anular la dirección predeterminada y especificar la dirección IPv4 del enrutador.

4. El enrutador de reenvío desencapsula el encabezado IPv4 de los paquetes 6to4 y, de este modo, revela la dirección de destino IPv6 nativa.
5. A continuación, el enrutador de reenvío envía los paquetes, que ahora son sólo IPv6, a la red IPv6, donde los recibe un enrutador de la ubicación Site B. El enrutador reenvía los paquetes al nodo IPv6 de destino.

Extensiones de IPv6 para servicios de nombres de Oracle Solaris

En esta sección se describen los cambios de denominación incorporados con la implementación de IPv6. Puede almacenar direcciones IPv6 en cualquiera de los servicios de nombres de Oracle Solaris, NIS, LDAP, DNS y archivos. También puede utilizar NIS en transportes IPv6 RPC para recuperar datos de NIS.

Extensiones de DNS para IPv6

El registro de recursos AAAA, propio de IPv6, se ha especificado en la RFC 1886 *DNS Extensions to Support IP Version 6*. Este registro AAAA asigna un nombre de host en una dirección IPv6 de 128 bits. El registro PTR se sigue usando en IPv6 para asignar direcciones IP en nombres de host. Las cuatro porciones de 32 bits de las direcciones de 128 bits se invierten para una dirección IPv6. Cada porción se convierte a su correspondiente valor ASCII hexadecimal. A continuación, se agrega `ip6.int`.

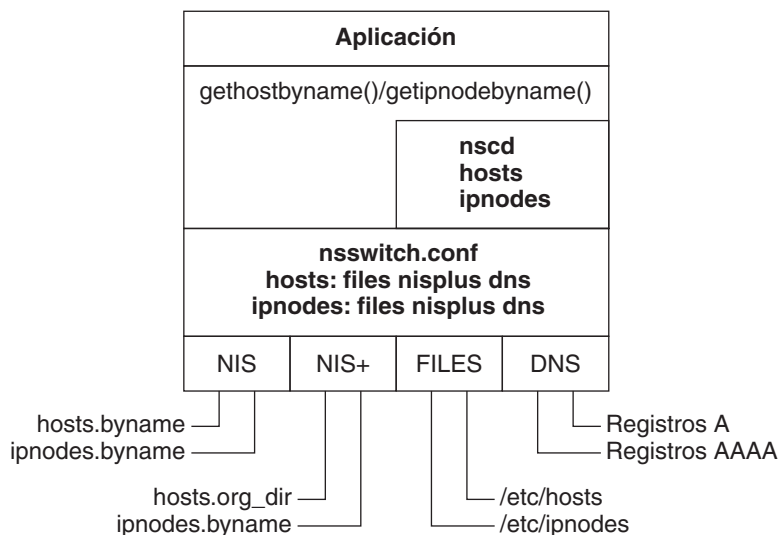
Cambios en el archivo `nsswitch.conf`

En Solaris 10 11/06 y versiones anteriores, aparte de poder buscar direcciones IPv6 mediante `/etc/inet/ipnodes`, se ha incorporado la admisión de IPv6 a los nombres de servicios DNS, NIS y LDAP. En consecuencia, se ha modificado el archivo `nsswitch.conf` para poder realizar búsquedas de IPv6.

```
hosts:  files dns nisplus [NOTFOUND=return]
ipnodes: files dns nisplus [NOTFOUND=return]
```

Nota – Antes de cambiar el archivo `/etc/nsswitch.conf` para buscar `ipnodes` en varios servicios de nombres, debe rellenar estas bases de datos de `ipnodes` con direcciones IPv4 e IPv6. De lo contrario, pueden darse retrasos innecesarios en la resolución de direcciones de host, incluso en el momento del inicio.

El diagrama siguiente ilustra la relación nueva entre el archivo `nsswitch.conf` y las nuevas bases de datos de servicios de nombres para aplicaciones que utilizan los comandos `gethostbyname` y `getipnodebyname`. Los términos en cursiva son nuevos. El comando `gethostbyname` comprueba únicamente las direcciones IPv4 almacenadas en `/etc/inet/hosts`. En Solaris 10 11/06 y versiones anteriores, el comando `getipnodebyname` consulta la base de datos que se indica en la entrada `ipnodes` del archivo `nsswitch.conf`. Si falla la búsqueda, el comando comprueba la base de datos que se indica en la entrada `hosts` del archivo `nsswitch.conf`.

FIGURA 11-8 Relación entre `nsswitch.conf` y los servicios de nombres

Para obtener más información acerca de los servicios de nombres, consulte la [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

Cambios en los comandos de servicio de nombres

Para admitir IPv6, busque direcciones IPv6 con los comandos del servicio de nombres vigente. Por ejemplo, el comando `ypmatch` funciona con las nuevas asignaciones NIS. El comando `nslookup` busca los nuevos registros AAAA en DNS.

Admisión de NFS y RPC IPv6

NFS y Remote Procedure Call (RPC) son programas totalmente compatibles con IPv6. No han cambiado los comandos ya existentes relacionados con los servicios de NFS. Además, la mayoría de las aplicaciones RPC también funcionan con IPv6 sin cambios. Es posible que haya que actualizar algunas aplicaciones RPC avanzadas con reconocimiento de transporte.

Admisión de IPv6 en ATM

Oracle Solaris admite IPv6 en ATM, PVC (Permanent Virtual Circuits, circuitos virtuales permanentes) y SVC (Static Switched Virtual Circuits, circuitos virtuales conmutados estáticos).

P A R T E I I I

DHCP

Esta parte contiene información conceptual acerca del Protocolo de configuración de host dinámico (DHCP) y tareas para planificar, configurar, administrar y resolver problemas del servicio DHCP.

Acerca de DHCP (descripción general)

En este capítulo se introduce el Protocolo de configuración dinámica de host (DHCP), y se describen los conceptos relativos a dicho protocolo. Además, se relatan las ventajas del uso de DHCP en una red.

Este capítulo contiene la información siguiente:

- “Acerca del Protocolo DHCP” en la página 301
- “Ventajas del uso de DHCP” en la página 302
- “Funcionamiento de DHCP” en la página 303
- “El servidor DHCP” en la página 306
- “El cliente DHCP” en la página 315

Acerca del Protocolo DHCP

El protocolo DHCP permite configurar automáticamente los sistemas host de una red TCP/IP durante el inicio de los sistemas. DHCP utiliza un mecanismo de cliente-servidor. Los servidores almacenan y gestionan la información de configuración de los clientes y la suministran cuando éstos la solicitan. Esta información incluye la dirección IP del cliente y los servicios de red de los que el cliente puede disponer.

DHCP ha evolucionado de un protocolo anterior, BOOTP, que se diseñó para el inicio en una red TCP/IP. DHCP utiliza el mismo formato que BOOTP para los mensajes entre el cliente y el servidor. No obstante, a diferencia de los mensajes BOOTP, los mensajes DHCP pueden incluir datos de configuración de red para el cliente.

Una de las ventajas de DHCP es la posibilidad de gestionar la asignación de direcciones IP mediante permisos. Los *permisos* permiten reclamar las direcciones IP cuando no están en uso. Las direcciones IP reclamadas se pueden reasignar a otros clientes. Un sitio que utilice DHCP puede utilizar una agrupación de direcciones IP menor que la que se necesitaría si todos los clientes tuvieran asignada una dirección IP permanente.

Ventajas del uso de DHCP

Gracias a DHCP no tendrá que dedicar gran parte de su tiempo a configurar una red TCP/IP ni a la administración diaria de dicha red. Tenga en cuenta que en la implementación de Oracle Solaris, DHCP sólo funciona con IPv4.

DHCP ofrece las ventajas siguientes:

- **Administración de direcciones IP:** una de las principales ventajas de DHCP es que facilita la administración de las direcciones IP. En una red sin DHCP, debe asignar manualmente las direcciones IP. Debe asignar una dirección IP exclusiva a cada cliente y configurar cada uno de los clientes de modo individual. Si un cliente se pasa a una red distinta, debe realizar modificaciones manuales para dicho cliente. Si DHCP está activo, el servidor DHCP administra y asigna las direcciones IP sin necesidad de que intervenga el administrador. Los clientes pueden moverse a otras subredes sin necesidad de reconfiguración manual, ya que obtienen del servidor DHCP la nueva información de cliente necesaria para la nueva red.
- **Configuración de cliente de red centralizada:** Puede crear una configuración a medida para determinados clientes o para determinados tipos de clientes. La información de configuración se almacena en un lugar, el almacén de datos de DHCP. No es necesario iniciar sesión en un cliente para cambiar su configuración. Puede realizar modificaciones en múltiples clientes cambiando la información del almacén de datos.
- **Compatibilidad con clientes BOOTP:** Tanto los servidores BOOTP como los servidores DHCP escuchan y responden las emisiones de los clientes. El servidor DHCP puede responder a las solicitudes de clientes BOOTP y de clientes DHCP. Los clientes BOOTP reciben una dirección IP y la información que necesitan para iniciar desde un servidor.
- **Compatibilidad con clientes locales y remotos:** BOOTP permite reenviar mensajes de una red a otra. DHCP aprovecha la función de reenvío de BOOTP de distintos modos. La mayoría de los enrutadores de red se pueden configurar como agentes de reenvío de BOOTP para transferir solicitudes BOOTP a servidores que no se encuentren en la red del cliente. Las solicitudes DHCP se pueden reenviar del mismo modo, ya que el enrutador no distingue las solicitudes DHCP de las solicitudes BOOTP. El servidor DHCP también se puede configurar como agente de reenvío de BOOTP, si no hay disponible ningún enrutador que admita el reenvío de BOOTP.
- **Inicio de red:** los clientes pueden utilizar DHCP para obtener la información necesaria para iniciar desde un servidor de la red, en lugar de utilizar RARP (Reverse Address Resolution Protocol) y el archivo `bootparams`. El servidor DHCP puede facilitar a un cliente toda la información que necesita para funcionar, incluida la dirección IP, el servidor de inicio y la información de configuración de red. Dado que las solicitudes DHCP se pueden reenviar por subredes, es posible usar menos servidores de inicio en la red cuando se utiliza el inicio de red DHCP. El inicio RARP requiere que cada subred tenga un servidor de inicio.
- **Amplia compatibilidad de red:** las redes con millones de clientes DHCP pueden utilizar DHCP. El servidor DHCP utiliza varios subprocesos para procesar a la vez múltiples solicitudes de clientes. El servidor también admite almacenes de datos optimizados para

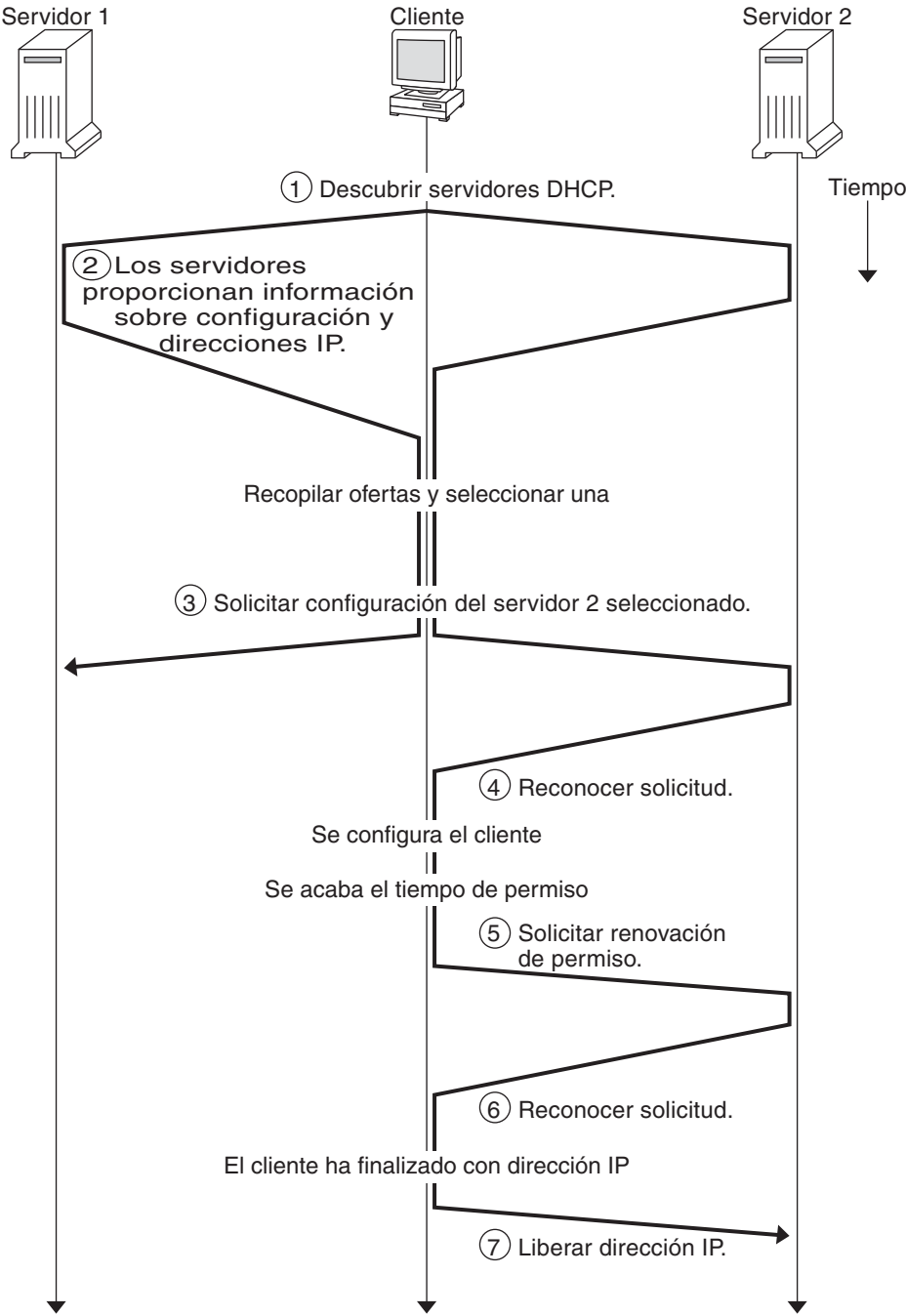
administrar grandes cantidades de datos. El acceso de los almacenes de datos se administra mediante módulos de procesamiento independientes. Este tipo de almacén de datos permite la compatibilidad para cualquier base de datos que se necesite.

Funcionamiento de DHCP

En primer lugar, debe instalar y configurar el servidor DHCP. Durante la configuración, se especifica la información sobre la red en la que deben funcionar los clientes. Una vez especificada esta información, los clientes pueden solicitar y recibir información de red.

La secuencia de eventos del servicio DHCP se muestra en el diagrama siguiente. Los números de los círculos corresponden a los elementos que se enumeran en la descripción que sigue al diagrama.

FIGURA 12-1 Secuencia de eventos para el servicio DHCP



El diagrama anterior muestra los siguientes pasos:

1. El cliente descubre un servidor DHCP emitiendo un *mensaje de descubrimiento* a la dirección de emisión limitada (255 . 255 . 255 . 255) de la subred local. Si hay un enrutador y está configurado para hacer de agente de reenvío de BOOTP, la solicitud se transfiere a otros servidores DHCP de diferentes subredes. La *emisión* del cliente incluye su ID exclusivo, que, en la implementación de DHCP en Oracle Solaris, se obtiene de la dirección de control de acceso de soportes (MAC) del cliente. En una red Ethernet, la dirección MAC es la misma que la dirección Ethernet.

Los servidores DHCP que reciben el mensaje de descubrimiento pueden determinar la red del cliente con la información siguiente:

- ¿En qué interfaz de red se sitúa la solicitud? El servidor determina si el cliente se encuentra en la red a la que está conectada la interfaz o si está utilizando un agente de reenvío de BOOTP conectado a dicha red.
 - ¿Incluye la solicitud la dirección IP de un agente de reenvío de BOOTP? Cuando una solicitud pasa por un agente de reenvío, éste inserta su dirección en el encabezado de la solicitud. Cuando el servidor detecta una *dirección de agente de reenvío*, el servidor sabe que la parte de red de la dirección indica la dirección de red del cliente porque el agente de reenvío debe estar conectado a la red del cliente.
 - ¿La red del cliente cuenta con subredes? El servidor consulta la tabla `netmasks` para encontrar la máscara de subred que se utiliza en la red que indica la dirección del agente de reenvío o la dirección de la interfaz de red que recibió la solicitud. Cuando el servidor conoce la máscara de subred que se utiliza, puede determinar qué parte de la dirección de red es la parte del host, y a continuación seleccionar una dirección IP adecuada para el cliente. Consulte la página del comando `man netmasks(4)` para obtener información sobre `netmasks`.
2. Cuando los servidores DHCP determinan la red del cliente, seleccionan una dirección IP adecuada y verifican que no esté en uso. A continuación, los servidores DHCP responden al cliente emitiendo un *mensaje de oferta*. El mensaje de oferta incluye la dirección IP seleccionada e información sobre los servicios que se pueden configurar para el cliente. Cada servidor reserva temporalmente la dirección IP ofrecida hasta que el cliente determina si utilizará la dirección IP.
 3. El cliente selecciona la mejor oferta basándose en el número y el tipo de servicios ofrecidos. El cliente emite una solicitud que especifica la dirección IP del servidor que realizó la mejor oferta. La emisión garantiza que todos los servidores DHCP de respuesta sepan que el cliente ha seleccionado un servidor. Los servidores que no se eligen pueden cancelar las reservas de las direcciones IP que habían ofrecido.
 4. El servidor seleccionado asigna la dirección IP para el cliente y almacena la información en el almacén de datos DHCP. El servidor también envía un mensaje de reconocimiento (ACK) al cliente. El *mensaje de reconocimiento* contiene los parámetros de configuración de red

para el cliente. La utilidad ping permite al cliente probar la dirección IP para asegurarse de que no la esté utilizando otro sistema. A continuación, el cliente sigue iniciándose para unirse a la red.

5. El cliente supervisa el tiempo de permiso. Una vez transcurrido un periodo determinado, el cliente envía un nuevo mensaje al servidor seleccionado para aumentar el tiempo de permiso.
6. El servidor DHCP que recibe la solicitud amplía el tiempo de permiso si el permiso sigue cumpliendo la directiva de permiso local que ha fijado el administrador. Si el servidor no responde en 20 segundos, el cliente emite una solicitud para que uno de los demás servidores DHCP pueda ampliar el permiso.
7. Cuando el cliente ya no necesita la dirección IP, notifica al servidor que la dirección IP está libre. Esta notificación puede tener lugar durante un cierre ordenado y también se puede realizar manualmente.

El servidor DHCP

El servidor DHCP se ejecuta como daemon en Oracle Solaris en un sistema host. El servidor desempeña dos funciones básicas:

- **Administra direcciones IP:** El servidor DHCP controla una serie de direcciones IP y las asigna a los clientes, ya sea de forma permanente o durante un periodo determinado. El servidor utiliza un mecanismo de permiso para determinar durante cuánto tiempo un cliente puede utilizar una dirección que no sea permanente. Cuando se deja de utilizar la dirección, se devuelve a la agrupación y se puede volver a asignar. El servidor contiene información sobre la vinculación de direcciones IP a los clientes de sus tablas de red DHCP, con lo cual se garantiza que no haya más de un cliente que utilice la misma red.
- **Configura la red para los clientes:** El servidor asigna una dirección IP y proporciona otra información para la configuración de red, como un nombre de host, una dirección de emisión, una máscara de subred, un portal predeterminado, un servicio de nombres y mucha otra información. La información de configuración de red se obtiene de la base de datos dhcptab del servidor.

El servidor DHCP también se puede configurar para llevar a cabo las siguientes funciones adicionales:

- **Responder a las solicitudes de clientes BOOTP:** el servidor escucha las emisiones de los clientes BOOTP en las que se descubre un servidor BOOTP y les proporciona una dirección IP y los parámetros de inicio. Un administrador debe configurar la información de modo estático. El servidor DHCP puede actuar como servidor BOOTP y como servidor DHCP de forma simultánea.
- **Reenviar solicitudes:** El servidor reenvía solicitudes de BOOTP y DHCP a los servidores pertinentes de otras subredes. El servidor no puede proporcionar el servicio DHCP o BOOTP cuando está configurado como agente de reenvío de BOOTP.

- **Proporcionar compatibilidad con inicio de red para los clientes DHCP:** el servidor puede proporcionar a los clientes DHCP la información necesaria para iniciar desde la red: una dirección IP, los parámetros de inicio y la información de configuración de la red. El servidor también puede proporcionar la información que necesitan los clientes DHCP para iniciar e instalar una red de área extensa (WAN).
- **Actualizar las tablas DNS para los clientes que proporcionan un nombre de host:** Para los clientes que proporcionan un valor y una opción `Hostname` en sus solicitudes para el servicio DHCP, el servidor puede tratar de actualizar DNS en su lugar.

Administración del servidor DHCP

Como superusuario, puede iniciar, detener y configurar el servidor DHCP con el Administrador de DHCP o con las utilidades de línea de comandos que se describen en [“Utilidades de la línea de comandos de DHCP” en la página 310](#). Por norma general, el servidor DHCP está configurado para iniciarse automáticamente cuando se inicia el sistema, y para detenerse cuando se cierra el sistema. En condiciones normales, no es necesario iniciar y detener manualmente el servidor.

Almacén de datos de DHCP

Todos los datos que utiliza el servidor DHCP se guardan en un almacén de datos. El almacén de datos puede contener archivos de texto sin formato, tablas NIS+ o archivos de formato binario. Al configurar el servicio DHCP, debe seleccionar el tipo de almacén de datos que utilizará. En la sección [“Selección del almacén de datos DHCP” en la página 323](#) se describen las diferencias entre los distintos tipos de almacenes de datos. Puede cambiar el formato de un almacén de datos utilizando el Administrador de DHCP o el comando `dhcpconfig`.

También puede transferir los datos de un almacén de datos de un servidor DHCP a otro almacén de datos de otro servidor. Puede utilizar las funciones de importación y exportación de los almacenes de datos, aunque los servidores utilicen distintos formatos de almacenes de datos. Es posible importar y exportar todo el contenido de un almacén de datos, o sólo algunos de los datos que contiene, utilizando el Administrador de DHCP o el comando `dhcpconfig`.

Nota – Puede utilizar cualquier formato de archivo o base de datos para el almacenamiento de datos de DHCP si desarrolla su propio módulo de código para proporcionar una interfaz entre DHCP (herramientas de administración y servidor) y la base de datos. Para obtener más información, consulte [Solaris DHCP Service Developer's Guide](#).

El almacén de datos de DHCP incluye dos tipos de tablas. Puede ver y administrar el contenido de estas tablas utilizando el Administrador de DHCP o las utilidades de la línea de comandos. Las tablas de datos son:

- Tabla `dhcptab`: Incluye la información de configuración que se puede transferir a los clientes.
- **Tablas de red DHCP**: Contienen información sobre los clientes DHCP y BOOTP que residen en la red especificada en el nombre de tabla. Por ejemplo, la red `192.168.32.0` tendría una tabla cuyo nombre incluye `192_168_32_0`.

La tabla `dhcptab`

La tabla `dhcptab` contiene toda la información que pueden obtener los clientes del servidor DHCP. El servidor DHCP explora la tabla `dhcptab` cada vez que se inicia. El nombre de archivo de la tabla `dhcptab` varía en función del almacén de datos que se utiliza. Por ejemplo, la tabla `dhcptab` creada por el almacén de datos NIS+ `SUNWnisplus` es `SUNWnisplus1_dhcptab`.

El protocolo DHCP define una serie de elementos de información estándar que se pueden transferir a los clientes. Estos elementos se denominan parámetros, símbolos u opciones. Las opciones se definen en el protocolo DHCP mediante códigos numéricos y etiquetas de texto, pero sin valores. En la tabla siguiente se incluyen algunas de las opciones estándar que se utilizan normalmente.

TABLA 12-1 Ejemplo de opciones estándar de DHCP

Código	Etiqueta	Descripción
1	Subnet	Dirección IP de máscara de subred
3	Router	Dirección IP para el enrutador
6	DNSserv	Dirección IP para el servidor DNS
12	Hostname	Cadena de texto para el nombre de host del cliente
15	DNSdmain	Nombre de dominio DNS

Al proporcionar información durante la configuración del servidor, se asignan valores automáticamente a algunas opciones. Puede asignar valores a otras opciones de forma explícita posteriormente. Las opciones y sus valores se transfieren al cliente para proporcionar información de configuración. Por ejemplo, el par de opción/valor, `DNSdmain=Georgia.Peach.COM`, configura el nombre de dominio DNS del cliente como `Georgia.Peach.COM`.

Las opciones se pueden agrupar con otras opciones en contenedores conocidos como *macros*, lo cual facilita la transferencia de información a un cliente. Algunas macros se crean automáticamente durante la configuración del servidor y contienen las opciones a las que se asignó valores durante la configuración. Las macros pueden contener a su vez otras macros.

El formato de la tabla `dhcptab` se describe en la página del comando `man dhcpd(4)`. En el Administrador de DHCP, toda la información que se muestra en las fichas Opciones y Macros proviene de la tabla `dhcptab`. Consulte [“Acerca de las opciones DHCP” en la página 313](#) para obtener más información acerca de las opciones. Consulte [“Acerca de macros DHCP” en la página 313](#) si desea más información sobre las macros.

La tabla `dhcptab` no debe editarse manualmente. Debe utilizar el comando `dhtadm` o el Administrador de DHCP para crear, eliminar o modificar las opciones y macros.

Tablas de red DHCP

Una tabla de red DHCP asigna identificadores de cliente a las direcciones IP y el parámetro de configuración asociado con cada dirección. El formato de las tablas de red se describe en la página del comando `man dhcp_network(4)`. En el Administrador DHCP, toda la información de la ficha Direcciones proviene de las tablas de red.

Administrador de DHCP

El Administrador de DHCP es una herramienta de interfaz gráfica de usuario (GUI) que puede utilizar para llevar a cabo todas las tareas de administración asociadas al servicio DHCP. Puede utilizarlo para administrar el servidor y los datos que utiliza. Debe ser superusuario para ejecutar el Administrador de DHCP.

Puede utilizar el Administrador de DHCP para:

- Configurar y desconfigurar el servidor DHCP
- Iniciar, detener y reiniciar el servidor DHCP
- Desactivar y activar el servicio DHCP
- Personalizar la configuración del servidor DHCP

El Administrador de DHCP permite administrar las direcciones IP, las macros de configuración de red y las opciones de configuración de red de los modos siguientes:

- Agregar y eliminar redes en la administración de DHCP
- Ver, agregar, modificar, eliminar y liberar direcciones IP en la administración de DHCP
- Ver, agregar, modificar y eliminar macros de configuración de red
- Ver, agregar, modificar y eliminar opciones de configuración de red que no sean estándar

El Administrador de DHCP permite administrar los almacenes de datos DHCP de los modos siguientes:

- Convertir datos a un nuevo formato de almacén de datos
- Mover los datos de DHCP de un servidor DHCP a otro exportándolos del primer servidor y luego importándolos en el segundo.

El Administrador de DHCP incluye una amplia ayuda en línea sobre los procedimientos que permite realizar la herramienta. Para más información, consulte [“Acerca del Administrador de DHCP” en la página 346](#).

Utilidades de la línea de comandos de DHCP

Todas las funciones de administración de DHCP se pueden llevar a cabo con las utilidades de la línea de comandos. Puede ejecutar las utilidades si ha iniciado sesión como superusuario o como usuario asignado al perfil de administración de DHCP. Consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).

En la tabla siguiente se enumeran las utilidades y se describe la finalidad de cada una de ellas.

TABLA 12-2 Utilidades de la línea de comandos de DHCP

Orden	Descripción y finalidad	Vínculos de página del comando man
<code>in.dhcpd</code>	El daemon del servicio DHCP. Los argumentos de la línea de comandos permiten configurar varias opciones del tiempo de ejecución.	in.dhcpd(1M)
<code>dhcpconfig</code>	Se utiliza para configurar y anular la configuración de un servidor DHCP. Esta utilidad permite realizar muchas de las funciones del Administrador de DHCP desde la línea de comandos. Esta utilidad está diseñada principalmente para utilizarse en secuencias de comandos para sitios que deseen automatizar algunas funciones de configuración. <code>dhcpconfig</code> recopila información de los archivos de topología de red del sistema de servidor para crear información útil para la configuración inicial.	dhcpconfig(1M)
<code>dhtadm</code>	Se utiliza para agregar, eliminar y modificar las opciones de configuración y las macros para los clientes DHCP. Esta utilidad permite editar la tabla <code>dhcptab</code> de forma indirecta, con lo cual se garantiza que la tabla <code>dhcptab</code> tenga el formato correcto. No debe editar directamente la tabla <code>dhcptab</code> .	dhtadm(1M)

TABLA 12-2 Utilidades de la línea de comandos de DHCP (Continuación)

Orden	Descripción y finalidad	Vínculos de página del comando man
pnadm	<p>Se utiliza para administrar las tablas de red de DHCP. Esta utilidad permite llevar a cabo las siguientes tareas:</p> <ul style="list-style-type: none"> ■ Agregar y eliminar direcciones IP y redes en la administración de DHCP. ■ Modificar la configuración de red para las direcciones IP especificadas. ■ Mostrar información sobre las direcciones IP y redes en la administración de DHCP. 	pnadm(1M)

Control de acceso basado en roles para los comandos DHCP

La seguridad de los comandos `dhcpconfig`, `dhtadm` y `pnadm` la determina la configuración del control de acceso basado en roles (RBAC). De modo predeterminado, sólo el superusuario puede ejecutar los comandos. Si desea utilizar los comandos con otro nombre de usuario, debe asignar el nombre de usuario al perfil de administración de DHCP tal como se describe en “Configuración del acceso de usuario a los comandos de DHCP” en la página 349.

Configuración del servidor DHCP

Puede configurar el servidor DHCP la primera vez que ejecute el Administrador de DHCP en un sistema en el que vaya a ejecutar el servidor DHCP.

Los cuadros de diálogo de configuración del servidor del Administrador de DHCP solicitan la información básica necesaria para permitir y ejecutar el servidor DHCP en una red. Algunos valores predeterminados se obtienen de los archivos del sistema. Si no ha configurado el sistema para la red, no habrá valores predeterminados. El Administrador de DHCP le solicita la siguiente información:

- El rol del servidor, tanto si es el servidor DHCP como el agente de reenvío de BOOTP
- El tipo de almacén de datos (archivos, archivos binarios, NIS+ o lo que haya especificado en su sitio)
- Los parámetros de configuración del almacén de datos para el tipo de almacén de datos seleccionado
- El servicio de nombres que utilizar para actualizar los registros del host, en caso de haberlos (/etc/hosts , NIS+ o DNS)
- La duración del permiso y si los clientes deben poder renovarlo

- El nombre de dominio DNS y las direcciones IP de los servidores DNS
- Las direcciones de red y la máscara de subred de la primera red que desee configurar para el servicio DHCP
- El tipo de red, tanto si se trata de una red de área local (LAN) como de una red de punto a punto
- El descubrimiento del enrutador o la dirección IP de un enrutador específico
- El nombre de dominio NIS y la dirección IP de los servidores NIS
- El nombre de dominio NIS+ y la dirección IP de los servidores NIS+

También puede configurar el servidor DHCP utilizando el comando `dhcpconfig`. Esta utilidad recopila información automáticamente de los archivos de sistema existentes para proporcionar una configuración inicial útil. Por tanto, debe asegurarse de que los archivos sean correctos antes de ejecutar `dhcpconfig`. Consulte la página del comando `man dhcpconfig(1M)` para obtener información sobre los archivos que utiliza `dhcpconfig` para obtener información.

Asignación de direcciones IP

El servidor DHCP admite los siguientes tipos de asignación de direcciones IP:

- **Asignación manual:** El servidor proporciona una dirección IP específica seleccionada para un cliente DHCP concreto. La dirección no se puede reclamar ni asignar a otro cliente.
- **Asignación automática o permanente:** El servidor proporciona una dirección IP que no tenga vencimiento, con lo cual se asocia de forma permanente con el cliente hasta que se cambie la asignación o el cliente libere la dirección.
- **Asignación dinámica:** El servidor proporciona una dirección IP a un cliente que la solicite, con un permiso para un periodo específico. Cuando venza el permiso, la dirección volverá al servidor y se podrá asignar a otro cliente. El periodo lo determina el tiempo de permiso que se configure para el servidor.

Información de configuración de red

Determine qué información va a proporcionar a los clientes DHCP. Cuando configure el servidor DHCP, facilite la información básica sobre la red. Posteriormente, puede agregar a los clientes la información adicional que desee.

El servidor DHCP almacena la información de configuración de red en la tabla `dhcptab`, como pares de opción/valor y macros. Las opciones son palabras clave para los datos de red que desee proporcionar a los clientes. Se asignan valores a las opciones y se transfieren a los clientes de los mensajes DHCP. Por ejemplo, la dirección del servidor NIS se transfiere mediante una opción denominada `NISservs`. La opción `NISservs` tiene un valor que equivale a una lista de direcciones IP, que asigna el servidor DHCP. Las macros constituyen una forma cómoda de

agrupar cualquier cantidad de opciones que desee proporcionar a los clientes. Puede utilizar el Administrador de DHCP para crear macros para agrupar opciones y asignar valores a las opciones. Si prefiere una herramienta de línea de comandos, puede utilizar `dhtadm`, la utilidad de administración de la tabla de configuración DHCP, para trabajar con las opciones y macros.

Acerca de las opciones DHCP

En DHCP, una *opción* es un dato de red que se puede transferir a un cliente. La documentación sobre DHCP también hace referencia a las opciones como *símbolos* o *etiquetas*. Una opción se define mediante un código numérico y una etiqueta de texto. Una opción recibe un valor cuando se utiliza en el servicio DHCP.

El protocolo DHCP define un número mayor de opciones estándar para los datos de red especificados de modo común: Subnet, Router, Broadcast, NIS+dom, Hostname y LeaseTime son algunos ejemplos. En la página del comando `man dhcp_inittab(4)` se muestra una lista completa de las opciones estándar. Las palabras clave de las opciones estándar no se pueden modificar de ningún modo. Sin embargo, puede asignar valores a las opciones relevantes para su red cuando incluya las opciones en las macros.

Puede crear nuevas opciones para los datos que no estén representados por las opciones estándar. Las opciones que cree deben clasificarse en una de estas tres categorías:

- **Extendidas:** Se reserva para las opciones que se han convertido opciones de DHCP estándar pero se incluyen en la implementación del servidor DHCP. Puede utilizar la opción extendida si conoce una opción estándar que desee utilizar, pero no desea actualizar el servidor DHCP.
- **Sitio:** Se reserva para opciones exclusivas del sitio. Estas opciones se crean.
- **Distribuidor:** se reserva para las opciones que sólo deben aplicarse a los clientes de una clase concreta, como una plataforma de distribuidor o hardware. La implementación de DHCP incluye una serie de opciones de distribuidor para los clientes de Oracle Solaris. Por ejemplo, la opción `SrootIP4` se utiliza para especificar la dirección IP de un servidor que debería utilizar un cliente que se inicia desde la red para su sistema de archivos raíz (`/`).

El [Capítulo 15, “Administración de DHCP \(tareas\)”](#) incluye los procedimientos para crear, modificar y eliminar las opciones de DHCP.

Acerca de macros DHCP

En el servicio DHCP, una *macro* es un conjunto de opciones de configuración de red y los valores que se les asignan. Las macros se crean para agrupar opciones para transferir a clientes o tipos de clientes específicos. Por ejemplo, una macro diseñada para todos los clientes de una subred concreta podrían contener pares de opción/valor para la máscara de subred, direcciones IP de enrutador, direcciones de emisión, dominio NIS+ y tiempo de permiso.

Procesamiento de macros con el servidor DHCP

Cuando el servidor DHCP procesa una macro, coloca las opciones de red y los valores definidos en la macro en un mensaje DHCP para un cliente. El servidor procesa algunas macros automáticamente para los clientes de un tipo específico.

Para que el servidor procese automáticamente una macro, el nombre de la macro debe formar parte de una de las categorías que se incluyen en la tabla siguiente.

TABLA 12-3 Categorías de macros DHCP para procesamiento automático

Categoría de macro	Descripción
Clase de cliente	El nombre de la macro coincide con una clase de cliente, que se indica mediante el tipo de máquina del cliente, el sistema operativo, o ambos. Por ejemplo, si un servidor tiene una macro denominada <code>SUNW.Sun-Blade-100</code> , cualquier cliente cuya implementación de hardware sea <code>SUNW.Sun-Blade-100</code> recibirá automáticamente los valores de la macro <code>SUNW.Sun-Blade-100</code> .
Dirección de red	El nombre de la macro coincide con una dirección IP de la red administrada por DHCP. Por ejemplo, si un servidor tiene una macro denominada <code>10.53.224.0</code> , cualquier cliente conectado a la red <code>10.53.224.0</code> recibirá de manera automática los valores de la macro <code>10.53.224.0</code> .
ID de cliente	El nombre de macro coincide con algunos identificadores exclusivos del cliente, que normalmente se obtienen de una dirección MAC o Ethernet. Por ejemplo, si un servidor tiene una macro denominada <code>08002011DF32</code> , el cliente con el ID de cliente <code>08002011DF32</code> (derivado de la dirección Ethernet <code>8:0:20:11:DF:32</code>), recibirá automáticamente los valores de la macro denominada <code>08002011DF32</code> .

Una macro con un nombre que no utilice una de las categorías incluidas en la [Tabla 12-3](#) sólo se puede procesar si se cumple una de estas condiciones:

- La macro está asignada a una dirección IP.
- La macro se incluye en otra macro que se procesa automáticamente.
- La macro se incluye en otra macro que está asignada a una dirección IP.

Nota – Al configurar un servidor, se crea de forma predeterminada una macro cuyo nombre coincide con el nombre del servidor. Esta macro de servidor *no* se procesa automáticamente para ningún cliente porque no tiene el nombre de uno de los tipos que desencadenan el procesamiento automático. Cuando crea direcciones IP en el servidor posteriormente, las direcciones IP se asignan para utilizar la macro del servidor de modo predeterminado.

Orden del procesamiento de macros

Cuando un cliente DHCP solicita servicios DHCP, el servidor DHCP determina qué macros coinciden con el cliente. El servidor procesa las macros utilizando las categorías de macro para determinar el orden del procesamiento. La categoría más general se procesa en primer lugar, y la más específica en último lugar. Las macros se procesan en el siguiente orden:

1. Macros de clase de cliente: la categoría más general.
2. Macros de dirección de red: más específicas que las de clase de cliente.
3. Macros asignadas a direcciones IP: más específicas que las de dirección de red.
4. Macros de ID de cliente: la categoría más específica, que pertenece a un cliente.

Una macro que está incluida en otra macro se procesa como parte de la macro que la contiene.

Si la misma opción se incluye en más de una macro, se utiliza el valor de dicha opción en la macro cuya categoría sea más específica, ya que se procesa en último lugar. Por ejemplo, si una macro de dirección de red contiene la opción de tiempo de permiso con un valor de 24 horas, y una macro de ID de cliente contiene la opción de tiempo de permiso con un valor de 8 horas, el cliente recibe un tiempo de permiso de 8 horas.

Límite de tamaño para las macros DHCP

La suma total de los valores asignados a todas las opciones de una macro no debe superar los 255 bytes, incluidos los códigos de opción y la información sobre la longitud. Este límite lo dicta el protocolo DHCP.

Las macros con más probabilidad de verse afectadas por este límite son las que se utilizan para transferir rutas a los archivos de los servidores de instalación de Oracle Solaris. Por lo general debe pasar la mínima información necesaria sobre el distribuidor. Debe usar nombres cortos para las rutas en las opciones que necesiten nombres de rutas. Si crea vínculos simbólicos con rutas largas, podrá transferir los nombres de vínculos más breves.

El cliente DHCP

El término "cliente" se utiliza a veces para hacer referencia a un equipo físico que está desempeñando un rol de cliente en la red. Sin embargo, el cliente DHCP descrito en este documento es una entidad de software. El cliente DHCP es un daemon (dhcpcd) que se ejecuta en Oracle Solaris en un sistema configurado para recibir su configuración de red de un servidor DHCP. Los clientes DHCP de otros proveedores también pueden utilizar los servicios del servidor de DHCP. Sin embargo, este documento sólo describe el cliente de DHCP.

Consulte el [Capítulo 16, “Configuración y administración del cliente DHCP”](#) para obtener información detallada sobre el cliente DHCP.

Planificación del servicio DHCP (tareas)

Puede utilizar el servicio DHCP en una red que esté creando o en una que ya exista. Si está configurando una red, consulte el [Capítulo 2, “Planificación de la red TCP/IP \(tareas\)”](#) antes de configurar el servicio DHCP. Si ya existe una red, continúe en este capítulo.

En él se describen los pasos necesarios para configurar el servicio DHCP en la red. La información está destinada para uso con el Administrador de DHCP, aunque también puede utilizar la utilidad de línea de comandos de `dhcpconfig` para configurar el servicio DHCP.

Este capítulo contiene la información siguiente:

- “Preparación de la red para el servicio DHCP (mapa de tareas)” en la página 317
- “Toma de decisiones para la configuración del servidor DHCP (mapa de tareas)” en la página 322
- “Toma de decisiones para la administración de direcciones IP (mapa de tareas)” en la página 325
- “Planificación de múltiples servidores DHCP” en la página 329
- “Planificación de la configuración DHCP de las redes remotas” en la página 330
- “Selección de la herramienta para configurar DHCP” en la página 330

Preparación de la red para el servicio DHCP (mapa de tareas)

Antes de configurar la red para el uso de DHCP, debe recopilar la información que le permita tomar las decisiones sobre la configuración de uno o más servidores. Con el mapa de tareas de la tabla siguiente puede identificar las tareas requeridas para preparar la red para DHCP. La tabla muestra las tareas, las descripciones de lo que se consigue con cada una de ellas y las secciones que detallan los pasos para realizar las tareas individuales.

Tarea	Descripción	Para obtener instrucciones
Asignar topología de red.	Determina y localiza los servicios disponibles en la red.	“Asignación de topología de red” en la página 318
Determinar el número de servidores DHCP que se necesitan.	Utiliza el número previsto de clientes DHCP como base para determinar la cantidad de servidores DHCP que se necesitan.	“Cómo determinar el número de servidores DHCP” en la página 319
Actualizar archivos de sistema y tabla netmasks.	Refleja la topología de red de un modo preciso.	“Actualización de archivos de sistema y tablas de máscara de red” en la página 320

Asignación de topología de red

Si todavía no lo ha hecho, asigne la estructura física de la red. Indique la ubicación de los enrutadores y los clientes, así como la ubicación de los servidores que proporcionan servicios de red. Esta asignación de la topología de red le permite determinar qué servidor utilizar para el servicio DHCP. La asignación también le ayuda a determinar la información de configuración que el servidor DHCP puede proporcionar a los clientes.

Consulte el [Capítulo 2, “Planificación de la red TCP/IP \(tareas\)”](#) para obtener más información sobre la planificación de su red.

El proceso de configuración de DHCP permite reunir información de red de los archivos de red y el sistema del servidor. [“Actualización de archivos de sistema y tablas de máscara de red” en la página 320](#) describe estos archivos. Sin embargo, puede ofrecer a los clientes otra información de servicio, que debe especificar en las macros del servidor. Cuando examine la topología de red, registre las direcciones IP de cualquier servidor que desea que conozcan los clientes. Por ejemplo, los siguientes servidores pueden proporcionar servicios en su red. La configuración de DHCP no descubre estos servidores.

- Servidor de tiempo
- Servidor de registro
- Servidor de impresión
- Servidor de instalación
- Servidor de inicio
- Servidor proxy Web
- Servidor de intercambio
- Servidor de fuentes de ventanas X
- Servidor de Trivial File Transfer Protocol (TFTP)

Topología de red que evitar

En algunos entornos de red IP, varias redes de área local (LAN) comparten el mismo soporte de hardware de red. Las redes pueden utilizar varias interfaces de hardware de red o varias interfaces lógicas. DHCP no funciona bien en este tipo de redes de soportes compartidos. Cuando varias LAN se ejecutan en la misma red física, la solicitud de un cliente DHCP llega a todas las interfaces de hardware de red. Con ello parece que el cliente esté conectado a todas las redes IP de forma simultánea.

DHCP debe poder determinar la dirección de una red de cliente para asignar una dirección IP adecuada al cliente. Si en el soporte de hardware hay más de una red, el servidor no puede determinar la red del cliente. El servidor no puede asignar una dirección IP sin conocer el número de red.

Puede utilizar DHCP sólo en una de las redes. Si una red no satisface sus necesidades de DHCP, debe volver a configurar las redes. Debe tener en cuenta las siguientes sugerencias:

- Utilice una máscara de subred de longitud variable (VLSM) en las subredes para aprovechar al máximo el espacio de direcciones IP del que dispone. Es posible que no tenga que ejecutar varias redes en la misma red física. Consulte la página del comando `man netmasks(4)` para obtener información sobre la implementación de subredes de longitud variable. Para obtener más información sobre el enrutamiento entre dominios sin clase (CIDR) (CIDR) y VLSM, consulte <http://www.ietf.org/rfc/rfc1519.txt>.
- Configure los puertos de los conmutadores para asignar dispositivos a las diferentes LAN físicas. Esta técnica conserva la asignación de una LAN a una red IP, necesaria para DHCP. Consulte la documentación del conmutador para obtener información sobre cómo configurar los puertos.

Cómo determinar el número de servidores DHCP

La opción de almacén de datos que elija tiene un efecto directo en el número de servidores que debe tener para admitir los clientes DHCP. La tabla siguiente muestra el número máximo de clientes DHCP y BOOTP que puede admitir un servidor DHCP para cada almacén de datos.

TABLA 13-1 Número máximo estimado de clientes admitidos por un servidor DHCP

Tipo de almacén de datos	Número máximo de clientes admitidos
Archivos de texto	10.000
NIS+	40.000
Archivos binarios	100.000

Este número máximo es una pauta general, no una cifra absoluta. La capacidad de un cliente de servidor DHCP depende en gran medida de la cantidad de transacciones por segundo que deba procesar el servidor. Los tiempos de permisos y los patrones de uso tienen un impacto

significativo en la tasa de transacción. Por ejemplo, supongamos que los permisos están configurados en 12 horas y que los usuarios apagan los sistemas por la noche. Si muchos usuarios encienden sus sistemas a la misma hora por la mañana, el servidor debe administrar picos de transacciones, ya que muchos clientes solicitan permisos a la vez. El servidor DHCP admite menos clientes en dichos entornos. El servidor DHCP puede admitir más clientes en un entorno con permisos más largos, o en un entorno compuesto por dispositivos que están conectados permanentemente, como los módems por cable.

En la sección “[Selección del almacén de datos DHCP](#)” en la [página 323](#) se comparan los tipos de almacenes de datos.

Actualización de archivos de sistema y tablas de máscara de red

Durante la configuración de DHCP, las herramientas DHCP exploran varios archivos de sistema del servidor para obtener información que se pueda utilizar para configurar el servidor.

Debe estar seguro de que la información de los archivos del sistema sea actual antes de ejecutar el Administrador de DHCP o `dhcpcfg` para configurar el servidor. Si detecta errores antes de configurar el servidor, utilice el Administrador de DHCP o `dhtadm` para modificar las macros del servidor.

En la tabla siguiente se incluye parte de la información recopilada durante la configuración del servidor DHCP, y las fuentes de la información. Asegúrese de que esta información esté configurada correctamente en el servidor antes de configurar DHCP en el servidor. Si realiza cambios en los archivos del sistema después de configurar el servidor, debe volver a configurar el servicio para que los refleje.

TABLA 13–2 Información utilizada para la configuración de DHCP

Información	Origen	Comentarios
Zona horaria	Fecha del sistema, configuración de zona horaria	La fecha y la zona horaria se configuran inicialmente durante la instalación de Oracle Solaris. Puede cambiar la fecha utilizando el comando <code>date</code> . Puede cambiar la zona horaria editando el archivo <code>/etc/default/init</code> para fijar la variable de entorno <code>TZ</code> . Consulte la página del comando <code>man TIMEZONE(4)</code> para obtener más información.

TABLA 13-2 Información utilizada para la configuración de DHCP (Continuación)

Información	Origen	Comentarios
Parámetros de DNS	/etc/resolv.conf	El servidor DHCP utiliza el archivo /etc/resolv.conf para obtener los parámetros de DNS como el nombre de dominio DNS o las direcciones de servidor DNS. Consulte la Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP) o la página del comando <code>man resolv.conf(4)</code> para obtener más información sobre resolv.conf.
Parámetros NIS o NIS+	Nombre de dominio de sistema, nsswitch.conf, NIS o NIS+	El servidor DHCP utiliza el comando <code>domainname</code> para obtener el nombre de dominio del sistema de servidor. El archivo <code>nsswitch.conf</code> indica al servidor dónde debe buscar la información del dominio. Si el sistema de servidor es un cliente NIS o NIS+, el servidor DHCP realiza una consulta para obtener las direcciones IP del servidor NIS o NIS+. Consulte la página del comando <code>man nsswitch.conf(4)</code> para obtener más información.
Enrutador predeterminado	Tablas de enrutamiento del sistema, mensaje de usuario	El servidor DHCP busca en las tablas de enrutamiento del sistema el enrutador predeterminado para los clientes conectados a la red local. Para los clientes que no se encuentren en la misma red, el servidor DHCP debe solicitar la información.
Máscara de subred	Interfaz de red, tabla <code>netmasks</code>	El servidor DHCP busca sus propias interfaces de red para determinar la dirección de máscara de red y de emisión para los clientes locales. Si la solicitud la emite un agente de reenvío, el servidor obtiene la máscara de subred de la tabla <code>netmasks</code> de la red del agente de reenvío.
Dirección de emisión	Interfaz de red, tabla <code>netmasks</code>	Para la red local, el servidor DHCP obtiene la dirección de emisión consultando la interfaz de red. Para las redes remotas, el servidor utiliza la dirección IP del agente de reenvío BOOTP y la máscara de red de la red remota para calcular la dirección de emisión de la red.

Toma de decisiones para la configuración del servidor DHCP (mapa de tareas)

En esta sección se describen algunas de las decisiones que debe tomar antes de configurar el primer servidor DHCP de la red. La tabla siguiente es útil al configurar la red para usar DHCP; contiene vínculos de cada tarea a la correspondiente sección en que se describe el procedimiento requerido.

Tarea	Descripción	Para obtener instrucciones
Seleccionar un servidor para DHCP.	Determina si un servidor reúne los requisitos del sistema para ejecutar el servicio DHCP.	“Selección de un host para ejecutar el servicio DHCP” en la página 322
Elegir un almacén de datos.	Compara los tipos de almacén de datos para determinar el mejor para su sitio.	“Selección del almacén de datos DHCP” en la página 323
Definir una directiva de permiso.	Obtiene información de los permisos de direcciones IP para ayudarle a determinar la directiva de permiso adecuada para su sitio.	“Configuración de una directiva de permiso” en la página 324
Seleccionar una dirección de enrutador o descubrimiento de enrutador.	Determina si los clientes DHCP utilizan descubrimiento de enrutador o un enrutador específico.	“Cómo determinar los enrutadores para clientes DHCP” en la página 325

Selección de un host para ejecutar el servicio DHCP

Teniendo en cuenta la topología de red, puede utilizar los siguientes requisitos del sistema para seleccionar un host en el que configurar un servidor DHCP.

El host debe cumplir los siguientes requisitos:

- Debe ejecutar Solaris 2.6 o una versión posterior. Si necesita utilizar un número de clientes más elevado, debe instalar la versión Solaris 8 7/01 o una posterior.
- El host debe ser accesible a todas las redes que tengan clientes que necesiten utilizar DHCP, directamente en la red o a través de un agente de reenvío de BOOTP.
- El host debe estar configurado para utilizar el enrutamiento.
- Además, debe contar con una tabla netmasks configurada correctamente que refleje la topología de la red.

Selección del almacén de datos DHCP

Puede almacenar los datos DHCP en archivos de texto, archivos binarios o el servicio de directorios NIS+. La tabla siguiente resume las funciones de cada tipo de almacén de datos, e indica el entorno en el que utilizar cada tipo de almacén de datos.

TABLA 13-3 Comparación de almacenes de datos DHCP

Tipo de almacén de datos	Rendimiento	Mantenimiento	Uso compartido	Entorno
Archivos binarios	Alto rendimiento, gran capacidad	Bajo mantenimiento, no se necesitan servidores de bases de datos. El contenido debe visualizarse con el Administrador de DHCP o dhtadm y pntadm. Se recomienda realizar copias de seguridad regulares de los archivos.	Los almacenes de datos no se pueden compartir entre los servidores DHCP.	Entornos de medio y gran tamaño con múltiples redes y miles de clientes por red. Útiles para ISP de medio y gran tamaño.
NIS+	Capacidad y rendimiento moderados, en función de la capacidad y el rendimiento del servicio NIS+	El sistema de servidor DHCP debe estar configurado como cliente NIS+. Requiere mantenimiento del servicio NIS+. El contenido debe visualizarse con el Administrador de DHCP o dhtadm y pntadm. Se recomienda realizar copias de seguridad regulares con nisbackup.	Los datos DHCP se distribuyen en NIS+, y varios servidores pueden acceder a los mismos contenedores.	Entornos de pequeño a mediano tamaño, con un máximo de 5.000 clientes por red.
Archivos de texto	Rendimiento moderado, baja capacidad	Bajo mantenimiento, no se necesitan servidores de bases de datos. El formato ASCII se puede leer sin el Administrador de DHCP, dhtadm o pntadm. Se recomienda realizar copias de seguridad regulares de los archivos.	El almacén de datos se puede compartir entre servidores DHCP si los datos DHCP están almacenados en un sistema de archivos que se exporta mediante un punto de montaje NFS.	Entornos reducidos con menos de 10.000 clientes, de entre unos cientos hasta mil clientes por red.

Los NIS tradicionales no se ofrecen como opción de almacén de datos porque no admiten actualizaciones incrementales rápidas. Si la red utiliza NIS, debe utilizar los archivos de texto o binarios para el almacén de datos.

Configuración de una directiva de permiso

Un *permiso* especifica la cantidad de tiempo que el servidor DHCP permite a un cliente DHCP utilizar una dirección IP concreta. Durante la configuración inicial del servidor, debe especificar una directiva de permiso para el sitio. La *directiva de permiso* indica el tiempo de permiso y especifica si los clientes pueden renovar sus permisos. El servidor utiliza la información que proporciona para configurar los valores de opciones de las macros predeterminadas que crea el servidor durante la configuración. Puede establecer diferentes políticas de permiso para determinados clientes o tipos de clientes, configurando las opciones de las macros de configuración que cree.

El *tiempo de permiso* se especifica como cantidad de horas, días o semanas durante los que el permiso es válido. Cuando se asigna una dirección IP a un cliente, o se renegocia un permiso en una dirección IP, se calculan la fecha y la hora de vencimiento del permiso. La cantidad de horas del tiempo de permiso se agrega a la indicación de hora en el reconocimiento DHCP del cliente. Por ejemplo, supongamos que la indicación de hora del reconocimiento DHCP es el 16 de septiembre de 2005 a las 9:15, y que el tiempo de permiso es de 24 horas. El tiempo de vencimiento del permiso de este ejemplo será el 17 de septiembre de 2005 a las 9:15. El tiempo de vencimiento del permiso se guarda en el registro de red DHCP del cliente, que puede ver mediante el Administrador de DHCP o la utilidad `pntadm`.

El valor del tiempo de permiso debe ser relativamente bajo para que las direcciones vencidas se puedan reclamar rápidamente. El valor del tiempo de permiso también debe ser lo suficientemente elevado para que se admitan interrupciones del servicio DHCP. Los clientes deben poder funcionar mientras se repara el sistema que ejecuta el servicio DHCP. Una pauta general es especificar un plazo que sea dos veces mayor que el tiempo de inactividad previsto del sistema. Por ejemplo, si necesita cuatro horas para encontrar y sustituir una parte defectuosa y para reiniciar el sistema, especifique un tiempo de permiso de ocho horas.

La opción de negociación del permiso determina si un cliente puede volver a negociar su permiso con el servidor antes de que venza. Si se permite una negociación del permiso, el cliente realiza un seguimiento del tiempo que queda de su permiso. Una vez transcurrida la mitad del permiso, el cliente solicita al servidor DHCP que amplíe el permiso al tiempo de permiso original. La negociación del permiso debe desactivarse en los entornos en los que haya más sistemas que direcciones IP. A continuación, se aplica el límite de tiempo en el uso de las direcciones IP. Si hay suficientes direcciones IP, debe permitir la negociación del permiso para no obligar a los clientes a quitar las interfaces de red cuando venza el permiso. Si hace que los clientes obtengan nuevos permisos, sus conexiones TCP, como las sesiones NFS y telnet, podrían verse interrumpidas. Puede activar la negociación del permiso para todos los clientes

durante la configuración del servidor. La negociación del permiso se puede activar para determinados clientes o tipos de clientes mediante la opción `LeaseNeg` de las macros de configuración.

Nota – Los sistemas que proporcionan servicios en la red deben conservar sus direcciones IP. Dichos sistemas no deben estar sujetos a permisos breves. Puede utilizar DHCP con dichos sistemas si asigna direcciones IP manuales reservadas a los sistemas, en lugar de direcciones IP con permisos permanentes. Puede detectar cuándo se deja de utilizar la dirección IP del sistema.

Cómo determinar los enrutadores para clientes DHCP

Los sistemas host utilizan enrutadores para cualquier comunicación de red más allá de la red local. Los hosts deben conocer las direcciones IP de estos enrutadores.

Al configurar un servidor DHCP, debe proporcionar clientes DHCP con direcciones de enrutador, lo cual se puede hacer de dos modos. Uno es proporcionar direcciones IP específicas para los enrutadores. No obstante, el mejor método es especificar que los clientes busquen los enrutadores con el protocolo de descubrimiento de enrutadores.

Si los clientes de su red pueden realizar el descubrimiento de enrutadores, debe utilizar el protocolo de descubrimiento de enrutadores, aunque sólo haya un enrutador. El descubrimiento de enrutadores permite a un cliente adaptarse fácilmente a los cambios del enrutador en la red. Por ejemplo, supongamos que un enrutador falla y se sustituye por otro con una dirección nueva. Los clientes pueden descubrir automáticamente la nueva dirección sin necesidad de obtener una nueva configuración de red para conseguir la dirección del nuevo enrutador.

Toma de decisiones para la administración de direcciones IP (mapa de tareas)

Como parte de la configuración del servicio DHCP, debe determinar varios aspectos de las direcciones IP que debe administrar el servidor. Si la red requiere más de un servidor DHCP, puede asignar la responsabilidad para varias direcciones IP a cada servidor. Debe decidir cómo dividir la responsabilidad para las direcciones. La tabla siguiente describe las tareas para administrar direcciones IP al utilizar DHCP en la red. La tabla también contiene vínculos a las secciones que explican cómo realizar cada tarea.

Tarea	Descripción	Para obtener información
Especificar las direcciones que debe administrar el servidor.	Determina cuántas direcciones desea que administre el servidor DHCP, y cuáles son dichas direcciones.	“Número e intervalos de direcciones IP” en la página 326

Tarea	Descripción	Para obtener información
Decidir si el servidor debe generar automáticamente los nombres de host para los clientes.	Muestra cómo se generan los nombres de host de cliente para que pueda decidir si va a generar nombres de host.	“Generación de nombres de host de cliente” en la página 326
Determinar la macro de configuración que asignar a los clientes.	Muestra las macros de configuración de cliente para que pueda seleccionar una macro adecuada para los clientes.	“Macros de configuración de cliente predeterminadas” en la página 327
Determinar los tipos de permisos que utilizar.	Muestra los tipos de permisos para ayudarle a determinar cuál es mejor para sus clientes DHCP.	“Tipos de permiso dinámico y permanente” en la página 328

Número e intervalos de direcciones IP

Durante la configuración inicial del servidor, el Administrador de DHCP permite agregar un bloque (o intervalo) de direcciones IP en la administración de DHCP especificando el total de direcciones y la primera dirección del bloque. El Administrador DHCP agrega una lista de direcciones contiguas a partir de esta información. Si cuenta con varios bloques de direcciones no contiguas, puede agregar otros ejecutando de nuevo el Asistente de direcciones del Administrador de DHCP tras la configuración inicial.

Antes de configurar las direcciones IP, debe conocer cuántas direcciones hay en el bloque de direcciones inicial que desea agregar y la dirección IP de la primera dirección del intervalo.

Generación de nombres de host de cliente

La naturaleza dinámica de DHCP significa que una dirección IP no está asociada permanentemente con el nombre de host del sistema que la está utilizando. Las herramientas de administración de DHCP pueden generar un nombre de cliente para asociar con cada dirección IP si selecciona esta opción. Los nombres de cliente se componen de un prefijo, un nombre raíz, más un guión y un número asignado por el servidor. Por ejemplo, si el nombre raíz es `charlie`, los nombres de cliente serán `charlie-1`, `charlie-2`, `charlie-3`, etc.

De modo predeterminado, los nombres de clientes generados empiezan por el nombre del servidor DHCP que los administra. Esta estrategia resulta útil en entornos que tienen más de un servidor DHCP porque puede ver rápidamente en las tablas de red de DHCP qué clientes administra un servidor DHCP concreto. Sin embargo, puede cambiar el nombre raíz a un nombre de su elección.

Antes de configurar las direcciones IP, decida si desea que las herramientas de administración de DHCP generen nombres de clientes y, de ser así, qué nombre raíz se debe utilizar para los nombres.

Los nombres de cliente generados se pueden asignar a las direcciones IP de `/etc/inet/hosts`, DNS o NIS+ si especifica que se registren los nombres de host durante la configuración de DHCP. Consulte [“Registro de nombres de host de cliente” en la página 362](#) para obtener más información.

Macros de configuración de cliente predeterminadas

En DHCP una *macro* es un conjunto de opciones de configuración de red y sus valores asignados. El servidor DHCP utiliza las macros para determinar qué información de configuración de red se enviará a un cliente DHCP.

Al configurar el servidor DHCP, las herramientas de administración recopilan información de los archivos del sistema y directamente del usuario a través de consultas o las opciones de la línea de comandos que especifique. Con esta información, las herramientas de administración crean las siguientes macros:

- **Macro de dirección de red:** el nombre de la macro de dirección de red coincide con la dirección IP de la red del cliente. Por ejemplo, si la red es `192.68.0.0`, la macro de la dirección de red recibe el nombre `192.68.0.0`. La macro contiene la información que necesita cualquier cliente que forme parte de la red, como la máscara de subred, la dirección de emisión de red, el enrutador predeterminado o el token de descubrimiento del enrutador, así como el servidor y el dominio NIS/NIS+ si el servidor utiliza NIS/NIS+. Podrían incluirse otras opciones aplicables a la red. La macro de la dirección de red se procesa automáticamente para todos los clientes que se encuentran en dicha red, tal como se describe en [“Orden del procesamiento de macros” en la página 315](#).
- **Macro de configuración regional:** esta macro recibe el nombre de `Local`. Contiene el desfase (en segundos) de la hora universal coordinada (UTC) para especificar la zona horaria. La macro de configuración regional no se procesa automáticamente, pero se incluye en la macro del servidor.
- **Macro del servidor:** el nombre de esta macro coincide con el nombre de host del servidor. Por ejemplo, si el servidor se denomina `pineola`, la macro del servidor también se llamará `pineola`. La macro del servidor contiene información sobre la directiva de permiso, el servidor de tiempo, el dominio DNS y el servidor DNS, y posiblemente otra información que el programa de configuración haya obtenido de los archivos del sistema. La macro del servidor incluye la macro de configuración regional, de modo que el servidor DHCP procesa la macro de configuración regional como parte de la macro de servidor.

Al configurar las direcciones IP para la primera red, debe seleccionar una macro de configuración de cliente para utilizar con todos los clientes DHCP que utilicen las direcciones que está configurando. La macro que selecciona se asigna a las direcciones IP. De modo predeterminado, se selecciona la macro de servidor porque contiene la información que necesitan todos los clientes que utilizan este servidor.

Los clientes reciben las opciones que contiene la macro de dirección de red antes que las opciones de la macro que está asignada a las direcciones IP. Este orden de procesamiento hace que las opciones de la macro del servidor tengan prioridad sobre cualquier opción de la macro de dirección de red. Consulte “[Orden del procesamiento de macros](#)” en la [página 315](#) para obtener más información sobre el orden en el que se procesan las macros.

Tipos de permiso dinámico y permanente

El *tipo de permiso* determina si la directiva de permiso se aplica a las direcciones IP que se están configurando. Durante la configuración inicial del servidor, el Administrador de DHCP permite seleccionar permisos dinámicos o permanentes para las direcciones que se están agregando. Si configura el servidor DHCP con el comando `dhcpconfig`, los permisos son dinámicos.

Cuando una dirección tiene un *permiso dinámico*, el servidor DHCP puede administrar la dirección. El servidor DHCP puede asignar la dirección IP a un cliente, ampliar el tiempo de permiso, detectar cuándo se deja de utilizar una dirección y reclamar la dirección. Si una dirección IP tiene un *permiso permanente*, el servidor DHCP sólo puede asignar la dirección. El cliente es propietario de la dirección hasta que la libere de forma explícita. Cuando se libera la dirección, el servidor puede asignarla a otro cliente. La dirección no está sujeta a la directiva de permiso si la dirección está configurada con un tipo de permiso permanente.

Si se configura un intervalo de direcciones IP, el tipo de permiso que seleccione se aplicará a todas las direcciones del intervalo. Para aprovechar al máximo DHCP, debe utilizar los permisos dinámicos para la mayoría de las direcciones. Posteriormente puede modificar direcciones concretas para convertirlas en permanentes, si es preciso. No obstante, la cantidad total de permisos permanentes debe ser mínima.

Tipos de permisos y direcciones IP reservadas

Las direcciones IP se pueden reservar asignándolas manualmente a clientes específicos. Una dirección reservada se puede asociar con un permiso permanente o un permiso dinámico. Cuando se asigna un permiso permanente a una dirección reservada, se aplica lo siguiente:

- La dirección sólo se puede asignar al cliente que está vinculado a la dirección.
- El servidor DHCP no puede asignar la dirección a otro cliente.
- El servidor DHCP no puede reclamar esta dirección.

Cuando se asigna un permiso dinámico a una dirección reservada, la dirección sólo se puede asignar al cliente que está vinculado a la dirección. Sin embargo, el cliente debe controlar el tiempo del permiso y negociar una ampliación del mismo, como si la dirección no estuviera reservada. Esta estrategia permite controlar mediante la tabla de red cuándo utiliza la dirección el cliente.

No es posible crear direcciones reservadas para todas las direcciones IP durante la configuración inicial. Las direcciones reservadas están diseñadas para utilizarse con moderación para las direcciones individuales.

Planificación de múltiples servidores DHCP

Si desea configurar más de un servidor DHCP para que administre las direcciones IP, tenga en cuenta lo siguiente:

- Divida la agrupación de direcciones IP de modo que cada servidor sea responsable de un intervalo de direcciones y no se solapen las responsabilidades.
- Elija NIS+ como almacén de datos, si está disponible. Si no lo está, seleccione los archivos de texto y especifique un directorio compartido para la ruta absoluta al almacén de datos. El almacén de datos de archivos binarios no se puede compartir.
- Configure cada servidor por separado para que la propiedad de las direcciones se asigne correctamente y las macros del servidor se puedan crear automáticamente.
- Configure los servidores para analizar las opciones y las macros de la tabla `dhcptab` a intervalos específicos de modo que los servidores utilicen la información más reciente. Puede utilizar el Administrador de DHCP para programar la lectura automática de `dhcptab`, tal como se describe en [“Personalización de las opciones de rendimiento del servidor DHCP” en la página 363](#).
- Asegúrese de que todos los clientes puedan acceder a todos los servidores DHCP de modo que se complementen. Un cliente con un permiso de dirección IP válido podría tratar de verificar su configuración o ampliar el permiso cuando no se puede acceder al servidor que posee dicha dirección de cliente. Otro servidor puede responder al cliente si el cliente ha intentado contactar con el servidor principal durante 20 segundos. Si un cliente solicita una dirección IP específica y el servidor que posee dicha dirección no está disponible, uno de los servidores administrará la solicitud. En ese caso, el cliente no recibe la dirección solicitada. El cliente recibe una dirección IP que posee el servidor DHCP que responde.

Planificación de la configuración DHCP de las redes remotas

Tras la configuración DHCP inicial, puede colocar direcciones IP en redes remotas en la administración DHCP. Sin embargo, dado que los archivos del sistema no se guardan de forma local en el servidor, el Administrador de DHCP y `dhcpconfig` no pueden buscar información para proporcionar los valores predeterminados, de modo que el usuario debe facilitar la información. Antes de intentar configurar una red remota, asegúrese de contar con la siguiente información:

- La dirección IP de la red remota.
- La máscara de subred de la red remota. Esta información se puede obtener de la tabla `netmasks` del servicio de nombres. Si la red utiliza archivos locales, busque `/etc/netmasks` en un sistema de la red. Si la red utiliza NIS+, utilice el comando `niscat netmasks.org_dir`. Si la red utiliza NIS, utilice el comando `ypcat -k netmasks.byaddr`. Asegúrese de que la tabla `netmasks` contenga toda la información de topología de todas las subredes que desee administrar.
- El tipo de red. Los clientes se conectan a la red mediante una conexión de red de área local (LAN) o un Protocolo punto a punto (PPP).
- Información de enrutamiento. ¿Los clientes pueden utilizar el descubrimiento de enrutadores? Si no, debe determinar la dirección IP de un enrutador que puedan utilizar.
- El dominio NIS y los servidores NIS, si es preciso.
- El dominio NIS+ y los servidores NIS+, si es preciso.

Consulte “[Cómo agregar redes DHCP](#)” en la [página 369](#) para aprender a agregar redes DHCP.

Selección de la herramienta para configurar DHCP

Cuando haya reunido la información y planificado el servicio DHCP, podrá configurar un servidor DHCP. Puede utilizar el Administrador de DHCP o la utilidad de línea de comandos `dhcpconfig` para configurar un servidor. El Administrador de DHCP permite seleccionar opciones y especificar datos que se utilizan para crear `dhcptab` y las tablas de red que utiliza el servidor DHCP. La utilidad `dhcpconfig` requiere el uso de las opciones de línea de comandos para especificar los datos.

Funciones del Administrador de DHCP

El Administrador de DHCP, una herramienta de GUI basada en la tecnología de Java™, proporciona un asistente para la configuración de DHCP. El asistente de configuración se inicia automáticamente la primera vez que ejecuta el Administrador de DHCP en un sistema que no está configurado como servidor DHCP. El asistente para la configuración de DHCP proporciona una serie de cuadros de diálogo que le solicitan la información básica necesaria

para configurar un servidor: formato del almacén de datos, directiva de permiso, dominios y servidores DNS/NIS/NIS+ y direcciones de enrutadores. El asistente obtiene parte de la información de los archivos del sistema, y el usuario sólo debe confirmar que la información sea correcta o corregirla si es preciso.

A medida que avanza por los cuadros de diálogo y aprueba la información, el daemon del servidor DHCP se inicia en el sistema del servidor. A continuación, se le solicita que inicie el asistente para agregar direcciones para configurar las direcciones IP para la red. Inicialmente sólo se configura la red del servidor para DHCP y se asignan los valores predeterminados a las demás opciones del servidor. Puede volver a ejecutar el Administrador de DHCP una vez completada la configuración inicial para agregar redes y modificar las demás opciones del servidor.

Consulte “[Configuración y desconfiguración de un servidor DHCP utilizando el Administrador de DHCP](#)” en la [página 333](#) para obtener más información sobre el asistente para la configuración de DHCP. Consulte “[Acerca del Administrador de DHCP](#)” en la [página 346](#) para obtener más información acerca del Administrador de DHCP.

Funciones de `dhcpconfig`

La utilidad `dhcpconfig` admite opciones que permiten configurar y desconfigurar un servidor DHCP, así como convertir a un nuevo almacén de datos e importar/exportar datos de otros servidores DHCP. Si configura un servidor DHCP mediante la utilidad `dhcpconfig`, ésta obtiene información de los archivos del sistema que se describen en “[Actualización de archivos de sistema y tablas de máscara de red](#)” en la [página 320](#). No puede ver y confirmar la información que se obtiene de los archivos del sistema del mismo modo que con el Administrador de DHCP. Por tanto, es importante que los archivos del sistema estén actualizados antes de ejecutar `dhcpconfig`. También puede utilizar las opciones de la línea de comandos para modificar los valores que obtendría `dhcpconfig` de los archivos del sistema de modo predeterminado. El comando `dhcpconfig` puede utilizarse en secuencias. Consulte la página del comando `man dhcpconfig(1M)` para obtener más información.

Comparación del Administrador de DHCP y `dhcpconfig`

En la tabla siguiente se resumen las diferencias entre las dos herramientas de configuración del servidor.

TABLA 13–4 Comparación del Administrador de DHCP y el comando `dhcpconfig`

Funciones	Administrador de DHCP	<code>dhcpconfig</code> con opciones
Información de red que se obtiene del sistema.	Permite ver la información obtenida de los archivos del sistema, y cambiarla si es preciso.	Puede especificar la información de red con las opciones de la línea de comandos.
Configuración rápida.	Acelera el proceso de configuración al omitir la solicitud de opciones de servidor que no son imprescindibles y utilizar los valores predeterminados para ellas. Puede cambiar las opciones no imprescindibles tras la configuración inicial.	Proceso de configuración más rápido, pero es posible que necesite especificar los valores de múltiples funciones.

El [Capítulo 14, “Configuración del servicio DHCP \(tareas\)”](#) incluye los procedimientos que puede seguir para configurar el servidor con el Administrador de DHCP o la utilidad `dhcpconfig`.

Configuración del servicio DHCP (tareas)

Al configurar el servicio DHCP en la red, se configura e inicia el primer servidor DHCP. Más adelante, puede agregar otros servidores DHCP, que accedan a los mismos datos desde una ubicación compartida si el almacén de datos admite datos compartidos. En este capítulo se describen las tareas que permiten configurar el servidor DHCP y colocar las redes y sus direcciones IP asociadas en la administración de DHCP. En este capítulo también se explica cómo anular la configuración de un servidor DHCP.

Cada tarea incluye un procedimiento para ayudarle a realizar la tarea en el Administrador de DHCP y un procedimiento para la tarea equivalente con la utilidad `dhcpconfig`. Este capítulo contiene la información siguiente:

- “Configuración y desconfiguración de un servidor DHCP utilizando el Administrador de DHCP” en la página 333
- “Configuración y desconfiguración de un servidor DHCP mediante los comandos `dhcpconfig`” en la página 341

Si tiene problemas para configurar el servicio DHCP, consulte el [Capítulo 17, “Solución de problemas de DHCP \(referencia\)”](#).

Después de configurar el servicio DHCP, consulte el [Capítulo 15, “Administración de DHCP \(tareas\)”](#) para obtener información sobre la administración del servicio DHCP.

Configuración y desconfiguración de un servidor DHCP utilizando el Administrador de DHCP

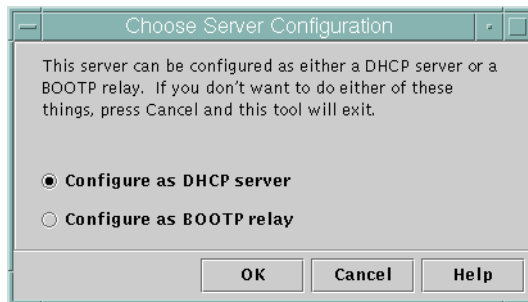
En esta sección se incluyen los procedimientos para configurar y desconfigurar un servidor DHCP con el Administrador de DHCP. Debe ejecutar un sistema de ventanas X como CDE o GNOME para utilizar el Administrador de DHCP.

El Administrador de DHCP se puede ejecutar como superusuario con el comando `/usr/sadm/admin/bin/dhcpmgr`. Consulte [“Acerca del Administrador de DHCP”](#)

en la [página 346](#) para obtener información general sobre la utilidad. Consulte “[Cómo iniciar y detener el servicio DHCP \(Administrador de DHCP\)](#)” en la [página 351](#) para obtener información más detallada sobre la ejecución del Administrador de DHCP.

Al ejecutar el Administrador de DHCP en un servidor que no esté configurado para DHCP, se muestra la siguiente pantalla. Puede especificar si desea configurar un servidor DHCP o un agente de reenvío BOOTP.

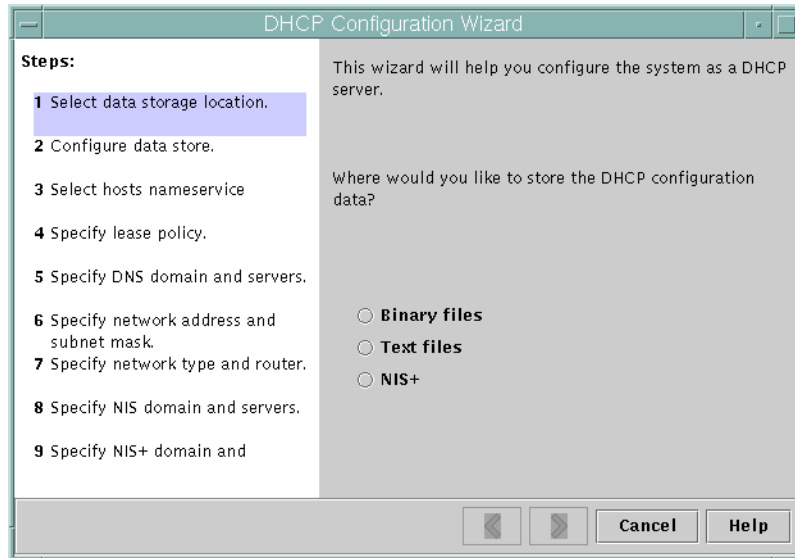
FIGURA 14-1 Cuadro de diálogo de selección de configuración del servidor en el Administrador de DHCP



Configuración de servidores DHCP

Al configurar un servidor DHCP, el Administrador de DHCP inicia el asistente para la configuración de DHCP, que le solicita la información necesaria para configurar el servidor. En la figura siguiente se muestra la pantalla inicial del asistente.

FIGURA 14-2 Pantalla inicial del asistente para la configuración de DHCP



Cuando haya completado la información que solicita el asistente, el Administrador de DHCP creará los elementos que se enumeran en la siguiente tabla.

TABLA 14-1 Elementos creados durante la configuración del servidor DHCP

Elemento	Descripción	Contenido
Archivo de configuración del servicio, <code>/etc/inet/dhcpsvc.conf</code>	Registra las palabras clave y los valores para las opciones de configuración del servidor.	Ubicación y tipo de almacén de datos, así como las opciones que se utilizan con <code>in.dhcpd</code> para iniciar el daemon DHCP cuando se inicia el sistema. No edite este archivo manualmente. Debe utilizar <code>dhcpcmgr</code> o <code>dhcpconfig</code> para modificar la información de configuración de DHCP.
tabla <code>dhcptab</code>	El Administrador de DHCP crea una tabla <code>dhcptab</code> si no existe.	Macros y opciones con valores asignados.
Macro de configuración regional (opcional), denominada <code>Locale</code>	Contiene el desfase en segundos de la zona horaria local de la Hora universal (UTC).	Opción <code>UTCoffset</code> con cantidad de segundos asignada.

TABLA 14-1 Elementos creados durante la configuración del servidor DHCP (Continuación)

Elemento	Descripción	Contenido
Macro de servidor, cuyo nombre coincide con el nombre del nodo del servidor	Contiene opciones cuyos valores están determinados por la entrada del administrador que ha configurado el servidor DHCP. Las opciones se aplican a todos los clientes que utilizan las direcciones que posee el servidor.	La macro Local más las siguientes opciones: <ul style="list-style-type: none">■ Timeserv, configurada para apuntar a la dirección IP principal del servidor.■ LeaseTim, configurada con la cantidad de segundos para los permisos.■ LeaseNeg, si ha seleccionado permisos negociables.■ DNSdomain y DNSserv, si se ha configurado DNS.■ Hostname, que <i>no debe</i> tener un valor asignado. La presencia de esta opción indica que el nombre de host debe obtenerse del servicio de nombres.
La macro de dirección de red, cuyo nombre coincide con la dirección de red de la red del cliente	Contiene opciones cuyos valores están determinados por la entrada del administrador que ha configurado el servidor DHCP. Las opciones se aplican a todos los clientes que residen en la red especificada por el nombre de la macro.	Las siguientes opciones: <ul style="list-style-type: none">■ Subnet, configurada con la máscara de subred para la subred local.■ Router, configurada con la dirección IP de un enrutador, o RDiscvyF, para que el cliente utilice el descubrimiento de enrutadores.■ Broadcast, configurada con la dirección IP de emisión. Esta opción sólo está presente si la red no es una red de punto a punto.■ MTU, para la unidad de transmisión máxima■ NISdomain y NISservs, si se ha configurado NIS.■ NIS+dom y NIS+serv, si se ha configurado NIS+.
Tabla de red para la red	Se crea una tabla vacía hasta que se crean las direcciones IP para la red.	No hay contenido hasta que no se agregan direcciones IP.

▼ Cómo configurar un servidor DHCP (Administrador de DHCP)

Antes de empezar

Asegúrese de leer el [Capítulo 13, “Planificación del servicio DHCP \(tareas\)”](#) antes de configurar el servidor DHCP. En concreto, siga las instrucciones de [“Toma de decisiones para la configuración del servidor DHCP \(mapa de tareas\)”](#) en la [página 322](#) para llevar a cabo las siguientes tareas:

- Seleccionar el sistema que se va a utilizar como servidor DHCP.
- Tomar decisiones sobre el almacén de datos, la directiva de permisos y la información de enrutadores.

1 Conviértase en superusuario en el sistema del servidor.

2 Inicie el Administrador de DHCP.

```
#/usr/sadm/admin/bin/dhcpmgr &
```

3 Elija la opción Configure as DHCP Server.

Se abrirá el asistente DHCP Configuration Wizard, que le ayudará a configurar el servidor.

4 Seleccione las opciones o escriba la información que se le solicita, basándose en las decisiones que ha tomado en la fase de planificación.

Si tiene problemas, haga clic en Help en la ventana del asistente para abrir el explorador web y ver la ayuda del asistente DHCP Configuration Wizard.

5 Haga clic en Finish para completar la configuración del servidor cuando haya terminado de especificar la información solicitada.

6 En Start Address Wizard, haga clic en Yes para configurar las direcciones IP para el servidor.

El asistente Add Addresses to Network permite especificar qué direcciones colocar bajo el control de DHCP.

7 Responda a los indicadores de acuerdo con las decisiones que tomó en la fase de planificación.

Consulte [“Toma de decisiones para la administración de direcciones IP \(mapa de tareas\)”](#) en la [página 325](#) para obtener más información. Si tiene problemas, haga clic en Help en la ventana del asistente para abrir el explorador web y ver la ayuda del asistente Add Addresses to Network.

8 Revise las selecciones y haga clic en Finish para agregar las direcciones IP a la tabla de red.

La tabla de red se actualiza con los registros para cada dirección del intervalo especificado.

Véase también Puede agregar más redes al servidor DHCP con el asistente Network Wizard, tal como se describe en [“Cómo agregar redes DHCP” en la página 369](#).

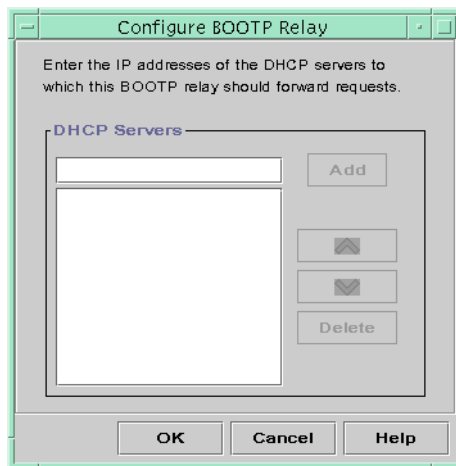
Configuración de los agentes de reenvío de BOOTP

Al configurar un agente de reenvío de BOOTP, el Administrador de DHCP lleva a cabo las siguientes acciones:

- Solicita la dirección IP de uno o más servidores DHCP a los que se deben reenviar las solicitudes.
- Almacena la configuración necesaria para el servicio de reenvío de BOOTP.

La figura siguiente muestra la pantalla que aparece al seleccionar la configuración de un agente de reenvío de BOOTP.

FIGURA 14-3 Configure el cuadro de diálogo BOOTP Relay en el Administrador de DHCP



▼ Cómo configurar un agente de reenvío de BOOTP (Administrador de DHCP)

Antes de empezar Lea el [Capítulo 13, “Planificación del servicio DHCP \(tareas\)”](#) antes de configurar el agente de reenvío de BOOTP. En concreto, consulte [“Selección de un host para ejecutar el servicio DHCP” en la página 322](#) para obtener ayuda para seleccionar el sistema que se va a utilizar.

- 1 **Conviértase en superusuario en el sistema del servidor.**

2 Inicie el Administrador de DHCP.

```
#/usr/sadm/admin/bin/dhcpmgr &
```

Si el sistema no se ha configurado como servidor DHCP o agente de reenvío de BOOTP, se abrirá el asistente DHCP Configuration Wizard. Si el sistema ya se ha configurado como servidor DHCP, primer debe desconfigurar el servidor. Consulte [“Desconfiguración de servidores DHCP y agentes de reenvío de BOOTP” en la página 339.](#)

3 Seleccione Configure as BOOTP Relay.

Se abrirá el cuadro de diálogo Configure BOOTP Relay.

4 Escriba la dirección IP o el nombre de host de uno o más servidores DHCP y haga clic en Add.

Los servidores DHCP especificados deben configurarse para admitir las solicitudes BOOTP o DHCP recibidas por este agente de reenvío de BOOTP.

5 Haga clic en OK para salir del cuadro de diálogo.

Observe que el Administrador de DHCP sólo ofrece el menú File para salir de la aplicación y el menú Service para administrar el servidor. Las opciones de menú desactivadas sólo son útiles en un servidor DHCP.

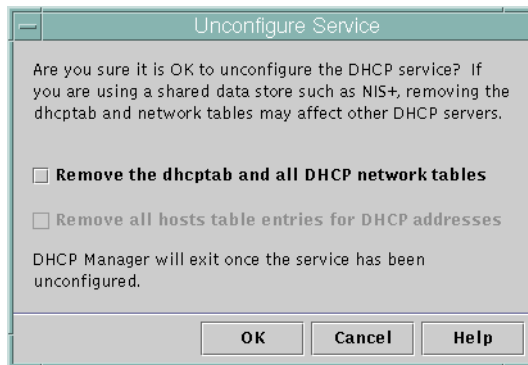
Desconfiguración de servidores DHCP y agentes de reenvío de BOOTP

Al desconfigurar un servidor DHCP o un agente de reenvío de BOOTP, el Administrador de DHCP lleva a cabo las acciones siguientes:

- Detiene el proceso del daemon DHCP (`in.dhpcd`).
- Elimina el archivo `/etc/inet/dhcpsvc.conf`, que registra información sobre el inicio del daemon y la ubicación del almacén de datos.

La figura siguiente muestra la pantalla que aparece al seleccionar la desconfiguración de un servidor DHCP.

FIGURA 14-4 Cuadro de diálogo Unconfigure Service del Administrador de DHCP



Datos DHCP en un servidor desconfigurado

Al desconfigurar un servidor DHCP, debe decidir qué va a hacer con la tabla `dhcpstab` y las tablas de red DHCP. Si los datos están repartidos en varios servidores, no debe eliminar la tabla `dhcpstab` ni las tablas de red DHCP. Si se eliminan, DHCP no se podrá utilizar en la red. Los datos se pueden compartir mediante NIS+ o en sistemas de archivos locales exportados. El archivo `/etc/inet/dhcpsvc.conf` registra el almacén de datos utilizado y su ubicación.

Puede desconfigurar un servidor DHCP pero dejar los datos intactos si no selecciona ninguna de las opciones para eliminar datos. Si desconfigura el servidor y deja los datos intactos, desactivará el servidor DHCP.

Si desea que otro servidor DHCP sea propietario de las direcciones IP, debe mover los datos DHCP al otro servidor DHCP. Los datos deben moverse antes de desconfigurar el servidor actual. Consulte [“Transferencia de datos de configuración entre servidores DHCP \(mapa de tareas\)” en la página 421](#) para obtener más información.

Si está seguro de que desea eliminar los datos, puede seleccionar una opción para eliminar la tabla `dhcpstab` y las tablas de red. Si ha generado nombres de cliente para las direcciones DHCP, también puede eliminar dichas entradas de la tabla de host. Las entradas de nombre de cliente se pueden eliminar de DNS, `/etc/inet/hosts` o NIS+.

Antes de desconfigurar un agente de reenvío de BOOTP, asegúrese de que no haya clientes que dependan de este agente para reenviar solicitudes a un servidor DHCP.

▼ **Cómo desconfigurar un servidor DHCP o un agente de reenvío de BOOTP (Administrador de DHCP)**

1 Conviértase en superusuario.

2 Inicie el Administrador de DHCP.

```
#/usr/sadm/admin/bin/dhcpmgr &
```

3 En el menú Service, elija Unconfigure.

Aparecerá el cuadro de diálogo Desconfigurar servicio. Si el servidor es un agente de reenvío de BOOTP, el cuadro de diálogo permite confirmar la intención de desconfigurar el agente de reenvío. Si el servidor es un servidor DHCP, debe decidir qué hacer con los datos DHCP y realizar las selecciones en el cuadro de diálogo. Consulte la [Figura 14-4](#).

4 (Opcional) Seleccione las opciones para eliminar los datos.

Si el servidor utiliza datos compartidos mediante NIS+ o en archivos compartidos mediante NFS, no seleccione ninguna opción para eliminar los datos. Si el servidor no utiliza datos compartidos, seleccione una o ambas opciones para eliminar los datos.

Consulte “[Datos DHCP en un servidor desconfigurado](#)” en la [página 340](#) para obtener más información acerca de la eliminación de datos.

5 Haga clic en Aceptar para desconfigurar el servidor.

Se cerrarán el cuadro de diálogo Desconfigurar servicio y el Administrador de DHCP.

Configuración y desconfiguración de un servidor DHCP mediante los comandos `dhcpconfig`

En esta sección se incluyen los procedimientos que debe seguir para configurar y desconfigurar un servidor DHCP o un agente de reenvío de BOOTP utilizando `dhcpconfig` con las opciones de línea de comandos.

▼ **Cómo configurar un servidor DHCP (`dhcpconfig -D`)**

Antes de empezar

Asegúrese de leer el [Capítulo 13, “Planificación del servicio DHCP \(tareas\)”](#) antes de configurar el servidor DHCP. En concreto, siga las instrucciones de [“Toma de decisiones para la configuración del servidor DHCP \(mapa de tareas\)”](#) en la [página 322](#) para llevar a cabo las siguientes tareas:

- Seleccionar el sistema que se va a utilizar como servidor DHCP.
- Tomar decisiones sobre el almacén de datos, la directiva de permisos y la información de enrutadores.

1 Inicie sesión en el sistema en el que desee configurar el servidor DHCP.

2 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP”](#) en la [página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

3 Configure el servidor DHCP escribiendo un comando con el siguiente formato:

```
#/usr/sbin/dhcpconfig -D -r datastore -p location
```

`almacén_datos` es uno de los siguientes: `SUNWfiles`, `SUNWbinfiles` o `SUNWnispplus`.

La *ubicación* es la ubicación que depende del almacén de datos donde se desea almacenar los datos DHCP. Para `SUNWfiles` y `SUNWbinfiles`, la ubicación debe ser un nombre de ruta absoluto. Para `SUNWnispplus`, la ubicación debe ser un directorio NIS+ especificado por completo.

Por ejemplo, puede escribir un comando similar al siguiente:

```
dhcpconfig -D -r SUNWbinfiles -p /var/dhcp
```

La utilidad `dhcpconfig` utiliza los archivos de red y los archivos de sistema del host para determinar los valores que se utilizan para configurar el servidor DHCP. Consulte la [página del comando `man dhcpconfig\(1M\)`](#) para obtener información sobre las opciones adicionales para el comando `dhcpconfig` que permiten modificar los valores predeterminados.

4 Agregue una o más redes al servicio DHCP.

Consulte [“Cómo agregar una red DHCP \(`dhcpconfig`\)”](#) en la [página 371](#) para conocer el procedimiento para agregar una red.

▼ **Cómo configurar un agente de reenvío de BOOTP (`dhcpconfig -R`)**

Antes de empezar

Seleccione el sistema que desee utilizar como agente de reenvío de BOOTP, utilizando los requisitos que se mencionan en [“Selección de un host para ejecutar el servicio DHCP” en la página 322](#).

- 1 **Inicie sesión en el servidor que desee configurar como agente de reenvío de BOOTP.**
- 2 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 3 **Configure el agente de reenvío de BOOTP escribiendo un comando con el siguiente formato:**

```
# /usr/sbin/dhcpconfig -R server-addresses
```

Especifique una o más direcciones IP de los servidores DHCP a los que desea reenviar las solicitudes. Si especifica más de una dirección, sepárelas con comas.

Por ejemplo, puede escribir un comando similar al siguiente:

```
/usr/sbin/dhcpconfig -R 192.168.1.18,192.168.42.132
```

▼ **Cómo desconfigurar un servidor DHCP o un agente de reenvío de BOOTP (`dhcpconfig -U`)**

- 1 **Inicie sesión en el servidor DHCP o el sistema de agente de reenvío de BOOTP que desee desconfigurar.**
- 2 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

3 Desconfigure el servidor DHCP o el agente de reenvío de BOOTP:

`/usr/sbin/dhcpconfig -U`

Si el servidor no utiliza datos compartidos, también puede utilizar la opción `-x` para eliminar `dhcptab` y las tablas de red. Si el servidor utiliza datos compartidos, no utilice la opción `-x`. La opción `-h` puede utilizarse para eliminar nombres de host de la tabla `host`. Consulte la página del comando `man dhcpconfig(1M)` para obtener más información sobre las opciones `dhcpconfig`.

Consulte “[Datos DHCP en un servidor desconfigurado](#)” en la página 340 para obtener más información acerca de la eliminación de datos.

Administración de DHCP (tareas)

En este capítulo se describen las tareas que le pueden ser de utilidad durante la administración del servicio DHCP. El capítulo incluye las tareas para el servidor, el agente de reenvío de BOOTP y el cliente. Cada tarea incluye un procedimiento para ayudarlo a realizar la tarea en el Administrador de DHCP y un procedimiento para desempeñar una tarea equivalente con las utilidades de línea de comandos de DHCP. Las utilidades de línea de comandos de DHCP se describen con mayor detalle en las páginas de comando man.

Antes de continuar con este capítulo, debe haber completado la configuración inicial del servicio DHCP y la red inicial. El [Capítulo 14, “Configuración del servicio DHCP \(tareas\)”](#) trata sobre la configuración de DHCP.

Este capítulo contiene la información siguiente:

- “Acerca del Administrador de DHCP” en la página 346
- “Configuración del acceso de usuario a los comandos de DHCP” en la página 349
- “Cómo iniciar y detener el servicio DHCP” en la página 350
- “Servicio DHCP y Utilidad de gestión de servicios” en la página 352
- “Modificación de las opciones del servicio DHCP (mapa de tareas)” en la página 353
- “Cómo agregar, modificar y eliminar redes DHCP (mapa de tareas)” en la página 366
- “Clientes BOOTP con el servicio DHCP (mapa de tareas)” en la página 376
- “Uso de direcciones IP en el servicio DHCP (mapa de tareas)” en la página 379
- “Cómo usar macros DHCP (mapa de tareas)” en la página 395
- “Uso de opciones DHCP (mapa de tareas)” en la página 406
- “Instalación en red de Oracle Solaris con el servicio DHCP” en la página 415
- “Inicio remoto y clientes de inicio sin disco (mapa de tareas)” en la página 416
- “Configuración de clientes DHCP sólo para recibir información (mapa de tareas)” en la página 418
- “Conversión a un nuevo almacén de datos DHCP” en la página 418
- “Transferencia de datos de configuración entre servidores DHCP (mapa de tareas)” en la página 421

Acerca del Administrador de DHCP

El Administrador de DHCP es una interfaz gráfica de usuario (GUI) que puede utilizar para llevar a cabo las tareas de administración en el servicio DHCP.

Ventana del Administrador de DHCP

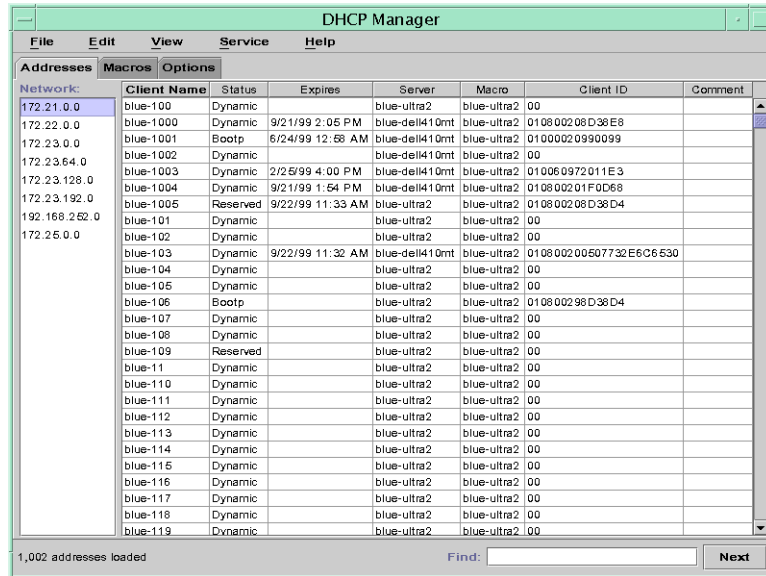
El aspecto de la ventana del Administrador de DHCP depende del modo en que se configura el servidor DHCP en el sistema en el que se ejecuta el Administrador de DHCP.

El Administrador de DHCP utiliza una ventana con fichas cuando el sistema está configurado como servidor DHCP. Debe seleccionar una ficha para el tipo de información con el que desee trabajar. El Administrador de DHCP incluye las siguientes fichas:

- **Ficha Direcciones:** enumera todas las redes y direcciones IP que se incluyen durante la administración de DHCP. En la ficha Direcciones, puede trabajar con las redes y direcciones IP. Puede agregar o eliminar elementos individualmente o por bloques. También puede modificar las propiedades de las redes o direcciones IP individuales o realizar las mismas modificaciones de propiedades de forma simultánea para un bloque de direcciones. Al iniciar el Administrador de DHCP, se abre la ficha Direcciones en primer lugar.
- **Ficha Macros:** enumera todas las macros disponibles de la tabla de configuración de DHCP (dhcptab) y las opciones que contienen las macros. En la ficha Macros, puede crear o eliminar macros. También puede modificar macros agregando opciones y asignándoles valores.
- **Ficha Opciones:** enumera todas las opciones definidas para este servidor DHCP. Las opciones que se enumeran en esta ficha no son las opciones estándar definidas en el protocolo DHCP. Las opciones son extensiones de las opciones estándar, y tienen la clase Extendidas, Distribuidor o Sitio. Las opciones estándar no se pueden modificar de ningún modo, por lo que no se incluyen aquí.

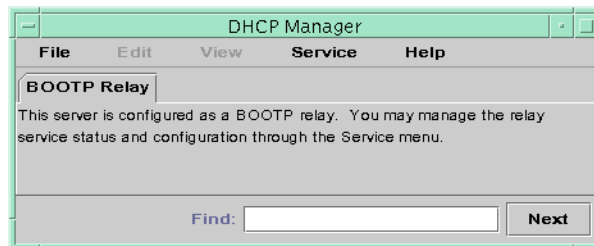
En la figura siguiente se muestra el aspecto que puede tener el Administrador de DHCP al iniciarlo en un servidor DHCP.

FIGURA 15-1 Administrador de DHCP en un sistema de servidor DHCP



Cuando el servidor se configura como agente de reenvíos de BOOTP, la ventana del Administrador de DHCP no incluye estas fichas. El agente de reenvío de BOOTP no necesita la misma información. Sólo puede modificar las propiedades del agente de reenvío de BOOTP y detener o reiniciar el daemon DHCP con el Administrador de DHCP. En la figura siguiente se muestra el aspecto que podría tener el Administrador de DHCP en un sistema configurado como agente de reenvío de BOOTP.

FIGURA 15-2 Administrador de DHCP en un agente de reenvío de BOOTP



Menús del Administrador de DHCP

Los menús del Administrador de DHCP incluyen los siguientes elementos:

- **File:** Cierra el Administrador de DHCP.
- **Edit:** Lleva a cabo tareas de administración para redes, direcciones, macros y opciones.
- **View:** Cambia el aspecto de la ficha seleccionada.
- **Service:** Administra el daemon de DHCP y el almacén de datos.
- **Help:** Abre el explorador web y muestra ayuda para el Administrador de DHCP.

Cuando el Administrador de DHCP se ejecuta en un agente de reenvío de BOOTP, los menús Edit y View están desactivados.

Todas las tareas de administración de DHCP se llevan a cabo mediante los menús Edit y Service.

Los comandos del menú Edit permiten crear, eliminar y modificar elementos de la ficha seleccionada. Los elementos pueden incluir redes, direcciones, macros y opciones. Si está seleccionada la ficha Addresses, el menú Edit también enumera los asistentes. Los asistentes son conjuntos de cuadros de diálogo que ayudan a crear redes y varias direcciones IP.

El menú Service enumera los comandos que permiten administrar el daemon de DHCP. En el menú Service puede llevar a cabo las tareas siguientes:

- Iniciar y detener el daemon de DHCP.
- Habilitar e inhabilitar el daemon de DHCP.
- Modificar la configuración del servidor.
- Desconfigurar el servidor.
- Convertir el almacén de datos.
- Exportar e importar datos en el servidor.

Cómo iniciar y detener el Administrador de DHCP

Debe ejecutar el Administrador de DHCP en un sistema de servidor DHCP como superusuario. Si necesita ejecutar remotamente el Administrador de DHCP, puede enviar la visualización al sistema utilizando la función de visualización remota de ventanas X.

▼ Cómo iniciar y detener el Administrador de DHCP

- 1 **Conviértase en superusuario en el sistema de servidor DHCP.**

- 2 (Opcional) Si se registra remotamente en el sistema de servidor DHCP, visualice el Administrador de DHCP en el sistema local del modo siguiente.

- a. Escriba lo siguiente en el sistema local:

```
# xhost +server-name
```

- b. Escriba lo siguiente en el sistema de servidor DHCP remoto:

```
# DISPLAY=local-hostname;export DISPLAY
```

- 3 Inicie el Administrador de DHCP.

```
# /usr/sadm/admin/bin/dhcpmgr &
```

Se abrirá la ventana del Administrador de DHCP. Si el servidor se configura como servidor DHCP, la ventana muestra la ficha Direcciones. Si el servidor se configura como agente de reenvío de BOOTP, la ventana no incluirá ninguna ficha.

- 4 Para detener el Administrador de DHCP, elija Exit en el menú File.

Se cerrará la ventana del Administrador de DHCP.

Configuración del acceso de usuario a los comandos de DHCP

De modo predeterminado, sólo el usuario root o el superusuario pueden ejecutar los comandos dhcpconfig, dhtadm y pntadm. Si desea que los usuarios que no sean root puedan utilizar los comandos, puede configurar el control de acceso basado en roles (RBAC) para dichos comandos.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

Las siguientes páginas de comando man también pueden resultarle útiles: [rbac\(5\)](#), [exec_attr\(4\)](#) y [user_attr\(4\)](#).

El procedimiento siguiente explica cómo asignar el perfil de administración de DHCP, que permite al usuario ejecutar los comandos DHCP.

▼ Cómo conceder a los usuarios acceso a los comandos de DHCP

- 1 Asígnese los privilegios de superusuario en el sistema del servidor DHCP.

- 2 **Edite el archivo `/etc/user_attr` para agregar una entrada con el siguiente formato. Agregue una entrada para cada usuario o rol que deba administrar el servicio DHCP.**

```
username:::type=normal;profiles=DHCP Management
```

Por ejemplo, para el usuario `ram`, debe agregar la siguiente entrada:

```
ram:::type=normal;profiles=DHCP Management
```

Cómo iniciar y detener el servicio DHCP

Esta sección describe cómo iniciar y detener el servicio DHCP utilizando el Administrador de DHCP y el comando `dhcpconfig`. El servicio DHCP también se puede iniciar y detener utilizando los comandos de la Utilidad de gestión de servicios (SMF). Consulte [“Servicio DHCP y Utilidad de gestión de servicios” en la página 352](#) para obtener más información sobre el uso de los comandos de SMF con el servicio DHCP.

Para iniciar y detener el servicio DHCP, es preciso llevar a cabo varios niveles de acción para modificar el funcionamiento del daemon de DHCP. Debe comprender lo que significa cada acción para seleccionar el procedimiento correcto con el fin de obtener el resultado deseado. Se aplican las siguientes condiciones:

- Los comandos para **iniciar, detener y reiniciar** afectan al daemon sólo para la sesión actual. Por ejemplo, si detiene el servicio DHCP, el daemon finaliza pero se reinicia al reiniciarse el sistema. La detención del servicio no afecta a las tablas de datos DHCP. Puede utilizar los comandos del Administrador de DHCP o SMF para iniciar y detener temporalmente el servicio DHCP sin habilitar ni inhabilitar el servicio.
- Los comandos para **activar y desactivar** afectan al daemon para la sesión actual y para futuras sesiones. Si inhabilita el servicio DHCP, el daemon que está en ejecución finaliza y no se inicia al reiniciar el servidor. Debe habilitar el daemon de DHCP para que se inicie automáticamente al iniciar el sistema. Las tablas de datos de DHCP no se ven afectadas. Puede utilizar el Administrador de DHCP, el comando `dhcpconfig` o los comandos SMF para habilitar e inhabilitar el servicio DHCP.
- El comando **unconfigure** cierra el daemon, impide que el daemon se inicie al iniciarse el sistema y permite eliminar las tablas de datos de DHCP. Puede utilizar el Administrador de DHCP o el comando `dhcpconfig` para desconfigurar el servicio DHCP. La desconfiguración se describe en el [Capítulo 14, “Configuración del servicio DHCP \(tareas\)”](#).

Nota – Si un servidor tiene varias interfaces de red pero no desea proporcionar servicios DHCP en todas las redes, consulte [“Especificación de interfaces de redes para la supervisión de DHCP” en la página 367](#).

Los siguientes procedimientos le ayudarán a iniciar, detener, habilitar e inhabilitar el servicio DHCP.

▼ Cómo iniciar y detener el servicio DHCP (Administrador de DHCP)

- 1 Asígnese los privilegios de superusuario en el sistema del servidor DHCP.
- 2 Inicie el Administrador de DHCP.
`# /usr/sadm/admin/bin/dhcpmgr &`
- 3 Seleccione una de las siguientes opciones:
 - Elija Start en el menú Service para iniciar el servicio DHCP.
 - Elija Stop en el menú Service para detener el servicio DHCP.
 El daemon de DHCP se detiene hasta que se reinicia o se reinicia el sistema.
 - Elija Restart en el menú Service para detener y reiniciar inmediatamente el servicio DHCP.

▼ Cómo habilitar e inhabilitar el servicio DHCP (Administrador de DHCP)

- En el Administrador de DHCP, siga uno de estos procedimientos:
 - Elija Enable en el menú Service para configurar el daemon DHCP para el inicio automático cuando se inicie el sistema.
 El servicio DHCP se inicia automáticamente cuando se habilita.
 - Elija Disable en el menú Service para evitar que el daemon DHCP se inicie automáticamente cuando se inicie el sistema.
 El servicio DHCP se detiene inmediatamente cuando está inhabilitado.

▼ Cómo habilitar e inhabilitar el servicio DHCP (dhcpconfig -S)

- 1 Inicie sesión en el sistema de servidor DHCP.

2 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349.](#)

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

3 **Elija una de las siguientes opciones:**

- **Para habilitar el servicio DHCP, escriba el comando siguiente:**

```
# /usr/sbin/dhcpconfig -S -e
```

- **Para inhabilitar el servicio DHCP, escriba el comando siguiente:**

```
# /usr/sbin/dhcpconfig -S -d
```

Servicio DHCP y Utilidad de gestión de servicios

La Utilidad de gestión de servicios (SMF) se describe en el [Capítulo 18, “Gestión de servicios \(descripción general\)” de Guía de administración del sistema: administración básica.](#) El comando `svcadm` de SMF se puede utilizar para habilitar e iniciar el servidor DHCP, así como para deshabilitar y detener el servidor DHCP. Sin embargo, los comandos de SMF no se pueden utilizar para modificar las opciones del servicio DHCP que permiten configurar las herramientas de DHCP. En concreto, las opciones de servicio que se almacenan en el archivo `/etc/dhcp/dhcpd.conf` no se pueden configurar utilizando las herramientas de SMF.

La tabla siguiente asigna los comandos de DHCP a los comandos de SMF equivalentes.

TABLA 15-1 Comandos de SMF para tareas de servidor DHCP

Tarea	Comando de DHCP	Comando de SMF
Habilitar el servicio DHCP	<code>dhcpconfig -S -e</code>	<code>svcadm enable svc:/network/dhcp-server</code>
Inhabilitar el servicio DHCP	<code>dhcpconfig -S -d</code>	<code>svcadm disable svc:/network/dhcp-server</code>
Iniciar el servicio de DHCP sólo para la sesión actual	Ninguna	<code>svcadm enable -t svc:/network/dhcp-server</code>
Detener el servicio de DHCP para la sesión actual	Ninguna	<code>svcadm disable -t svc:/network/dhcp-server</code>

TABLA 15-1 Comandos de SMF para tareas de servidor DHCP (Continuación)

Tarea	Comando de DHCP	Comando de SMF
Reiniciar el servicio de DHCP	<code>dhcpconfig -S -r</code>	<code>svcadm restart svc:/network/dhcp-server</code>

Modificación de las opciones del servicio DHCP (mapa de tareas)

Puede cambiar los valores de algunas funciones adicionales del servicio DHCP. Es posible que no haya podido hacerlo durante la configuración inicial del Administrador de DHCP. Para cambiar las opciones del servicio, puede utilizar el cuadro de diálogo Modify Service Options del Administrador de DHCP. También puede especificar las opciones con el comando `dhcpconfig`.

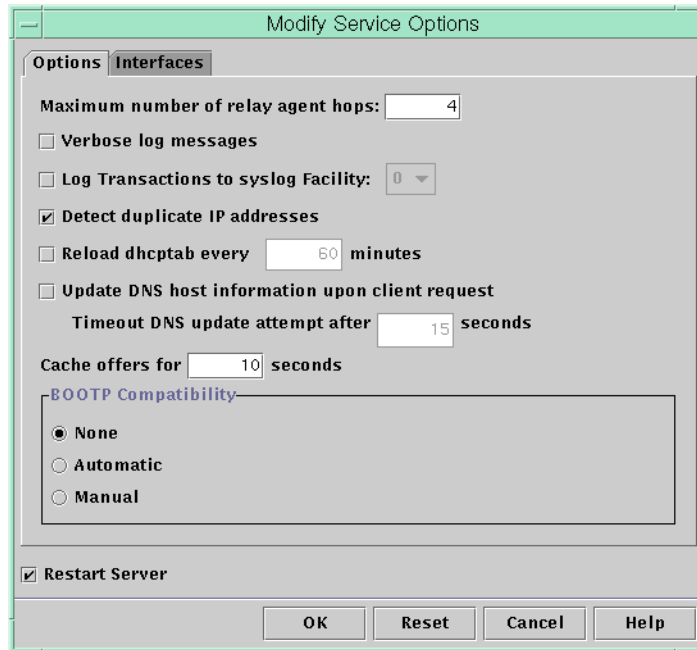
La tabla siguiente describe las tareas que modificación de opciones del servicio DHCP. También incluye vínculos a procedimientos para efectuar cada tarea.

Tarea	Descripción	Para obtener instrucciones
Cambiar opciones de registro.	Habilita o inhabilita el registro, y selecciona una utilidad <code>syslog</code> para utilizar para el registro de transacciones DHCP.	“Cómo generar mensajes de registro DHCP detallados (Administrador de DHCP)” en la página 357 “Cómo generar mensajes de registro DHCP detallados (línea de comandos)” en la página 357 “Cómo habilitar e inhabilitar el registro de transacciones DHCP (Administrador de DHCP)” en la página 358 “Cómo habilitar e inhabilitar el registro de transacciones DHCP (línea de comandos)” en la página 359 “Cómo registrar transacciones DHCP en un archivo <code>syslog</code> independiente” en la página 359
Cambiar opciones de actualización de DNS.	Habilita o inhabilita la función del servidor de agregar entradas de DNS dinámicamente para los clientes que proporcionan un nombre de host. Determina el tiempo máximo que debe dedicar el servidor a intentar actualizar el DNS.	“Cómo activar la actualización de DNS dinámica para los clientes DHCP” en la página 361

Tarea	Descripción	Para obtener instrucciones
Habilitar o inhabilitar la detección de direcciones IP duplicadas.	Habilita o inhabilita la posibilidad del servidor DHCP de determinar si una dirección IP no está siendo utilizada antes de ofrecer la dirección a un cliente.	“Cómo personalizar las opciones de rendimiento DHCP (Administrador de DHCP)” en la página 364 “Cómo personalizar las opciones de rendimiento DHCP (línea de comandos)” en la página 365
Cambiar las opciones para la lectura de información de configuración del servidor DHCP.	Habilita o inhabilita la lectura automática de dhcpcd a intervalos concretos, o cambia el intervalo entre lecturas.	“Cómo personalizar las opciones de rendimiento DHCP (Administrador de DHCP)” en la página 364 “Cómo personalizar las opciones de rendimiento DHCP (línea de comandos)” en la página 365
Cambiar el número de saltos del agente de reenvío.	Aumenta o disminuye el número de redes que puede atravesar una solicitud antes de que el daemon DHCP la coloque.	“Cómo personalizar las opciones de rendimiento DHCP (Administrador de DHCP)” en la página 364 “Cómo personalizar las opciones de rendimiento DHCP (línea de comandos)” en la página 365
Cambiar el tiempo de almacenamiento en caché de una oferta de dirección IP.	Aumenta o disminuye la cantidad de segundos durante los que el servicio DHCP reserva una dirección IP ofrecida antes de ofrecerla a un nuevo cliente.	“Cómo personalizar las opciones de rendimiento DHCP (Administrador de DHCP)” en la página 364 “Cómo personalizar las opciones de rendimiento DHCP (línea de comandos)” en la página 365

La figura siguiente muestra el cuadro de diálogo Modify Service Options del Administrador de DHCP.

FIGURA 15-3 Cuadro de diálogo Modify Service Options del Administrador de DHCP



Cómo cambiar las opciones de registro de DHCP

El servicio DHCP puede registrar mensajes de servicio DHCP y transacciones de DHCP en syslog. Consulte las páginas de comando `man syslogd(1M)` y `syslog.conf(4)` para obtener más información sobre syslog.

Los mensajes del servicio DHCP registrados en syslog incluyen:

- Mensajes de error, que indican las condiciones que impiden al servicio DHCP cumplir los requisitos de un cliente o usuario.
- Advertencias y avisos, que indican condiciones anómalas pero no impiden que el servicio DHCP cumpla una solicitud.

Puede aumentar la cantidad de información que se registra utilizando la opción detallada del daemon DHCP. El resultado del mensaje detallado puede ayudarle a resolver problemas relativos a DHCP. Consulte “[Cómo generar mensajes de registro DHCP detallados \(Administrador de DHCP\)](#)” en la página 357.

Otra técnica de resolución de problemas útil es el registro de transacciones. Las transacciones proporcionan información sobre cualquier intercambio entre un servidor DHCP y reenvío de BOOTP y los clientes. Las transacciones DHCP incluyen los siguientes tipos de mensajes:

- **ASSIGN**: asignación de dirección IP
- **ACK**: el servidor reconoce que el cliente acepta la dirección IP ofrecida, y envía los parámetros de configuración
- **EXTEND**: ampliación del permiso
- **RELEASE**: liberación de dirección IP
- **DECLINE**: el cliente rechaza la asignación de dirección
- **INFORM**: el cliente solicita parámetros de configuración de red pero no una dirección IP
- **NAK**: el servidor no reconoce la solicitud de un cliente para utilizar una dirección IP utilizada previamente
- **ICMP_ECHO**: el servidor detecta que la dirección IP potencial está siendo utilizada por otro host

Las transacciones de reenvío de BOOTP incluyen los siguientes tipos de mensajes:

- **RELAY-CLNT**: el mensaje se reenvía del cliente DHCP a un servidor DHCP
- **RELAY-SRVR**: el mensaje se reenvía del servidor DHCP al cliente DHCP

El registro de transacciones DHCP está inhabilitado de modo predeterminado. Si está activado, el registro de transacciones DHCP utiliza la utilidad `local0` de `syslog` de modo predeterminado. Los mensajes de transacciones DHCP se generan con un nivel de gravedad de `syslog` de *notice*. Este nivel de seguridad hace que las transacciones DHCP se registren en el archivo en el que se registran otros avisos del sistema. Sin embargo, dado que se utiliza la utilidad `local`, los mensajes de transacciones DHCP se pueden registrar por separado de otros avisos. Para registrar los mensajes de transacciones por separado, debe editar el archivo `syslog.conf` para especificar un archivo de registro distinto. Consulte la página de comando [man `syslog.conf`\(4\)](#) para obtener más información sobre el archivo `syslog.conf`.

Puede habilitar o inhabilitar el registro de transacciones, y especificar una utilidad `syslog` diferente, desde `local0` hasta `local7`, tal como se describe en [“Cómo habilitar e inhabilitar el registro de transacciones DHCP \(Administrador de DHCP\)” en la página 358](#). En el archivo `syslog.conf` del sistema del servidor, también puede indicar a `syslogd` que almacene los mensajes de transacciones DHCP en un archivo separado. Consulte [“Cómo registrar transacciones DHCP en un archivo `syslog` independiente” en la página 359](#) para obtener más información.

▼ Cómo generar mensajes de registro DHCP detallados (Administrador de DHCP)

- 1 En el Administrador de DHCP, elija **Modify** en el menú **Service**.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la página 348 para obtener información sobre el Administrador de DHCP.

Se abrirá el cuadro de dialogo **Modify Service Options** con la ficha **Options**. Consulte la [Figura 15–3](#).

- 2 Seleccione **Verbose Log Messages**.

- 3 Seleccione **Restart Server**.

La opción **Restart Server** se encuentra en la parte inferior del cuadro de diálogo.

- 4 Haga clic en **Aceptar**.

El daemon se ejecuta en modo detallado para esta sesión y cada sesión subsiguiente hasta que se restablece esta opción. El modo detallado puede reducir la eficacia del daemon debido al tiempo que necesita para mostrar los mensajes.

▼ Cómo generar mensajes de registro DHCP detallados (línea de comandos)

- 1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte “[Configuración del acceso de usuario a los comandos de DHCP](#)” en la página 349.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 Escriba el comando siguiente para establecer el modo detallado:

```
# /usr/sbin/dhcpconfig -P VERBOSE=true
```

La próxima vez que se inicie el servidor DHCP, se ejecutará en modo detallado hasta que se desactive dicho modo.

Para desactivar el modo detallado, escriba el comando siguiente:

```
# /usr/sbin/dhcpconfig -P VERBOSE=
```

Este comando configura la palabra clave `VERBOSE` con ningún valor, lo que hace que se elimine la palabra clave del archivo de configuración del servidor.

El modo detallado puede reducir la eficacia del daemon debido al tiempo que necesita para mostrar los mensajes.

▼ **Cómo habilitar e inhabilitar el registro de transacciones DHCP (Administrador de DHCP)**

Este procedimiento habilita e inhabilita el registro de transacciones para todas las sesiones de servidor DHCP subsiguientes.

1 En el Administrador de DHCP, elija `Modify` en el menú `Service`.

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.

2 Seleccione `Log Transactions to Syslog Facility`.

Para inhabilitar el registro de transacciones, anule la selección de esta opción.

3 (Opcional) Seleccione una utilidad local de 0 a 7 para utilizar para el registro de transacciones DHCP.

De modo predeterminado, las transacciones DHCP se registran en la ubicación en la que se registran los avisos del sistema, que depende de la configuración de `syslogd`. Si desea que las transacciones DHCP se registren en un archivo independiente de los demás avisos, del sistema, consulte [“Cómo registrar transacciones DHCP en un archivo `syslog` independiente” en la página 359](#).

El tamaño de los archivos de mensajes puede aumentar rápidamente cuando está activado el registro de transacciones.

4 Seleccione `Restart Server`.

5 Haga clic en `Aceptar`.

El daemon registra las transacciones en la utilidad `syslog` seleccionada para esta sesión y cada sesión subsiguiente hasta que se inhabilita el registro.

▼ Cómo habilitar e inhabilitar el registro de transacciones DHCP (línea de comandos)

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP”](#) en la página 349.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Elija uno de estos pasos:**

- **Para habilitar el registro de transacciones DHCP, escriba el comando siguiente:**

```
# /usr/sbin/dhcpconfig -P LOGGING_FACILITY=syslog-local-facility
```

syslog-local-facility es un número del 0 al 7. Si omite esta opción, se utilizará 0.

De modo predeterminado, las transacciones DHCP se registran en la ubicación en la que se registran los avisos del sistema, que depende de la configuración de *syslogd*. Si desea que las transacciones DHCP se registren en un archivo independiente de los demás avisos, del sistema, consulte [“Cómo registrar transacciones DHCP en un archivo *syslog* independiente”](#) en la página 359.

El tamaño de los archivos de mensajes puede aumentar rápidamente cuando está activado el registro de transacciones.

- **Para inhabilitar el registro de transacciones DHCP, escriba el comando siguiente:**

```
# /usr/sbin/dhcpconfig -P LOGGING_FACILITY=
```

No se proporciona ningún valor para el parámetro.

▼ Cómo registrar transacciones DHCP en un archivo *syslog* independiente

- 1 **Adquiera la categoría de superusuario o función equivalente en el sistema de servidores DHCP.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

Un rol al que se asigna un perfil de administración de DHCP podría no ser suficiente para esta tarea. El rol debe tener permiso para editar archivos *syslog*.

2 Edite el archivo `/etc/syslog.conf` en el sistema servidor para agregar una línea con el formato siguiente:

`localn.notice path-to-logfile`

n es el número de utilidad de `syslog` especificado para el registro de transacciones, y *ruta_archivo_registro* es la ruta completa al archivo que se utilizará para registrar transacciones.

Por ejemplo, puede agregar la línea siguiente:

`local0.notice /var/log/dhcpsrv`

Consulte la página de comando `man syslog.conf(4)` para obtener más información sobre el archivo `syslog.conf`.

Habilitación de las actualizaciones DNS dinámicas por parte del servidor DHCP

DNS proporciona servicios de nombre a dirección y de dirección a nombre para Internet. Una vez realizada una asignación DNS, se puede alcanzar un sistema mediante su nombre de host o dirección IP. El sistema también se puede alcanzar desde fuera de su dominio.

El servicio DHCP puede utilizar DNS de dos modos:

- El servidor DHCP puede buscar el nombre de host asignado a una dirección IP que el servidor asigna al cliente. A continuación, el servidor devuelve el nombre de host del cliente junto con el resto de información de configuración del cliente.
- El servidor DHCP puede intentar realizar una asignación de DNS en nombre de un cliente, si el servidor DHCP está configurado para actualizar DNS. El cliente puede proporcionar su propio nombre de host al solicitar el servicio DHCP. Si el servidor DHCP se configura para realizar actualizaciones de DNS, intenta actualizar el servidor DNS con el nombre de host sugerido del cliente. Si la actualización del DNS se realiza correctamente, el servidor DHCP devuelve el nombre de host solicitado al cliente. Si la actualización de DNS no se lleva a cabo correctamente, el servidor DHCP devuelve un nombre de host distinto al cliente.

Puede configurar el servicio DHCP para que actualice el servicio DNS para los clientes DHCP que proporcionen sus propios nombres de host. Para que funcione la actualización de DNS, el servidor DNS, el servidor DHCP y el cliente DHCP deben estar configurados correctamente. Asimismo, el nombre de host solicitado no debe estar en uso por otro sistema del dominio.

La función de actualización de DNS del servidor DHCP funciona si se cumplen las siguientes condiciones:

- El servidor DNS es compatible con RFC 2136.
- El software DNS se basa en BIND v8.2.2, nivel de parche 5 o posterior, tanto si se encuentra en el sistema servidor DHCP como en el sistema servidor DNS.

- El servidor DNS se configura para aceptar las actualizaciones de DNS dinámicas del servidor DHCP.
- El servidor DHCP se configura para llevar a cabo actualizaciones de DNS dinámicas.
- La compatibilidad con DNS se configura para la red del cliente DHCP en el servidor DHCP.
- El cliente DHCP se configura para proporcionar un nombre de host solicitado en su mensaje de solicitud de DHCP.
- El nombre de host solicitado corresponde a una dirección que pertenece a DHCP. El nombre de host podría no tener ninguna dirección correspondiente.

▼ Cómo activar la actualización de DNS dinámica para los clientes DHCP

Nota – Las actualizaciones de DNS dinámicas suponen un *peligro para la seguridad*.

De modo predeterminado, el daemon Oracle Solaris DNS (`in.named`) no permite actualizaciones dinámicas. La autorización para las actualizaciones de DNS dinámicas se concede en el archivo de configuración `named.conf` del sistema de servidor de DNS. No se proporciona ninguna seguridad adicional. Debe considerar detenidamente la conveniencia de esta utilidad para los usuarios teniendo en cuenta el riesgo que plantea la habilitación de actualizaciones de DNS dinámicas.

- 1 En el servidor DNS, edite el archivo `/etc/named.conf` como superusuario.
- 2 Busque la sección `zone` para el dominio adecuado en el archivo `named.conf`.
- 3 Agregue las direcciones IP del servidor DHCP a la palabra clave `allow-update`.

Si la palabra clave `allow-update` no existe, insértela.

Por ejemplo, si el servidor DHCP se encuentra en las direcciones `10.0.0.1` y `10.0.0.2`, el archivo `named.conf` de la zona `dhcp.domain.com` debe modificarse del siguiente modo:

```
zone "dhcp.domain.com" in {
    type master;
    file "db.dhcp";
    allow-update { 10.0.0.1; 10.0.0.2; };
};

zone "10.IN-ADDR.ARPA" in {
    type master;
    file "db.10";
    allow-update { 10.0.0.1; 10.0.0.2; };
};
```

Tenga en cuenta que `allow-update` para ambas zonas debe estar habilitado para permitir al servidor DHCP actualizar tanto los registros A como PTR en el servidor DNS.

4 En el servidor DHCP, inicie el Administrador de DHCP.

```
# /usr/sadm/admin/bin/dhcpmgr &
```

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información más detallada.

5 Elija Modify en el menú Service.

Se abrirá el cuadro de diálogo Modify Service Options.

6 Seleccione Update DNS Host Information Upon Client Request.

7 Especifique el número de segundos que debe esperar una respuesta del servidor DNS antes de desconectar y haga clic en OK.

El valor predeterminado de 15 segundos debe ser suficiente. Si tiene problemas con el tiempo de espera, puede aumentar el valor más adelante.

8 Haga clic en la ficha Macros y asegúrese de especificar el dominio DNS correcto.

La opción DNSdomain debe transferirse con el nombre de dominio correcto a cualquier cliente que requiera asistencia dinámica para la actualización de DNS. De modo predeterminado, DNSdomain se especifica en la macro del servidor, que se utiliza como la macro de configuración vinculada a cada dirección IP.

9 Configure el cliente DHCP para especificar su nombre de host cuando solicite el servicio DHCP.

Si utiliza el cliente DHCP, consulte [“Cómo habilitar un cliente DHCPv4 para que solicite un nombre de host específico” en la página 443](#). Si su cliente no es un cliente DHCP, consulte la documentación de su cliente para obtener información sobre cómo especificar un nombre de host.

Registro de nombres de host de cliente

Si configura el servidor DHCP para que genere nombres de host para las direcciones IP que se colocan en el servicio DHCP, el servidor DHCP puede registrar dichos nombres de host en NIS+, /etc/inet/hosts o los servicios de nombres DNS. El registro del nombre de host no se puede realizar en NIS porque NIS no proporciona un protocolo que permita a los programas actualizar y propagar asignaciones NIS.

Nota – El servidor DHCP puede actualizar DNS con nombres de host generados sólo si el servidor DNS y el servidor DHCP se ejecutan en el mismo sistema.

Si un cliente DHCP proporciona su nombre de host y el servidor DNS está configurado para permitir las actualizaciones dinámicas del servidor DHCP, el servidor DHCP puede actualizar DNS en nombre del cliente. Las actualizaciones dinámicas se pueden realizar aunque los

servidores de DNS y DHCP se ejecuten en distintos sistemas. Consulte [“Habilitación de las actualizaciones DNS dinámicas por parte del servidor DHCP” en la página 360](#) para obtener más información sobre la habilitación de esta función.

La tabla siguiente resume el registro de nombres de host de cliente para los sistemas cliente DHCP con los distintos servicios de nombres.

TABLA 15–2 Registro de nombres de host de cliente en los servicios de nombres

Servicio de nombres	Quién registra el nombre de host	
	Nombre de host generado por DHCP	Nombre de host proporcionado por el cliente DHCP
NIS	Administrador NIS	Administrador NIS
NIS+	Herramientas de DHCP	Herramientas de DHCP
/etc/hosts	Herramientas de DHCP	Herramientas de DHCP
DNS	Herramientas de DHCP, si el servidor DNS se ejecuta en el mismo sistema que el servidor DHCP	Servidor DHCP, si se configura para las actualizaciones de DNS dinámicas
	Administrador de DNS, si el servidor DNS se ejecuta en un sistema diferente	Administrador de DNS, si el servidor DHCP no está configurado para las actualizaciones de DNS dinámicas

Los clientes DHCP pueden solicitar nombres de host específicos en las solicitudes DHCP si están configurados para hacerlo de acuerdo con lo descrito en [“Cómo habilitar un cliente DHCPv4 para que solicite un nombre de host específico” en la página 443](#). Consulte la documentación del proveedor para los demás clientes DHCP con el fin de averiguar si se admite esta posibilidad.

Personalización de las opciones de rendimiento del servidor DHCP

Puede cambiar las opciones que afectan al rendimiento del servidor DHCP. Estas opciones se describen en la tabla siguiente.

TABLA 15-3 Opciones que afectan al rendimiento del servidor DHCP

Opción de servidor	Descripción	Palabra clave
Número máximo de saltos de agentes de reenvío BOOTP	Si una solicitud ha pasado por más de un número específico de agentes de reenvío BOOTP, la solicitud se soltará. El número máximo predeterminado de saltos de agentes de reenvío es cuatro. Este número normalmente es suficiente para la mayoría de las redes. Es posible que una red necesite más de cuatro saltos si las solicitudes DHCP pasan por varios agentes de reenvío BOOTP antes de alcanzar un servidor DHCP.	RELAY_HOPS= <i>entero</i>
Detectar direcciones duplicadas	De modo predeterminado, el servidor establece una conexión ping con una dirección IP antes de ofrecer la dirección a un cliente. Si no hay respuesta para la conexión ping, se verifica que la dirección no esté en uso. Puede inhabilitar esta función para reducir el tiempo que necesita el servidor para realizar una oferta. Sin embargo, al inhabilitar la función existe el riesgo de utilizar direcciones IP duplicadas.	ICMP_VERIFY=TRUE/FALSE
Volver a cargar dhcptab automáticamente a intervalos específicos	El servidor se puede configurar para leer automáticamente dhcptab en el intervalo especificado en minutos. Si la información de configuración de red no cambia con frecuencia y no tiene múltiples servidores DHCP, no es necesario volver a cargar dhcptab automáticamente. Asimismo, el Administrador de DHCP ofrece la opción de que el servidor vuelva a cargar dhcptab tras haber realizado cambios en los datos.	RESCAN_INTERVAL= <i>min</i>
Ofertas de caché de direcciones IP para intervalos específicos	Después de que un servidor ofrezca una dirección IP a un cliente, la oferta se almacena en la memoria caché. Mientras la oferta se encuentre en la memoria caché, el servidor no volverá a ofrecer la dirección. Puede cambiar el número de segundos durante el que se almacena la oferta en la memoria caché. El valor predeterminado es de 10 segundos. En redes más lentas, es posible que tenga que aumentar el tiempo de oferta.	OFFER_CACHE_TIMEOUT= <i>seg</i>

Los procedimientos siguientes describen cómo cambiar estas opciones.

▼ Cómo personalizar las opciones de rendimiento DHCP (Administrador de DHCP)

1 En el Administrador de DHCP, elija Modify en el menú Service.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la [página 348](#) para obtener información sobre el Administrador de DHCP.

2 Cambie las opciones que desee.

Para obtener información sobre las opciones, consulte la [Tabla 15–3](#).

3 Seleccione Restart Server.**4 Haga clic en Aceptar.**

▼ **Cómo personalizar las opciones de rendimiento DHCP (línea de comandos)**

Si cambia las opciones de este procedimiento, las opciones modificadas sólo se utilizarán después de reiniciar el servidor DHCP.

1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte “[Configuración del acceso de usuario a los comandos de DHCP](#)” en la página 349.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

2 Modifique una o más opciones de rendimiento:

```
# /usr/sbin/dhccpconfig -P keyword=value,keyword=value...
```

palabra_clave=valor puede ser cualquiera de las siguientes palabras clave:

RELAY_HOPS=*entero*

Especifica el número máximo de saltos de agentes de reenvío que puede tener lugar antes de que el daemon suelte el datagrama DHCP o BOOTP.

ICMP_VERIFY=TRUE/FALSE

Habilita o inhabilita la detección automática de direcciones IP duplicadas. No se recomienda configurar esta palabra clave como FALSE.

RESCAN_INTERVAL=*minutos*

Especifica el intervalo en minutos que el servidor DHCP debe utilizar para planificar la relectura automática de la información de dhcptab.

OFFER_CACHE_TIMEOUT=*segundos*

Especifica la cantidad de segundos que el servidor DHCP debe almacenar en caché las ofertas que se extienden al descubrimiento de clientes DHCP. El valor predeterminado es de 10 segundos.

Ejemplo 15-1 Configuración de las opciones de rendimiento de DHCP

A continuación se incluye un ejemplo de cómo especificar todas las opciones de comandos.

```
# dhcpconfig -P RELAY_HOPS=2,ICMP_VERIFY=TRUE,\
RESCAN_INTERVAL=30,OFFER_CACHE_TIMEOUT=20
```

Cómo agregar, modificar y eliminar redes DHCP (mapa de tareas)

Al configurar un servidor DHCP, también debe configurar como mínimo una red para poder utilizar el servicio DHCP. Puede agregar más redes en cualquier momento.

La tabla siguiente describe las tareas adicionales que se pueden llevar a cabo cuando se trabaje con redes DHCP después de su configuración inicial. El mapa de tareas incluye vínculos para los procedimientos que permiten llevar a cabo las tareas.

Tarea	Descripción	Para obtener instrucciones
Activar o desactivar el servicio DHCP en las interfaces de red del servidor	El comportamiento predeterminado es supervisar todas las interfaces de red para las solicitudes DHCP. Si no desea que todas las interfaces acepten solicitudes DHCP, puede eliminar una interfaz de la lista de interfaces supervisadas.	“Cómo especificar interfaces de red para la supervisión de DHCP (Administrador de DHCP)” en la página 368
Agregar una nueva red al servicio DHCP.	Coloca una red en la administración de DHCP para administrar las direcciones IP de la red.	“Como agregar una red DHCP (Administrador de DHCP)” en la página 370 “Cómo agregar una red DHCP (dhcpconfig)” en la página 371
Cambiar parámetros de una red administrada por DHCP.	Modifica la información que se pasa a los clientes de una red específica.	“Cómo modificar la configuración de una red DHCP (Administrador de DHCP)” en la página 372 “Cómo modificar la configuración de una red DHCP (dhtadm)” en la página 373
Eliminar una red del servicio DHCP.	Elimina una red para que DHCP deje de administrar las direcciones IP de la red.	“Cómo eliminar una red DHCP (Administrador de DHCP)” en la página 375 “Cómo eliminar una red DHCP (pntadm)” en la página 375

Especificación de interfaces de redes para la supervisión de DHCP

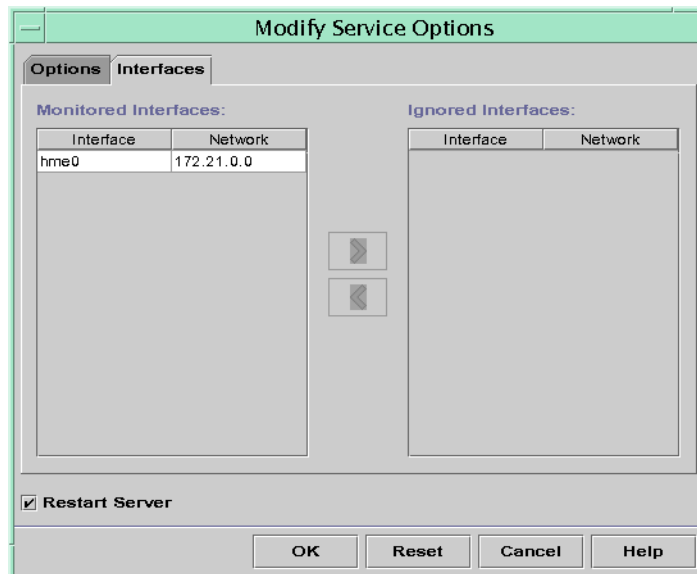
De modo predeterminado, tanto `dhcpconfig` como el asistente de configuración del Administrador de DHCP configuran el servidor DHCP para que supervise todas las interfaces de red del sistema servidor. Si agrega una nueva interfaz de red al sistema servidor, el servidor DHCP supervisa automáticamente la nueva interfaz al iniciar el sistema. A continuación, puede agregar cualquier red que se supervisará mediante la interfaz de red.

Sin embargo, también puede especificar qué interfaces de red se deben supervisar, y cuáles deben omitirse. Puede omitir una interfaz si no desea ofrecer un servicio DHCP en dicha red.

Si especifica que debe omitirse cualquier interfaz y luego instala una interfaz nueva, el servidor DHCP omite la nueva interfaz. Debe agregar la nueva interfaz a la lista de interfaces supervisadas del servidor. Puede especificar las interfaces con el Administrador de DHCP o la utilidad `dhcpconfig`.

Esta sección incluye los procedimientos que permiten especificar qué interfaces de red debe supervisar u omitir DHCP. El procedimiento del Administrador de DHCP utiliza la ficha Interfaces del cuadro de diálogo Modify Service Options del Administrador de DHCP, que se muestra en la figura siguiente.

FIGURA 15-4 Ficha Interfaces del cuadro de diálogo Modify Service Options del Administrador de DHCP



▼ **Cómo especificar interfaces de red para la supervisión de DHCP (Administrador de DHCP)**

- 1 **En el Administrador de DHCP, elija Modify en el menú Service.**

Se muestra el cuadro de diálogo Modify Service Options.

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.

- 2 **Seleccione la ficha Interfaces.**

- 3 **Seleccione la interfaz de red adecuada.**

- 4 **Haga clic en los botones de flechas para mover la interfaz a la lista adecuada.**

Por ejemplo, para omitir una interfaz, selecciónela en la lista Monitored Interfaces y, a continuación, haga clic en el botón de flecha derecha. La interfaz se muestra en la lista Ignored Interfaces.

- 5 **Seleccione Restart Server y haga clic en Aceptar.**

Los cambios que realice persistirán tras los reinicios.

▼ **Cómo especificar las interfaces de red para la supervisión de DHCP (dhcpconfig)**

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Escriba el comando siguiente en el sistema de servidor DHCP:**

```
# /usr/sbin/dhcpconfig -P INTERFACES=int,int,...
```

int, int,... es una lista de interfaces que supervisar. Los nombres de interfaz deben separarse con comas.

Por ejemplo, debe utilizar el siguiente comando para supervisar sólo ge0 y ge1:

```
#/usr/sbin/dhcpconfig -P INTERFACES=ge0,ge1
```


Las interfaces que desea omitir deben omitirse de la línea de comandos `dhcpconfig`.

Los cambios realizados con este comando persistirán tras los reinicios.

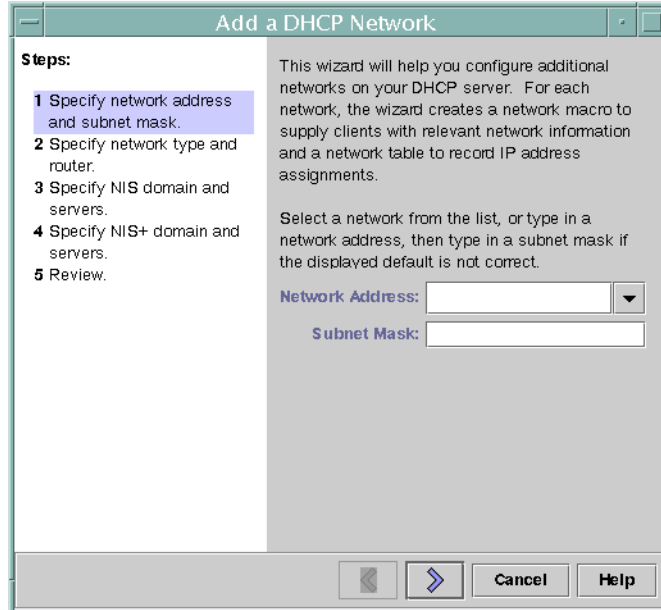
Cómo agregar redes DHCP

Si utiliza el Administrador de DHCP para configurar el servidor, la primera red también se configura a la vez. La primera red es normalmente la red local de la interfaz principal del sistema de servidor. Si desea configurar redes adicionales, utilice el asistente Network Wizard del Administrador de DHCP.

Si utiliza el comando `dhcpconfig -D` para configurar el servidor, debe configurar por separado todas las redes que desee que utilicen el servicio DHCP. Consulte [“Cómo agregar una red DHCP \(dhcpconfig\)” en la página 371](#) para obtener más información.

La figura siguiente muestra el cuadro de diálogo inicial para el asistente Network Wizard del Administrador de DHCP.

FIGURA 15-5 Asistente Network Wizard del Administrador de DHCP



Al configurar una nueva red, el Administrador de DHCP crea los componentes siguientes:

- Una tabla de red en el almacén de datos. La nueva red se muestra en la lista de red de la ficha Addresses del Administrador de DHCP.
- Una macro de red que contiene la información que necesitan los clientes que residen en esta red. El nombre de la macro de red coincide con la dirección IP de la red. La macro de red se agrega a la tabla dhcptab del almacén de datos.

▼ Como agregar una red DHCP (Administrador de DHCP)

1 En el Administrador de DHCP, haga clic en la ficha Addresses.

Aparecerá cualquier red que ya esté configurada para el servicio DHCP.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la [página 348](#) para obtener información sobre el Administrador de DHCP.

2 Elija Network Wizard en el menú Edit.

3 Seleccione las opciones o escriba la información necesaria. Utilice las decisiones que tomó durante la fase de planificación para determinar la información que se debe especificar.

La planificación se describe en “[Planificación de la configuración DHCP de las redes remotas](#)” en la [página 330](#).

Si tiene problemas con el uso del asistente, haga clic en Help en la ventana del asistente. El navegador Web muestra ayuda para el asistente Network Wizard de DHCP.

4 Haga clic en Finish para completar la configuración de la red cuando haya terminado de especificar la información solicitada.

El asistente Network Wizard crea una tabla de red vacía, que aparece en el panel izquierdo de la ventana.

El asistente Network Wizard también crea una macro de red cuyo nombre coincide con la dirección IP de la red.

5 (Opcional) Seleccione la ficha Macros y la macro de red para visualizar el contenido de la macro.

Puede confirmar que la información proporcionada en el asistente se ha insertado como valores para las opciones de la macro de red.

Véase también

Debe agregar direcciones para la red para poder administrar las direcciones IP de la red en DHCP. Consulte “[Cómo agregar direcciones IP al servicio DHCP](#)” en la [página 383](#) para obtener más información.

Si deja vacía la tabla de red, el servidor DHCP puede seguir proporcionando información de configuración a los clientes. Consulte [“Configuración de clientes DHCP sólo para recibir información \(mapa de tareas\)” en la página 418](#) para obtener más información.

▼ Cómo agregar una red DHCP (`dhcpconfig`)

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Escriba el comando siguiente en el sistema de servidor DHCP:**

```
# /usr/sbin/dhcpconfig -N network-address
```

dirección_red es la dirección IP de la red que desea agregar al servicio DHCP. Consulte la página del comando `man dhcpconfig(1M)` para conocer las subopciones que puede utilizar con la opción `-N`.

Si no utiliza las subopciones, `dhcpconfig` utiliza los archivos de red para obtener información sobre la red.

Véase también Debe agregar direcciones para la red para poder administrar las direcciones IP de la red en DHCP. Consulte [“Cómo agregar direcciones IP al servicio DHCP” en la página 383](#) para obtener más información.

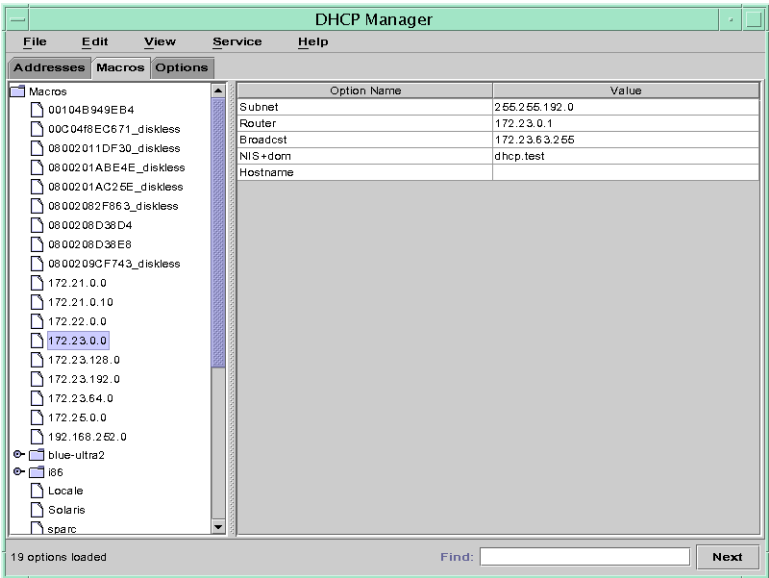
Si deja vacía la tabla de red, el servidor DHCP puede seguir proporcionando información de configuración a los clientes. Consulte [“Configuración de clientes DHCP sólo para recibir información \(mapa de tareas\)” en la página 418](#) para obtener más información.

Modificación de configuraciones de redes DHCP

Tras agregar una red al servicio DHCP, puede modificar la información de configuración que facilitó originalmente. La información de configuración se almacena en la macro de red que se utiliza para transferir información a los clientes de la red. Debe modificar la macro de red para cambiar la configuración de red.

La siguiente figura muestra la ficha Macros del Administrador de DHCP.

FIGURA 15-6 Ficha Macros del Administrador de DHCP



▼ **Cómo modificar la configuración de una red DHCP (Administrador de DHCP)**

- 1 **En el Administrador de DHCP, seleccione la ficha Macros.**
Todas las macros definidas para este servidor DHCP se enumeran en el panel izquierdo.
Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la [página 348](#) para obtener información sobre el Administrador de DHCP.
- 2 **Seleccione la macro de red cuyo nombre coincida con la configuración de red que está modificando.**
El nombre de la macro de red es la dirección IP de red.
- 3 **Elija Properties en el menú Edit.**
El cuadro de diálogo Macro Properties muestra una tabla con las opciones que incluye la macro.
- 4 **Seleccione la opción que desea modificar.**
El nombre de opción y su valor se muestran en los campos de texto en la parte superior del cuadro de diálogo.

- 5 **(Opcional) Modifique el nombre de opción o elija el botón Select para mostrar una lista con los nombres de opciones.**
El cuadro de diálogo Select Option incluye una lista de todas las opciones estándar de DHCP y una breve descripción de cada opción.
- 6 **(Opcional) Seleccione un nombre de opción en el cuadro de diálogo Select Option y haga clic en OK.**
El nuevo nombre de opción se muestra en el campo Option Name.
- 7 **Escriba el nuevo valor para la opción y haga clic en Modify.**
- 8 **(Opcional) También puede agregar opciones a la macro de red eligiendo Select en el cuadro de diálogo.**
Consulte [“Modificación de macros DHCP” en la página 398](#) para obtener más información general acerca de la modificación de macros.
- 9 **Seleccione Notify DHCP Server of Change y haga clic en OK.**
Esta selección indica al servidor DHCP que debe volver a leer la tabla dhcpstab para aplicar el cambio inmediatamente después de hacer clic en OK.

▼ **Cómo modificar la configuración de una red DHCP (dhtadm)**

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**
Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).
Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 **Determine qué macro incluye información para todos los clientes de la red.**
El nombre de la macro de red coincide con la dirección IP de la red.
Si no sabe qué macro incluye esta información, puede visualizar la tabla dhcpstab para ver todas las macros utilizando el comando dhtadm -P.
- 3 **Escriba un comando con el formato siguiente para cambiar el valor de la opción que desee cambiar:**

```
# dhtadm -M -m macro-name -e 'symbol=value' -g
```

Consulte la página del comando `man dhtadm(1M)` para obtener información sobre las opciones de línea de comandos `dhtadm`.

Ejemplo 15-2 Uso del comando `dhtadm` para modificar una macro de DHCP

Por ejemplo, para cambiar el tiempo de permiso de la macro `10.25.62.0` a 57.600 segundos y el dominio NIS a `sem.example.com`, debe escribir los siguientes comandos:

```
# dhtadm -M -m 10.25.62.0 -e 'LeaseTim=57600' -g
```

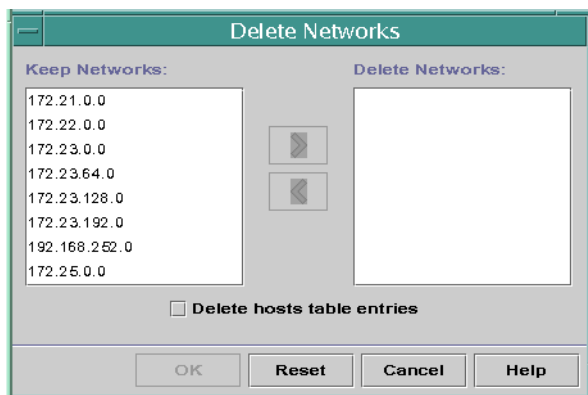
```
# dhtadm -M -m 10.25.62.0 -e 'NISdomain=sem.example.com' -g
```

La opción `-g` hace que el daemon de DHCP vuelva a leer la tabla `dhcptab` y aplique los cambios.

Eliminación de redes DHCP

El Administrador de DHCP permite eliminar varias redes de forma simultánea. Asimismo, tiene la opción de eliminar automáticamente las entradas de la tabla de hosts asociadas con las direcciones IP administradas por DHCP en dichas redes. La figura siguiente muestra el cuadro de diálogo `Delete Networks` del Administrador de DHCP.

FIGURA 15-7 Cuadro de diálogo `Delete Networks` del Administrador de DHCP



El comando `pntadm` requiere la eliminación de cada entrada de dirección IP de una red antes de eliminar dicha red. No puede eliminar más de una red a la vez.

▼ **Cómo eliminar una red DHCP (Administrador de DHCP)**

1 En el Administrador de DHCP, seleccione la ficha Addresses.

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.

2 Elija Delete Networks en el menú Edit.

Se abrirá el cuadro de diálogo Delete Networks.

3 En la lista Keep Networks, seleccione las redes que desee eliminar.

Pulse la tecla Control mientras hace clic con el ratón para seleccionar varias redes. Pulse la tecla Mayús mientras hace clic para seleccionar un intervalo de redes.

4 Haga clic en el botón de flecha derecha para mover las redes seleccionadas a la lista Delete Networks.

5 Si desea eliminar las entradas de tabla host para estas direcciones DHCP de la red, seleccione Delete Host Table Entries.

Tenga en cuenta que al eliminar las entradas de tabla host no se eliminan los registros host del servidor DNS para estas direcciones. Las entradas sólo se eliminan en el servicio de nombres local.

6 Haga clic en Aceptar.

▼ **Cómo eliminar una red DHCP (pntadm)**

Tenga en cuenta que este procedimiento elimina las direcciones IP de red de la tabla de red DHCP antes de eliminar la red. Las direcciones se eliminan para asegurarse de que los nombres de host se eliminen de la base de datos o el archivo hosts.

1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Escriba un comando con el siguiente formato para eliminar una dirección IP y su nombre de host del servicio de nombres:**

```
# pntadm -D -y IP-address
```

Por ejemplo, para eliminar la dirección IP 10.25.52.1, debe escribir el comando siguiente:

```
# pntadm -D -y 10.25.52.1
```

La opción -y especifica que se debe eliminar el nombre de host.

- 3 **Repita el comando pntadm -D -y para cada dirección de la red.**

Puede crear una secuencia para ejecutar el comando pntadm si necesita borrar múltiples direcciones.

- 4 **Una vez eliminadas todas las direcciones, escriba el comando siguiente para eliminar la red del servicio DHCP.**

```
# pntadm -R network-IP-address
```

Por ejemplo, para eliminar la red 10.25.52.0, debe escribir el comando siguiente:

```
# pntadm -R 10.25.52.0
```

Consulte la página del comando man [pntadm\(1M\)](#) para obtener más información sobre la utilidad pntadm.

Cientes BOOTP con el servicio DHCP (mapa de tareas)

Para ofrecer compatibilidad con clientes BOOTP en el servidor DHCP, debe configurar el servidor DHCP para que sea compatible con BOOTP. Si desea especificar qué clientes BOOTP pueden utilizar DHCP, puede registrar los clientes BOOTP en la tabla de red del servidor DHCP. También puede reservar una serie de direcciones IP para la asignación automática a clientes BOOTP.

Nota – Las direcciones BOOTP se asignan permanentemente, tanto si asigna explícitamente un permiso permanente para la dirección como si no lo hace.

La tabla siguiente describe tareas que podrían ser necesarias para la compatibilidad con clientes BOOTP. El mapa de tareas contiene vínculos a los procedimientos que se utilizan para llevar a cabo las tareas.

Tarea	Descripción	Para obtener instrucciones
Configurar compatibilidad automática con BOOTP.	<p>Proporciona la dirección IP para cualquier cliente BOOTP de una red administrada por DHCP, o en una red conectada mediante un agente de reenvío a una red administrada por DHCP.</p> <p>Debe reservar una agrupación de direcciones para uso exclusivo de los clientes BOOTP. Esta opción podría ser más útil si el servidor debe admitir una gran cantidad de clientes BOOTP.</p>	<p>“Cómo configurar la compatibilidad de cualquier cliente BOOTP (Administrador de DHCP)” en la página 377</p>
Configurar compatibilidad manual con BOOTP.	<p>Proporciona una dirección IP sólo para los clientes BOOTP que se han registrado manualmente con el servicio DHCP.</p> <p>Esta opción hace preciso vincular el ID de un cliente a una dirección IP específica que se ha marcado para los clientes BOOTP. Esta opción resulta útil para un número reducido de clientes BOOTP o cuando se desea limitar la cantidad de clientes BOOTP que pueden utilizar el servidor DHCP.</p>	<p>“Cómo configurar la compatibilidad de los clientes BOOTP registrados (Administrador de DHCP)” en la página 378</p>

▼ Cómo configurar la compatibilidad de cualquier cliente BOOTP (Administrador de DHCP)

- 1 En el Administrador de DHCP, seleccione **Modify** en el menú **Service**.

Se abrirá el cuadro de diálogo **Modify Service Options**.

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.

- 2 En la sección **BOOTP Compatibility** del cuadro de diálogo, seleccione **Automatic**.

- 3 Seleccione **Restart Server** y haga clic en **Aceptar**.

- 4 Seleccione la ficha **Addresses**.

- 5 Seleccione las direcciones que desee reservar para los clientes BOOTP.

Seleccione un intervalo de direcciones haciendo clic en la primera dirección, pulsando la tecla **Mayús** y haciendo clic en la última dirección. Seleccione varias direcciones no simultáneas pulsando la tecla **Control** mientras hace clic en cada dirección.

6 Seleccione Properties en el menú Edit.

Se abrirá el cuadro de diálogo Modify Multiple Addresses.

7 En la sección BOOTP, seleccione Assign All Addresses Only to BOOTP Clients.

Las opciones restantes se deben configurar como Keep Current Settings.

8 Haga clic en Aceptar.

Ahora cualquier cliente BOOTP podrá obtener una dirección de este servidor DHCP.

▼ **Cómo configurar la compatibilidad de los clientes BOOTP registrados (Administrador de DHCP)**

1 En el Administrador de DHCP, seleccione Modify en el menú Service.

Se abrirá el cuadro de diálogo Modify Service Options.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la página 348 para obtener información sobre el Administrador de DHCP.

2 En la sección BOOTP Compatibility del cuadro de diálogo, seleccione Manual.

3 Seleccione Restart Server y haga clic en Aceptar.

4 Seleccione la ficha Addresses.

5 Seleccione una dirección que desee asignar a un cliente BOOTP concreto.

6 Elija Properties en el menú Edit.

Se abrirá el cuadro de diálogo Address Properties.

7 En el cuadro de diálogo Address Properties, seleccione la ficha Lease.

8 En el campo Client ID, escriba el identificador del cliente.

Para un cliente BOOTP de &ProductBase en una red Ethernet, el ID de cliente es una cadena que se obtiene de la dirección Ethernet hexadecimal del cliente. El ID de cliente incluye un prefijo que indica el tipo de protocolo de resolución de direcciones (ARP) para Ethernet (01). Por ejemplo, un cliente BOOTP con la dirección Ethernet 8:0:20:94:12:1e utilizaría el ID de cliente 0108002094121E .

Consejo – Como superusuario de un sistema cliente de Oracle Solaris, escriba el comando siguiente para obtener la dirección Ethernet para la interfaz:

```
# ifconfig -a
```

9 Seleccione Reservado para reservar la dirección IP para este cliente.

10 Seleccione Assign Only to BOOTP Clients y haga clic en OK.

En la ficha Addresses, BOOTP se muestra en el campo Status y el ID de cliente especificado aparece en el campo Client ID.

Uso de direcciones IP en el servicio DHCP (mapa de tareas)

Puede utilizar el Administrador de DHCP o el comando `pntadm` para agregar direcciones IP, modificar propiedades de direcciones y eliminar direcciones del servicio DHCP. Antes de trabajar con direcciones IP, debe consultar la [Tabla 15–4](#) para familiarizarse con las propiedades de las direcciones IP. La tabla contiene información para los usuarios del Administrador de DHCP y `pntadm`.

Nota – La [Tabla 15–4](#) incluye ejemplos del uso de `pntadm` para especificar las propiedades de direcciones IP mientras se agregan y modifican las direcciones IP. Consulte también la página del comando `man pntadm(1M)` para obtener más información sobre `pntadm`.

El siguiente mapa de tareas enumera las tareas que se deben llevar a cabo para agregar, modificar o eliminar direcciones IP. El mapa de tareas también contiene vínculos a los procedimientos utilizados para llevar a cabo las tareas.

Tarea	Descripción	Para obtener instrucciones
Agregar una o varias direcciones IP al servicio DHCP.	Agrega direcciones IP en las redes que ya administra el servicio DHCP utilizando el Administrador de DHCP.	“Cómo agregar una única dirección IP (Administrador de DHCP)” en la página 385 “Cómo duplicar una dirección IP existente (Administrador de DHCP)” en la página 385 “Cómo agregar varias direcciones IP (Administrador de DHCP)” en la página 386 “Cómo agregar direcciones IP (pntadm)” en la página 386

Tarea	Descripción	Para obtener instrucciones
Cambiar las propiedades de una dirección IP.	Cambia cualquier propiedad de dirección IP descrita en la Tabla 15–4 .	“Cómo modificar las propiedades de direcciones IP (Administrador de DHCP)” en la página 388 “Cómo modificar las propiedades de direcciones IP (pntadm)” en la página 389
Eliminar direcciones IP del servicio DHCP.	Evita que DHCP utilice las direcciones IP especificadas.	“Cómo marcar direcciones IP como no utilizables (Administrador de DHCP)” en la página 390 “Cómo marcar direcciones IP como inutilizables (pntadm)” en la página 391 “Cómo eliminar direcciones IP del servicio DHCP (Administrador de DHCP)” en la página 392 “Cómo eliminar direcciones IP del servicio DHCP (pntadm)” en la página 392
Asignar una dirección IP coherente a un cliente DHCP.	Configura un cliente para recibir la misma dirección IP cada vez que el cliente solicita su configuración.	“Cómo asignar una dirección IP coherente a un cliente DHCP (Administrador de DHCP)” en la página 394 “Cómo asignar una dirección IP coherente a un cliente DHCP (pntadm)” en la página 395

La tabla siguiente enumera y describe las propiedades de las direcciones IP.

TABLA 15–4 Propiedades de direcciones IP

Propiedad	Descripción	Cómo especificar en el comando <code>pntadm</code>
Dirección de red	La dirección de la red que contiene la dirección IP con la que se está trabajando. La dirección de red se muestra en la lista Networks de la ficha Addresses del Administrador de DHCP.	La dirección de red debe ser el último argumento de la línea de comandos <code>pntadm</code> que se ha utilizado para crear, modificar o eliminar una dirección IP. Por ejemplo, para agregar una dirección IP a la red <code>10.21.0.0</code> , escriba: <code>pntadm -A opciones dirección_IP 10.21.0.0</code>
Dirección IP	La dirección con la que trabaja, tanto si está creando, modificando o eliminando la dirección. La dirección IP se muestra en la primera columna de la ficha Addresses del Administrador de DHCP.	La dirección IP debe acompañar a las opciones <code>-A</code> , <code>-M</code> y <code>-D</code> del comando <code>pntadm</code> . Por ejemplo, para modificar la dirección IP <code>10.21.5.12</code> , escriba: <code>pntadm -M 10.21.5.12 opciones 10.21.0.0</code>

TABLA 15-4 Propiedades de direcciones IP (Continuación)

Propiedad	Descripción	Cómo especificar en el comando <code>pntadm</code>
Nombre del cliente	El nombre de host asignado a la dirección IP de la tabla de hosts. El Administrador de DHCP puede generar automáticamente este nombre cuando se crean las direcciones. Si crea una sola dirección, puede facilitar el nombre.	Especifique el nombre de cliente con la opción <code>-h</code> . Por ejemplo, para especificar el nombre de cliente <code>carrot12</code> para <code>10.21.5.12</code> , escriba: <code>pntadm -M 10.21.5.12 -h carrot12 10.21.0.0</code>
Propiedad de un servidor	El servidor DHCP que administra la dirección IP y responde a la solicitud del cliente DHCP de una asignación de dirección IP.	Especifique el nombre de servidor propietario con la opción <code>-s</code> . Por ejemplo, para especificar el servidor <code>blue2</code> para que sea propietario de <code>10.21.5.12</code> , escriba: <code>pntadm -M 10.21.5.12 -s blue2 10.21.0.0</code>
Macro de configuración	La macro que utiliza el servidor DHCP para obtener las opciones de configuración de red de la tabla <code>dhcptab</code> . Cuando se configura un servidor y se agregan redes se crean automáticamente varias macros. Consulte “Acerca de macros DHCP” en la página 313 si desea más información sobre las macros. Cuando se crean direcciones, también se crea una macro de servidor. La macro de servidor se asigna como macro de configuración para cada dirección.	Especifique el nombre de macro con la opción <code>-m</code> . Por ejemplo, para asignar la macro de servidor <code>blue2</code> a la dirección <code>10.21.5.12</code> , escriba: <code>pntadm -M 10.21.5.12 -m blue2 10.21.0.0</code>
ID de cliente	Cadena de texto que es exclusiva en el servicio DHCP. Si el ID de cliente aparece como <code>00</code> , la dirección no está asignada a ningún cliente. Si especifica un ID de cliente al modificar las propiedades de una dirección IP, la dirección está vinculada exclusivamente a ese cliente. El fabricante del cliente DHCP determina el ID del cliente. Si el cliente no es un cliente DHCP, consulte la documentación del cliente para obtener más información.	Especifique el ID de cliente con la opción <code>-i</code> . Por ejemplo, para asignar el ID de cliente <code>08002094121E</code> a la dirección <code>10.21.5.12</code> , escriba: <code>pntadm -M 10.21.5.12 -i 0108002094121E 10.21.0.0</code>

TABLA 15-4 Propiedades de direcciones IP (Continuación)

Propiedad	Descripción	Cómo especificar en el comando <code>pntadm</code>
	<p>Para los clientes DHCP, el ID de cliente se obtiene de la dirección de hardware hexadecimal del cliente. El ID de cliente incluye un prefijo que representa el código ARP para el tipo de red, como 01 para Ethernet. Los códigos ARP los asigna la Autoridad de números asignados de Internet (IANA) en la sección ARP Parameters del estándar Assigned Numbers en http://www.iana.com/numbers.html</p> <p>Por ejemplo, un cliente de Oracle Solaris con la dirección Ethernet hexadecimal 8:0:20:94:12:1e utiliza el ID de cliente 0108002094121E. El ID de cliente aparece en el Administrador de DHCP y <code>pntadm</code> cuando un cliente está utilizando una dirección.</p> <p>Sugerencia: Como superusuario del sistema cliente de Oracle Solaris, escriba el comando siguiente para obtener la dirección Ethernet para la interfaz: <code>ifconfig -adladm show-phys -m</code></p>	
Reservado	<p>Parámetro que especifica que la dirección está reservada exclusivamente para el cliente indicado por el ID de cliente, y que el servidor DHCP no puede solicitar la dirección. Si elige esta opción, la dirección se asigna manualmente al cliente.</p>	<p>Especifique que la dirección está reservada, o se asigna manualmente, con la opción <code>-f</code>.</p> <p>Por ejemplo, para especificar que la dirección IP 10.21.5.12 está reservada para un cliente, escriba:</p> <p><code>pntadm -M 10.21.5.12 -f MANUAL 10.21.0.0</code></p>
Tipo de permiso o directiva	<p>Parámetro que determina el modo en que DHCP administra el uso que hacen los clientes de las direcciones IP. Un permiso puede ser dinámico o permanente. Consulte “Tipos de permiso dinámico y permanente” en la página 328 para obtener una descripción más detallada al respecto.</p>	<p>Especifique que la dirección está asignada permanentemente con la opción <code>-f</code>. De modo predeterminado, las direcciones obtienen permisos dinámicamente.</p> <p>Por ejemplo, para especificar que la dirección IP 10.21.5.12 tiene un permiso permanente, escriba:</p> <p><code>pntadm -M 10.21.5.12 -f PERMANENT 10.21.0.0</code></p>
Fecha de caducidad del permiso	<p>La fecha en que caduca el permiso, sólo aplicable cuando se especifica un permiso dinámico. La fecha se especifica con el formato <code>mm/dd/aaaa</code>.</p>	<p>Especifique una fecha de caducidad del permiso con la opción <code>-e</code>.</p> <p>Por ejemplo, para especificar la fecha de caducidad 1 de enero de 2006, debe escribir:</p> <p><code>pntadm -M 10.21.5.12 -e 01/01/2006 10.21.0.0</code></p>

TABLA 15-4 Propiedades de direcciones IP (Continuación)

Propiedad	Descripción	Cómo especificar en el comando <code>pntadm</code>
Parámetro BOOTP	Parámetro que marca la dirección como reservada para los clientes BOOTP. Consulte “Clientes BOOTP con el servicio DHCP (mapa de tareas)” en la página 376 para obtener más información sobre la compatibilidad con clientes BOOTP.	Reserve una dirección para los clientes BOOTP con la opción <code>-f</code> . Por ejemplo, para reservar la dirección IP 10.21.5.12 para los clientes BOOTP, debe escribir: <code>pntadm -M 10.21.5.12 -f BOOTP 10.21.0.0</code>
Parámetro inutilizable	Parámetro que marca la dirección para impedir que se asigne a cualquier cliente.	Marque una dirección como inutilizable con la opción <code>-f</code> . Por ejemplo, para marcar la dirección IP 10.21.5.12 como inutilizable, escriba: <code>pntadm -M 10.21.5.12 -f UNUSABLE 10.21.0.0</code>

Cómo agregar direcciones IP al servicio DHCP

Antes de agregar direcciones IP, debe agregar la red que posee las direcciones al servicio DHCP. Consulte [“Cómo agregar redes DHCP” en la página 369](#) para obtener información sobre cómo agregar redes.

Puede agregar direcciones con el Administrador de DHCP o el comando `pntadm`.

En las redes que ya administra el servicio DHCP, puede utilizar el Administrador de DHCP para agregar las direcciones de diferentes modos:

- **Agregue una única dirección IP:** coloque una nueva dirección IP en la administración de DHCP.
- **Duplique una dirección IP existente:** copie las propiedades de una dirección IP existente administrada por DHCP y proporciona una dirección IP y un nombre de cliente nuevos.
- **Agregue un intervalo de múltiples direcciones IP:** utilice el asistente Address Wizard para colocar una serie de direcciones IP en la administración de DHCP.

La siguiente figura muestra el cuadro de diálogo Create Address. El cuadro de diálogo Duplicate Address es idéntico al cuadro de diálogo Create Address, excepto en que los campos de texto muestran los valores para una dirección existente.

FIGURA 15-8 Cuadro de diálogo Create Address del Administrador de DHCP

The 'Create Address' dialog box is shown with the 'Address' tab selected. It includes input fields for 'IP Address', 'Client Name', 'Owned by Server' (containing 'blue-1006'), 'Configuration Macro' (a dropdown menu with 'blue-1006' selected), and 'Comment'. The bottom of the dialog features 'OK', 'Reset', 'Cancel', and 'Help' buttons.

La figura siguiente muestra el primer cuadro de diálogo del asistente Add Addresses to Network, que permite agregar un intervalo de direcciones IP.

FIGURA 15-9 Asistente Add Addresses to Network del Administrador de DHCP

The 'Add Addresses to Network' wizard is displayed. The left pane shows a list of steps: 1. Specify the number of IP addresses. (highlighted), 2. Select the server and starting IP address, 3. Confirm the IP address list, 4. Enter client configuration information, 5. Select the lease type, and 6. Review. The right pane provides instructions: 'This wizard will help you add IP addresses to a DHCP server in one operation. The wizard adds the IP addresses to the selected network table in the DHCP database.' It then asks 'How many addresses do you want to add?' with a 'Number of IP Addresses' field containing the value 10. Below this, it asks 'Why are you adding these addresses? Enter a comment, or leave this space blank.' with a 'Comment' field. The bottom of the wizard features a set of navigation buttons: a back button, a forward button, and 'Cancel' and 'Help' buttons.

▼ **Cómo agregar una única dirección IP (Administrador de DHCP)**

- 1 **En el Administrador de DHCP, seleccione la ficha Addresses.**
Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.
- 2 **Seleccione la red en la que se agregará la nueva dirección IP.**
- 3 **Elija Crear en el menú Editar.**
Se abrirá el cuadro de diálogo Crear dirección.
- 4 **Seleccione o escriba los valores para los parámetros de direcciones en las fichas Address y Lease.**
Pulse el botón Help para abrir un explorador web con ayuda para el cuadro de diálogo. Asimismo, consulte la [Tabla 15-4](#) para obtener información detallada sobre los parámetros.
- 5 **Haga clic en Aceptar.**

▼ **Cómo duplicar una dirección IP existente (Administrador de DHCP)**

- 1 **En el Administrador de DHCP, seleccione la ficha Addresses.**
Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.
- 2 **Seleccione la red en la que se encuentra la nueva dirección IP.**
- 3 **Seleccione la dirección que tenga las propiedades que desea duplicar.**
- 4 **Elija Duplicate en el menú Edit.**
- 5 **Especifique la nueva dirección IP en el campo IP Address.**
- 6 **(Opcional) Especifique un nuevo nombre de cliente para la dirección.**
No puede utilizar el mismo nombre que utilice la dirección que está duplicando.
- 7 **(Opcional) Modifique otros valores de opciones, si es preciso.**
La mayoría de las aplicaciones restantes no se modificarán.
- 8 **Haga clic en Aceptar.**

▼ **Cómo agregar varias direcciones IP (Administrador de DHCP)**

- 1 **En el Administrador de DHCP, seleccione la ficha Addresses.**

Consulte [“Cómo iniciar y detener el Administrador de DHCP”](#) en la página 348 para obtener información sobre el Administrador de DHCP.

- 2 **Seleccione la red en la que se agregarán las nuevas direcciones IP.**

- 3 **Elija Address Wizard en el menú Edit.**

El cuadro de diálogo Add Addresses to Network solicita que especifique valores para las propiedades de direcciones IP. Consulte la [Tabla 15-4](#) para obtener más información sobre las propiedades, o pulse el botón Help del cuadro de diálogo. [“Toma de decisiones para la administración de direcciones IP \(mapa de tareas\)”](#) en la página 325 incluye información más exhaustiva.

- 4 **Haga clic en el botón de flecha derecha cuando finalice cada pantalla, y haga clic en Finish en la última pantalla.**

La ficha Addresses se actualiza con las nuevas direcciones.

▼ **Cómo agregar direcciones IP (pntadm)**

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP”](#) en la página 349.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Agregue direcciones IP escribiendo un comando con el formato siguiente:**

```
# pntadm -A ip-address options network-address
```

Consulte la página del comando `man pntadm(1M)` para ver una lista de las opciones que puede utilizar con `pntadm -A`. Además, la [Tabla 15-4](#) incluye algunos ejemplos de comandos `pntadm` que especifican opciones.

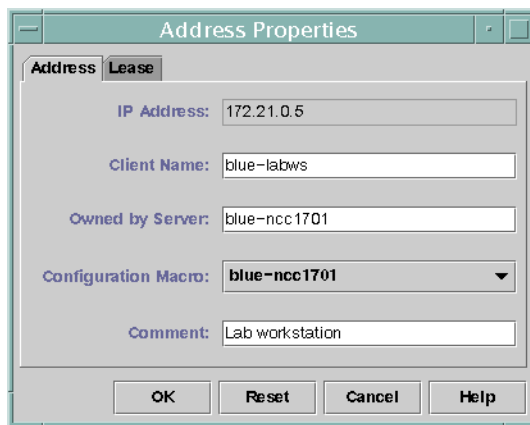
Nota – Puede escribir una secuencia para agregar varias direcciones con `pntadm`. Consulte el [Ejemplo 18-1](#) para obtener un ejemplo.

Modificación de direcciones IP en el servicio DHCP

Puede modificar cualquier propiedad de dirección descrita en la [Tabla 15-4](#) utilizando el Administrador de DHCP o el comando `pntadm -M`. Consulte la página del comando `man pntadm(1M)` para obtener más información sobre `pntadm -M`.

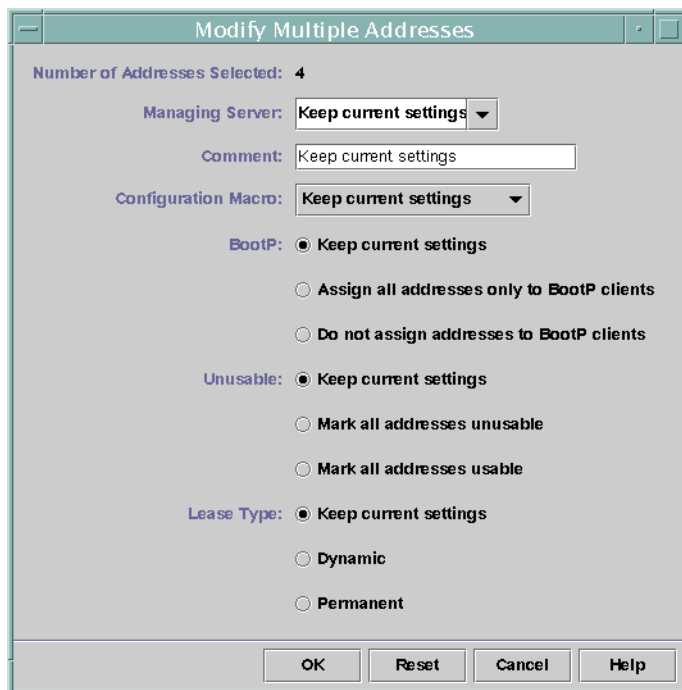
La figura siguiente muestra el cuadro de diálogo Address Properties que se utiliza para modificar las propiedades de direcciones IP.

FIGURA 15-10 Cuadro de diálogo Address Properties del Administrador de DHCP



La figura siguiente muestra el cuadro de diálogo Modify Multiple Addresses que se utiliza para modificar múltiples direcciones IP.

FIGURA 15-11 Cuadro de diálogo Modify Multiple Addresses del Administrador de DHCP



▼ Cómo modificar las propiedades de direcciones IP (Administrador de DHCP)

- 1 En el Administrador de DHCP, seleccione la ficha Addresses.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la [página 348](#) para obtener información sobre el Administrador de DHCP.

- 2 Seleccione la red de la dirección IP.
- 3 Seleccione una o más direcciones IP que modificar.

Si desea modificar más de una dirección, pulse la tecla Control mientras hace clic para seleccionar varias direcciones. También puede pulsar la tecla Mayús mientras hace clic para seleccionar un bloque de direcciones.

- 4 Elija Properties en el menú Edit.

Se abrirá el cuadro de diálogo Address Properties o Modify Multiple Address.

5 Cambie las propiedades que desee.

Haga clic en el botón Help o consulte la [Tabla 15–4](#) para obtener información sobre las propiedades.

6 Haga clic en Aceptar.

▼ **Cómo modificar las propiedades de direcciones IP (pntadm)**

1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP”](#) en la página 349.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

2 Modifique las propiedades de direcciones IP escribiendo un comando con el siguiente formato:

```
# pntadm -M ip-address options network-address
```

Muchas opciones pueden utilizarse con el comando pntadm, que se describe en la página del comando [man pntadm\(1M\)](#).

La [Tabla 15–4](#) incluye algunos ejemplos de comandos pntadm que especifican opciones.

Eliminación de direcciones IP del servicio DHCP

En ocasiones, puede necesitar que el servicio DHCP deje de administrar una dirección IP concreta o un grupo de direcciones IP. El método que utilice para eliminar una dirección de DHCP depende de si desea que el cambio sea temporal o permanente.

- Para impedir temporalmente el uso de direcciones, puede marcarlas como inutilizables en el cuadro de diálogo Address Properties, tal como se describe en [“Cómo marcar direcciones IP como inutilizables para el servicio DHCP”](#) en la página 390.
- Para impedir permanentemente que los clientes DHCP utilicen direcciones, elimine las direcciones de las tablas de red DHCP, tal como se describe en [“Eliminación de direcciones IP del servicio DHCP”](#) en la página 391.

Cómo marcar direcciones IP como inutilizables para el servicio DHCP

Puede utilizar el comando `pntadm -M` con la opción `-f UNUSABLE` para marcar direcciones como inutilizables.

En el Administrador de DHCP, utilice el cuadro de diálogo *Address Properties*, que se muestra en la [Figura 15–10](#), para marcar direcciones individuales. Utilice el cuadro de diálogo *Modify Multiple Addresses*, que se muestra en la [Figura 15–11](#), para marcar varias direcciones, tal como se describe en el procedimiento siguiente.

▼ Cómo marcar direcciones IP como no utilizables (Administrador de DHCP)

- 1 En el Administrador de DHCP, seleccione la ficha *Addresses*.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la [página 348](#) para obtener información sobre el Administrador de DHCP.

- 2 Seleccione la red de la dirección IP.

- 3 Seleccione una o más direcciones IP para marcar como inutilizables.

Si desea marcar más de una dirección como inutilizable, pulse la tecla *Control* mientras hace clic para seleccionar varias direcciones. También puede pulsar la tecla *Mayús* mientras hace clic para seleccionar un bloque de direcciones.

- 4 Elija *Properties* en el menú *Edit*.

Se abrirá el cuadro de diálogo *Address Properties* o *Modify Multiple Address*.

- 5 Si está modificando una dirección, seleccione la ficha *Lease*.

- 6 Seleccione *Address is Unusable*.

Si está editando múltiples direcciones, seleccione *Mark All Addresses Unusable*.

- 7 Haga clic en *Aceptar*.

▼ Cómo marcar direcciones IP como inutilizables (pntadm)

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP”](#) en la página 349.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Marque direcciones IP como inutilizables escribiendo un comando con el formato siguiente:**

```
# pntadm -M ip-address -f UNUSABLE network-address
```

Por ejemplo, para marcar la dirección 10.64.3.3 como inutilizable, escriba:

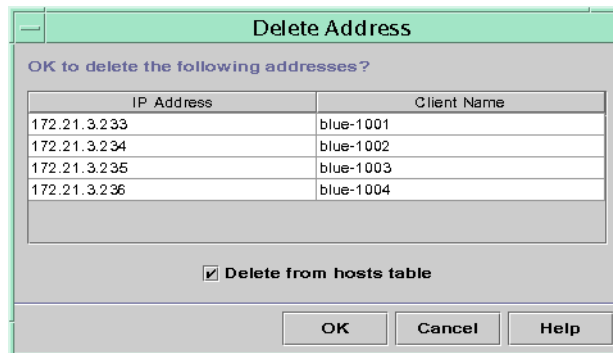
```
pntadm -M 10.64.3.3 -f UNUSABLE 10.64.3.0
```

Eliminación de direcciones IP del servicio DHCP

Debe eliminar las direcciones IP de las tablas de red DHCP si ya no desea que DHCP administre la dirección. Puede utilizar el comando `pntadm -D` o el cuadro de diálogo Delete Address del Administrador de DHCP.

La figura siguiente muestra el cuadro de diálogo Delete Address.

FIGURA 15–12 Cuadro de diálogo Delete Address del Administrador de DHCP



▼ **Cómo eliminar direcciones IP del servicio DHCP (Administrador de DHCP)**

- 1 **En el Administrador de DHCP, seleccione la ficha Addresses.**

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.

- 2 **Seleccione la red de la dirección IP.**

- 3 **Seleccione una o más direcciones IP que eliminar.**

Si desea eliminar más de una dirección, pulse la tecla Control mientras hace clic para seleccionar varias direcciones. También puede pulsar la tecla Mayús mientras hace clic para seleccionar un bloque de direcciones.

- 4 **Elija Delete en el menú Edit.**

El cuadro de diálogo Delete Address enumera las direcciones que ha seleccionado para que pueda confirmar la eliminación.

- 5 **Si desea eliminar los nombres de host de la tabla de hosts, seleccione Delete From Hosts Table.**

Si el Administrador de DHCP generó los nombres de host, puede eliminar los nombres de la tabla de hosts.

- 6 **Haga clic en Aceptar.**

▼ **Cómo eliminar direcciones IP del servicio DHCP (pntadm)**

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Elimine las direcciones IP escribiendo un comando con el formato siguiente:**

```
# pntadm -D ip-address options network-address
```

Si incluye la opción -y, el nombre de host se elimina del servicio de nombres que mantiene el nombre de host.

Por ejemplo, para eliminar la dirección 10.64.3.3 de la red 10.64.3.0, así como eliminar el nombre de host correspondiente, escriba:

```
pntadm -D 10.64.3.3 -y 10.64.3.0
```

Asignación de una dirección IP reservada a un cliente DHCP

El servicio DHCP intenta proporcionar la misma dirección IP a un cliente que ya obtuvo previamente una dirección a través de DHCP. Sin embargo, en ocasiones una dirección ya se ha reasignado a otro cliente.

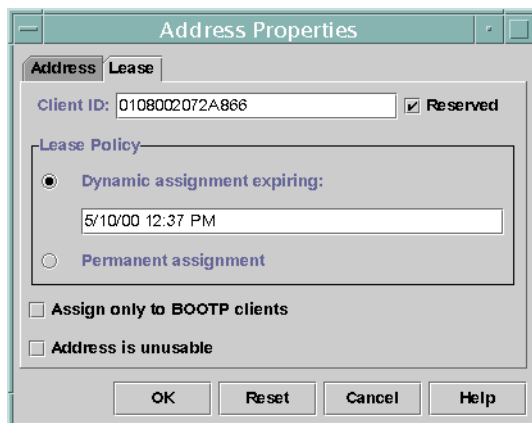
Los enrutadores, servidores NIS o NIS+, servidores DNS y otros hosts que son críticos para la red no deben ser clientes DHCP. Los hosts que proporcionan servicios a la red no deben depender de la red para obtener sus direcciones IP. Los clientes como servidores de impresión o servidores de archivos deben tener direcciones IP coherentes. Estos clientes pueden recibir su configuración de red y también recibir la asignación de una dirección IP coherente del servidor DHCP.

Puede configurar el servidor DHCP para proporcionar la misma dirección IP a un cliente cada vez que el cliente solicite su configuración. La dirección IP se reserva para el cliente asignando manualmente el ID de cliente a la dirección que desea que utilice el cliente. Puede configurar la dirección reservada para que utilice un permiso dinámico o un permiso permanente. Si la dirección del cliente utiliza un permiso dinámico, puede controlar fácilmente el uso de la dirección. Un cliente sin disco es un ejemplo de cliente que debe utilizar una dirección reservada con un permiso dinámico. Si la dirección del cliente utiliza un permiso permanente, no es posible controlar el uso de la dirección. Cuando un cliente obtiene un permiso permanente, no vuelve a ponerse en contacto con el servidor. El cliente sólo puede obtener información de configuración actualizada liberando la dirección IP y volviendo a iniciar la negociación del permiso DHCP.

Puede utilizar el comando `pntadm -M` o el cuadro de diálogo Address Properties del Administrador de DHCP para configurar las propiedades de permisos.

La figura siguiente muestra la ficha Lease del cuadro de diálogo Address Properties, que se utiliza para modificar el permiso.

FIGURA 15-13 Ficha Address Properties Lease del Administrador de DHCP



▼ Cómo asignar una dirección IP coherente a un cliente DHCP (Administrador de DHCP)

- 1 En el Administrador de DHCP, seleccione la ficha Addresses.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la [página 348](#) para obtener información sobre el Administrador de DHCP.

- 2 Seleccione la red adecuada.

- 3 Haga doble clic en la dirección IP que desea que utilice el cliente.

Se abrirá la ventana Address Properties.

- 4 Seleccione la ficha Lease.

- 5 En el campo Client ID, escriba el ID de cliente.

El ID De cliente se obtiene de la dirección de hardware del cliente. Consulte la entrada Client ID en la [Tabla 15-4](#) para obtener más información.

- 6 Seleccione la opción Reserved par impedir que el servidor reclame la dirección IP.

- 7 En el área Lease Policy de la ventana, seleccione Dynamic assignment o Permanent assignment.

Seleccione Dynamic si desea que el cliente negocio la renovación de permisos, lo que permite controlar el uso de la dirección. Dado que ha seleccionado Reserved, la dirección no se puede reclamar aunque se asigne un permiso dinámico. No es necesario especificar una fecha de caducidad para este permiso. El servidor DHCP calcula la fecha de caducidad utilizando el tiempo de permiso.

Si selecciona Permanent, no puede controlar el uso de la dirección IP a menos que active el registro de transacciones.

- 8 Haga clic en Aceptar.

▼ Cómo asignar una dirección IP coherente a un cliente DHCP (pntadm)

- 1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 Defina los indicadores de permiso; para esto, escriba un comando con el formato siguiente:

```
# pntadm -M ip-address -i client-id -f MANUAL+BOOTP network-address
```

Por ejemplo, para habilitar el cliente DHCP cuya dirección MAC es 08:00:20:94:12:1E para que reciba siempre la dirección IP 10.21.5.12, escriba:

```
pntadm -M 10.21.5.12 -i 0108002094121E -f MANUAL+BOOTP 10.21.0.0
```

Consejo – Consulte la entrada Client ID en la [Tabla 15–4](#) para obtener más información sobre cómo determinar los identificadores de cliente.

Cómo usar macros DHCP (mapa de tareas)

Las *macros DHCP* son contenedores de las opciones de DHCP. El servicio DHCP utiliza macros para recopilar las opciones que se deben transferir a los clientes. El Administrador de DHCP y la utilidad `dhcpconfig` crean una serie de macros automáticamente al configurar el servidor.

Consulte [“Acerca de macros DHCP” en la página 313](#) para obtener más información acerca de las macros. Consulte el [Capítulo 14, “Configuración del servicio DHCP \(tareas\)”](#) para obtener información sobre las macros que se crean de modo predeterminado.

Cuando se producen cambios en la red, es posible que tenga que realizar cambios en la información de configuración que se transfiere a los clientes. Para cambiar la información de configuración, debe utilizar macros DHCP. Las macros DHCP se pueden ver, crear, modificar, duplicar y eliminar.

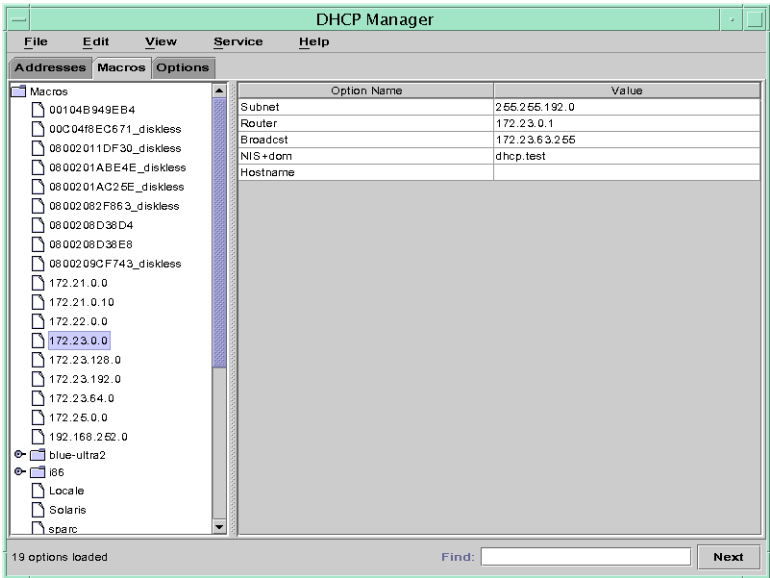
Cuando se utilizan macros, debe conocer las opciones estándar de DHCP, que se describen en la página del comando `man dhcp_inittab(4)`.

El siguiente mapa de tareas enumera las tareas que permiten ver, crear, modificar y eliminar macros DHCP. El mapa también incluye vínculos a secciones que explican cómo realizar cada tarea.

Tarea	Descripción	Para obtener instrucciones
Ver macros DHCP.	Visualiza una lista de todas las macros que se definen en el servidor DHCP.	“Cómo visualizar las macros definidas en un servidor DHCP (Administrador de DHCP)” en la página 397 “Cómo ver las macros definidas en un servidor DHCP (dhtadm)” en la página 398
Crear macros DHCP.	Crea nuevas macros para admitir clientes DHCP.	“Cómo crear una macro DHCP (Administrador de DHCP)” en la página 403 “Cómo crear una macro DHCP (dhtadm)” en la página 404
Modificar valores que se transfieren en macros a los clientes DHCP.	Cambiar las macros modificando las opciones existentes, agregando opciones a las macros o eliminando opciones de las macros.	“Cómo cambiar los valores de las opciones en una macro DHCP (Administrador de DHCP)” en la página 399 “Cómo cambiar los valores de las opciones en una macro DHCP (dhtadm)” en la página 400 “Cómo agregar opciones a una macro DHCP (Administrador de DHCP)” en la página 400 “Cómo agregar opciones a una macro DHCP (dhtadm)” en la página 401 “Como eliminar opciones de una macro DHCP (Administrador de DHCP)” en la página 402 “Como eliminar opciones de una macro DHCP (dhtadm)” en la página 402
Eliminar macros DHCP.	Elimina macros DHCP que ya no se utilizan.	“Cómo eliminar una macro DHCP (Administrador de DHCP)” en la página 405 “Cómo eliminar una macro DHCP (dhtadm)” en la página 406

La figura siguiente muestra la ficha Macros del Administrador de DHCP.

FIGURA 15–14 Ficha Macros del Administrador de DHCP



▼ Cómo visualizar las macros definidas en un servidor DHCP (Administrador de DHCP)

1 En el Administrador de DHCP, seleccione la ficha Macros.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la [página 348](#) para obtener información sobre el Administrador de DHCP.

El área Macros de la izquierda de la ventana incluye todas las macros definidas en el servidor DHCP, ordenadas alfabéticamente. Las macros precedidas de un icono de carpeta incluyen referencias a otras macros, mientras que las que van precedidas de un icono de documento no hacen referencia a otras macros.

2 Para abrir una carpeta de macro, haga clic en el icono identificador a la izquierda del icono de carpeta.

Se enumeran las macros que se incluyen en la macro seleccionada.

3 Para ver el contenido de una macro, haga clic en su nombre.

Se muestran las opciones y sus valores asignados.

▼ Cómo ver las macros definidas en un servidor DHCP (dhtadm)

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP”](#) en la página 349.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Visualice las macros con el siguiente comando:**

```
# dhtadm -P
```

Este comando imprime como resultado estándar el contenido con formato de la tabla `dhcptab`, incluidas todas las macros y los símbolos definidos en el servidor DHCP.

Modificación de macros DHCP

Puede modificar las macros cuando cambie algún aspecto de la red y uno o más clientes DHCP deban conocer el cambio. Por ejemplo, puede agregar un enrutador o un servidor NIS, crear una subred nueva o cambiar la directiva de permisos.

Antes de modificar una macro, determine el nombre de la opción DHCP que desee cambiar, agregar o eliminar. Las opciones DHCP estándar se enumeran en la ayuda del Administrador de DHCP y en la página del comando `man dhcp_inittab(4)`.

Puede utilizar el comando `dhtadm -M -m` o el Administrador de DHCP para modificar las macros. Consulte la página del comando `man dhtadm(1M)` para obtener más información sobre `dhtadm`.

La figura siguiente muestra el cuadro de diálogo Macro Properties del Administrador de DHCP.

FIGURA 15-15 Cuadro de diálogo Macro Properties del Administrador de DHCP

Macro Properties

Name: 172.23.0.0

Contents

Option Name: NIS+dom Select Add

Option Value: dhcp.test Modify

Option Name	Value
Subnet	255.255.192.0
Router	172.23.0.1
Broadcast	172.23.63.255
NIS+dom	dhcp.test
Hostname	

☒ Notify DHCP server of change

OK Reset Cancel Help

▼ Cómo cambiar los valores de las opciones en una macro DHCP (Administrador de DHCP)

- 1 En el Administrador de DHCP, seleccione la ficha Macros.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la página 348 para obtener información sobre el Administrador de DHCP.

- 2 Seleccione la macro que desee cambiar.

- 3 Elija Properties en el menú Edit.

Se abrirá el cuadro de diálogo Macro Properties.

- 4 En la tabla de opciones, seleccione la opción que desee modificar.

El nombre de la opción y su valor se muestran en los campos Option Name y Option Value.

- 5 En el campo Option Value, seleccione el valor antiguo y escriba el nuevo valor para la opción.

- 6 Haga clic en Modify.

El nuevo valor se muestra en la tabla de opciones.

- 7 Seleccione Notify DHCP Server of Change.

Esta selección indica al servidor DHCP que debe volver a leer la tabla dhcpstab para aplicar el cambio inmediatamente después de hacer clic en OK.

- 8 Haga clic en Aceptar.

▼ **Cómo cambiar los valores de las opciones en una macro DHCP (dhtadm)**

- 1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP”](#) en la página 349.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

- 2 Cambie los valores de opciones escribiendo un comando con el formato siguiente:

```
# dhtadm -M -m macroname -e 'option=value:option=value' -g
```

Por ejemplo, para cambiar el tiempo de permiso y el desfase de tiempo universal en la macro bluenote, escriba:

```
# dhtadm -M -m bluenote -e 'LeaseTim=43200:UTCOffset=28800' -g
```

▼ **Cómo agregar opciones a una macro DHCP (Administrador de DHCP)**

- 1 En el Administrador de DHCP, seleccione la ficha Macros.

Consulte [“Cómo iniciar y detener el Administrador de DHCP”](#) en la página 348 para obtener información sobre el Administrador de DHCP.

- 2 Seleccione la macro que desee cambiar.

- 3 Elija Properties en el menú Edit.

Se abrirá el cuadro de diálogo Macro Properties.

- 4 En el campo Option Name, especifique el nombre de una opción mediante uno de estos métodos:
 - Haga clic en el botón Select junto al campo Option Name para seleccionar una opción para agregar a la macro.
 El cuadro de dialogo Select Option muestra una lista ordenada alfabéticamente con los nombres de opciones de categoría estándar y sus descripciones. Si desea agregar una opción que no están en la categoría estándar, utilice la lista Category para seleccionar una categoría.
 Consulte [“Acerca de macros DHCP” en la página 313](#) para obtener más información acerca de las categorías de macros.
 - Escriba Include si desea incluir una referencia a una macro existente en la nueva macro.
- 5 Escriba el valor para la opción en el campo Option Value.
 Si ha escrito Include como nombre de opción, debe especificar el nombre de una macro existente en el campo Option Value.
- 6 Haga clic en Add.
 La opción se agrega en la parte inferior de la lista de opciones de esta macro. Para cambiar la posición de la opción en la macro, seleccione la opción y haga clic en los botones de flecha para subir o bajar una opción en la lista.
- 7 Seleccione Notify DHCP Server of Change.
 Esta selección indica al servidor DHCP que debe volver a leer la tabla dhcpstab para aplicar el cambio inmediatamente después de hacer clic en OK.
- 8 Haga clic en Aceptar.

▼ Cómo agregar opciones a una macro DHCP (dhtadm)

- 1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.
 Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).
 Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 Agregue opciones a una macro escribiendo un comando con el formato siguiente:

```
# dhtadm -M -m macroname -e 'option=value' -g
```

Por ejemplo, para agregar la posibilidad de negociar permisos en la macro `bluenote`, escriba el comando siguiente:

```
# dhtadm -M -m bluenote -e 'LeaseNeg=_NULL_VALUE' -g
```

Si una opción no requiere un valor, debe utilizar `_NULL_VALUE` como valor para la opción.

▼ Como eliminar opciones de una macro DHCP (Administrador de DHCP)

- 1 En el Administrador de DHCP, seleccione la ficha **Macros**.

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la [página 348](#) para obtener información sobre el Administrador de DHCP.

- 2 Seleccione la macro que desee cambiar.

- 3 Elija **Properties** en el menú **Edit**.

Se abrirá el cuadro de diálogo **Macro Properties**.

- 4 Seleccione la opción que desea eliminar de la macro.

- 5 Haga clic en **Delete**.

La opción se elimina de la lista de opciones para esta macro.

- 6 Seleccione **Notify DHCP Server of Change**.

Esta selección indica al servidor DHCP que debe volver a leer la tabla `dhcptab` para aplicar el cambio inmediatamente después de hacer clic en **OK**.

- 7 Haga clic en **Aceptar**.

▼ Como eliminar opciones de una macro DHCP (`dhtadm`)

- 1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte “[Configuración del acceso de usuario a los comandos de DHCP](#)” en la [página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

2 Elimine una opción de una macro escribiendo un comando con el formato siguiente:

```
# dhtadm -M -m macroname -e 'option=' -g
```

Por ejemplo, para eliminar la posibilidad de negociar permisos en la macro `bluenote`, escriba el comando siguiente:

```
# dhtadm -M -m bluenote -e 'LeaseNeg=' -g
```

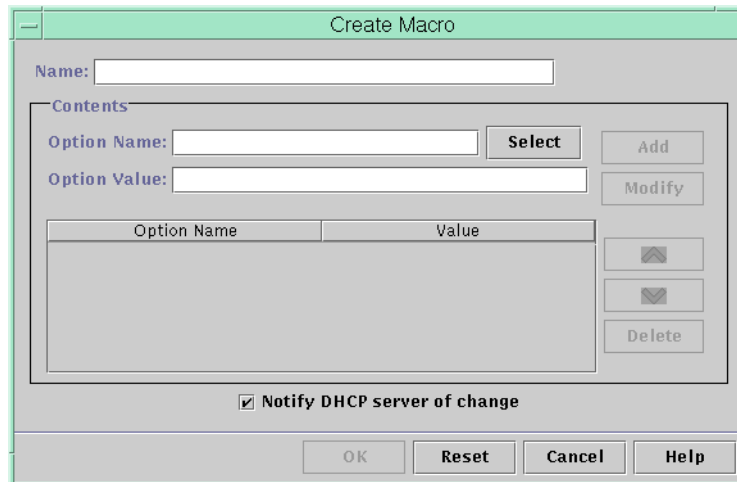
Si se especifica una opción sin ningún valor, la opción se elimina de la macro.

Creación de macros DHCP

Puede agregar nuevas macros en el servicio DHCP para que admitan clientes con necesidades específicas. Puede utilizar el comando `dhtadm -A -m` o el cuadro de diálogo `Create Macro` del Administrador de DHCP para agregar macros. Consulte la página del comando [man dhtadm\(1M\)](#) para obtener más información sobre el comando `dhtadm`.

La figura siguiente muestra el cuadro de diálogo `Create Macro` del Administrador DHCP.

FIGURA 15-16 Cuadro de diálogo `Create Macro` del Administrador de DHCP



▼ Cómo crear una macro DHCP (Administrador de DHCP)

1 En el Administrador de DHCP, seleccione la ficha Macros.

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.

2 Elija Crear en el menú Editar.

Se abrirá el cuadro de diálogo Crear macro.

3 Escriba un nombre exclusivo para la macro.

El nombre puede tener hasta 128 caracteres alfanuméricos. Si utiliza un nombre que coincida con un identificador de clase de proveedor, una dirección de red o un ID de cliente, la macro se procesa automáticamente para los clientes adecuados. Si utiliza un nombre distinto, la macro no se procesa automáticamente. La macro debe asignarse a una dirección IP específica o incluirse en otra macro que se procese automáticamente. Consulte [“Procesamiento de macros con el servidor DHCP” en la página 314](#) para obtener información más detallada.

4 Haga clic en el botón Select, junto al campo Option Name.

El cuadro de diálogo Select Option muestra una lista de los nombres de opciones de categorías estándar, ordenados alfabéticamente, y sus descripciones. Si desea agregar una opción que no están en la categoría estándar, utilice la lista Category. Seleccione la categoría que desee en la lista Category. Consulte [“Acerca de las opciones DHCP” en la página 313](#) para obtener más información sobre las categorías de opciones.

5 Seleccione la opción para agregar a la macro y haga clic en OK.

El cuadro de diálogo Macro Properties muestra la opción seleccionada en el campo Option Name.

6 Escriba el valor para la opción en el campo Option Value y haga clic en Add.

La opción se agrega en la parte inferior de la lista de opciones de esta macro. Para cambiar la posición de la opción en la macro, seleccione la opción y haga clic en los botones de flecha para subir o bajar una opción en la lista.

7 Repita el Paso 5 y el Paso 6 para cada opción que desee agregar a la macro.

8 Seleccione Notify DHCP Server of Change cuando haya terminado de agregar opciones.

Esta selección indica al servidor DHCP que debe volver a leer la tabla dhcpstab para aplicar el cambio inmediatamente después de hacer clic en OK.

9 Haga clic en Aceptar.

▼ **Cómo crear una macro DHCP (dhtadm)**

1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

2 Cree una macro escribiendo un comando con el formato siguiente:

```
# dhtadm -A -m macroname -d ':option=value:option=value:option=value:' -g
```

No hay ningún límite para el número de pares *opción=valor* que se puede incluir en el argumento para -d. El argumento debe empezar y acabar con dos puntos, y tener dos puntos entre cada par *opción=valor*. La cadena completa debe incluirse entre comillas.

Por ejemplo, para crear la macro bluenote, escriba el comando:

```
# dhtadm -A -m bluenote -d ':Router=10.63.6.121\ :LeaseNeg=_NULL_VALUE:DNSserv=10.63.2
```

Si una opción no requiere un valor, debe utilizar `_NULL_VALUE` como valor para la opción.

Eliminación de macros DHCP

Es posible eliminar una macro del servicio DHCP. Por ejemplo, si elimina una red del servicio DHCP, también puede eliminar la macro de red asociada.

Puede utilizar el comando `dhtadm -D -m` o el Administrador de DHCP para eliminar macros.

▼ Cómo eliminar una macro DHCP (Administrador de DHCP)

1 En el Administrador de DHCP, seleccione la ficha Macros.

Consulte [“Cómo iniciar y detener el Administrador de DHCP”](#) en la página 348 para obtener información sobre el Administrador de DHCP.

2 Seleccione la macro que va a eliminar.

El cuadro de diálogo Delete Macro le solicita que confirme que desea eliminar la macro especificada.

3 Seleccione Notify DHCP Server of Change.

Esta selección indica al servidor DHCP que debe volver a leer la tabla `dhcptab` para aplicar el cambio inmediatamente después de hacer clic en OK.

4 Haga clic en Aceptar.

▼ Cómo eliminar una macro DHCP (dhtadm)

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349.](#)

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

- 2 **Elimine una macro escribiendo un comando con el formato siguiente:**

```
# dhtadm -D -m macroname -g
```

Por ejemplo, para eliminar la macro bluenote, debe escribir el comando siguiente:

```
# dhtadm -D -m bluenote -g
```

Uso de opciones DHCP (mapa de tareas)

Las opciones son palabras clave para los parámetros de configuración de red que el servidor DHCP puede transferir a los clientes. En el servicio DHCP, no puede crear, eliminar ni modificar las opciones DHCP estándar. Las opciones estándar se definen mediante el protocolo DHCP, de modo que las opciones no pueden cambiar. Sólo puede realizar tareas en las opciones que cree para el sitio. Por este motivo, al configurar por primera vez el servicio DHCP, la ficha Options del Administrador de DHCP está vacía hasta que se crean las opciones para el sitio.

Si crea opciones en el servidor DHCP, también debe agregar información sobre las opciones en el cliente DHCP. Para el cliente DHCP, debe editar el archivo `/etc/dhcp/inittab` para agregar entradas para las nuevas opciones. Consulte la página del comando `man dhcp_inittab(4)` para obtener más información acerca de este archivo.

Si tiene clientes DHCP que no son clientes de Oracle Solaris, consulte la documentación de los clientes para obtener información sobre cómo agregar opciones o símbolos. Consulte [“Acerca de las opciones DHCP” en la página 313](#) para obtener más información acerca de las opciones en DHCP.

Puede utilizar el Administrador de DHCP o el comando `dhtadm` para crear, modificar o eliminar opciones.

Consejo – Las opciones se denominan *símbolos* en la documentación sobre DHCP. El comando `dhtadm` y su página del comando man relacionada también hacen referencia a las opciones como símbolos.

El siguiente mapa de tareas incluye las tareas que debe realizar para crear, modificar y eliminar opciones DHCP. El mapa de tareas contiene vínculos a los procedimientos necesarios para realizar las tareas.

Tarea	Descripción	Para obtener instrucciones
Crear opciones DHCP.	Agrega nuevas opciones para la información que no cubre una opción DHCP estándar.	“Cómo crear opciones DHCP (Administrador de DHCP)” en la página 410 “Cómo crear opciones DHCP (dhtadm)” en la página 411 “Modificar la información de opciones de cliente DHCP” en la página 415
Modificar opciones DHCP.	Cambia las propiedades de las opciones DHCP que se han creado.	“Cómo modificar las propiedades de opciones DHCP (Administrador de DHCP)” en la página 412 “Cómo modificar las propiedades de opciones DHCP (dhtadm)” en la página 413
Eliminar opciones DHCP.	Elimina las opciones DHCP que se han creado.	“Cómo eliminar opciones DHCP (Administrador de DHCP)” en la página 414 “Cómo eliminar opciones DHCP (dhtadm)” en la página 415

Antes de crear opciones DHCP, debe estar familiarizado con las propiedades de las opciones que se incluyen en la tabla siguiente.

TABLA 15-5 Propiedades de opciones DHCP

Propiedad de opción	Descripción
Category	<p>La <i>categoría</i> de una opción debe ser una de las siguientes:</p> <ul style="list-style-type: none"> ■ Vendor: opciones específicas para la plataforma de proveedor de un cliente, tanto si es hardware como software. ■ Site: opciones específicas del sitio. ■ Extend: opciones más recientes incorporadas al protocolo DHCP, pero que todavía no se han implementado como opciones estándar en DHCP.

TABLA 15-5 Propiedades de opciones DHCP (Continuación)

Propiedad de opción	Descripción
Código	<p>El <i>código</i> es un número exclusivo que se asigna a una opción. No es posible utilizar el mismo código para cualquier otra opción dentro de su categoría de opción. El código debe ser adecuado para la categoría de opción:</p> <ul style="list-style-type: none">■ Vendor: valores de código del 1 al 254 para cada clase de proveedor■ Site: valores de código del 128 al 254■ Extend: valores de código del 77 al 127
Data type	<p>El <i>tipo de datos</i> especifica la clase de datos que se pueden asignar como valor para la opción. En la lista siguiente se incluyen los tipos de datos válidos.</p> <ul style="list-style-type: none">■ ASCII: valor de cadena de texto.■ BOOLEAN: no se asocia ningún valor con el tipo de datos booleano. Si la opción está presente, significa que una condición es verdadera, y si está ausente, indica que una condición es falsa. Por ejemplo, la opción <code>Host name</code> es booleana. La presencia de <code>Host name</code> en una macro hace que el servidor DHCP busque el nombre de host asociado con la dirección asignada.■ IP: una o más direcciones IP, en formato decimal con punto (<code>xxx.xxx.xxx.xxx</code>).■ OCTET: representación ASCII no interpretada de datos binarios. Por ejemplo, un ID de cliente utiliza el tipo de datos de octetos. Los caracteres válidos son 0-9, A-F y a-f. Se necesitan dos caracteres ASCII para representar una cantidad de 8 bits.■ UNNUMBER8, UNNUMBER16, UNNUMBER32, UNNUMBER64, SNUMBER8, SNUMBER16, SNUMBER32 o SNUMBER64: valor numérico. Una U o S iniciales indican si el número está firmado o no. Los dígitos al final indican cuántos bits hay en el número.
Granularidad	<p>La <i>granularidad</i> especifica cuántas "instancias" del tipo de datos se necesitan para representar un valor de opción completo. Por ejemplo, un tipo de datos de IP y una granularidad de 2 indicaría que el valor de opción debe contener dos direcciones IP.</p>
Máximo	<p>El número máximo de valores que se puede especificar para la opción. Por ejemplo, supongamos que el máximo es 2, la granularidad es 2 y el tipo de datos es IP. En ese caso, el valor de opción podría contener un máximo de dos pares de direcciones IP.</p>

TABLA 15-5 Propiedades de opciones DHCP (Continuación)

Propiedad de opción	Descripción
Clases de cliente del proveedor	<p>Esta opción sólo está disponible cuando la categoría de opción es Proveedor. Las clases de cliente del proveedor identifican las clases de cliente con las que está asociada la opción Proveedor. La clase es una cadena ASCII que representa el sistema operativo o el tipo de equipo del cliente. Por ejemplo, la cadena de clase para algunos modelos de estaciones de trabajo de Sun es <code>SUNW.Sun-Blade-100</code>. Este tipo de opción permite definir los parámetros de configuración que se transfieren a los clientes de la misma clase, y <i>sólo</i> a los clientes de esa clase.</p> <p>Puede especificar varias clases de cliente. Sólo los clientes DHCP con un valor de clase de cliente que coincida con la clase que se especifique recibirán las opciones previstas para esa clase.</p> <p>La clase de cliente la determina el proveedor del cliente DHCP. Para los clientes DHCP que no sean clientes de Oracle Solaris, consulte la documentación del proveedor para el cliente DHCP de la clase de cliente.</p> <p>Para los clientes de Oracle Solaris, la clase de cliente Proveedor puede obtenerse mediante el comando <code>prtconf -b</code>. Para especificar la clase de cliente Proveedor, sustituya los puntos por las comas de la cadena que devuelve el comando <code>uname</code>. Por ejemplo, si el comando <code>prtconf -b</code> devuelve la cadena <code>SUNW.Sun-Blade-100</code>, debe especificar la clase de cliente Proveedor como <code>SUNW.Sun-Blade-100</code>.</p>

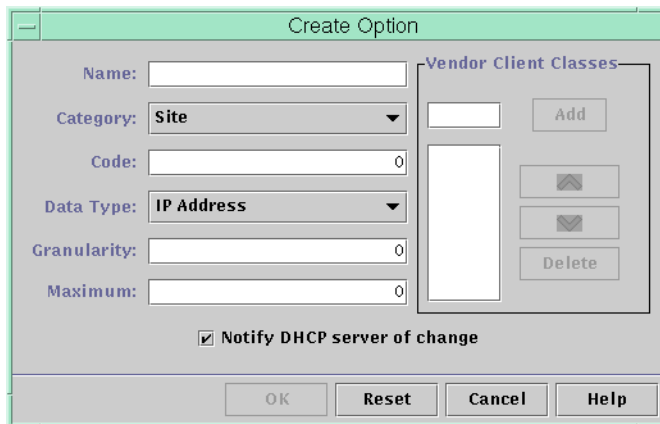
Creación de opciones DHCP

Si necesita transferir información de cliente para la que todavía no hay una opción en el protocolo DHCP, puede crear una opción. Consulte la página de comando `man dhcp_inittab(4)` para obtener una lista de todas las opciones definidas en DHCP antes de crear su propia opción.

Puede utilizar el comando `dhtadm -A -s` o el cuadro de diálogo Crear opción del Administrador de DHCP para crear opciones nuevas.

La figura siguiente muestra el cuadro de diálogo Create Option del Administrador de DHCP.

FIGURA 15-17 Cuadro de diálogo Create Option del Administrador de DHCP



▼ Cómo crear opciones DHCP (Administrador de DHCP)

- 1 En el Administrador de DHCP, seleccione la ficha Options.

Consulte “Cómo iniciar y detener el Administrador de DHCP” en la página 348 para obtener información sobre el Administrador de DHCP.

- 2 Elija Crear en el menú Editar.

Se abrirá el cuadro de diálogo Create Options.

- 3 Incluya una breve descripción para la nueva opción.

El nombre puede contener hasta 128 caracteres alfanuméricos y espacios.

- 4 Escriba o seleccione valores para cada parámetro del cuadro de diálogo.

Consulte la [Tabla 15-5](#) para obtener información sobre cada parámetro, o visualice la ayuda del Administrador de DHCP.

- 5 Seleccione Notify DHCP Server of Change si ha terminado de crear las opciones.

Esta selección indica al servidor DHCP que debe volver a leer la tabla `dhcptab` para aplicar el cambio inmediatamente después de hacer clic en OK.

- 6 Haga clic en Aceptar.

Ahora puede agregar la opción a las macros, y asignar un valor a la opción para transferir a los clientes.

▼ Cómo crear opciones DHCP (dhtadm)

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349.](#)

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

- 2 **Cree una opción DHCP escribiendo un comando con el siguiente formato:**

```
# dhtadm -A -s option-name -d 'category,code,data-type,granularity,maximum' -g
```

nombre_opción Es una cadena alfanumérica de 128 caracteres menos.

categoría Es una de las siguientes: Site, Extend o Vendor=*lista_clases*. *lista_clases* es una lista separada por espacios de clases de cliente de proveedor a la que se aplica la opción. Consulte la [Tabla 15-5](#) para obtener información sobre cómo determinar la clase de cliente de proveedor.

código Es un valor numérico apropiado para la categoría de opción, tal como se explica en la [Tabla 15-5](#).

tipo_datos Se especifica mediante una palabra clave que indica el tipo de datos que se transfiere con la opción, tal como se describe en la [Tabla 15-5](#).

granularidad Se especifica como número no negativo, como se explica en la [Tabla 15-5](#).

máximo Es un número no negativo, como se explica en la [Tabla 15-5](#).

Ejemplo 15-3 Creación de una opción DHCP con dhtadm

El comando siguiente crearía una opción denominada NewOpt, que es una opción de categoría Sitio. El código de la opción es 130. El valor de la opción se puede configurar como un único entero de 8 bits sin firmar.

```
# dhtadm -A -s NewOpt -d 'Site,130,UNUMBER8,1,1' -g
```

El comando siguiente crearía una opción denominada NewServ, que es una opción de categoría Proveedor que se aplica a los clientes cuyo tipo de equipo es SUNW, Sun-Blade-100 o SUNW, Sun-Blade-1000. El código de la opción es 200. El valor de la opción se puede configurar como una dirección IP.

```
# dhtadm -A -s NewServ -d 'Vendor=SUNW.Sun-Blade-100 \ SUNW.Sun-Blade-1000,200,IP,1,1'
```

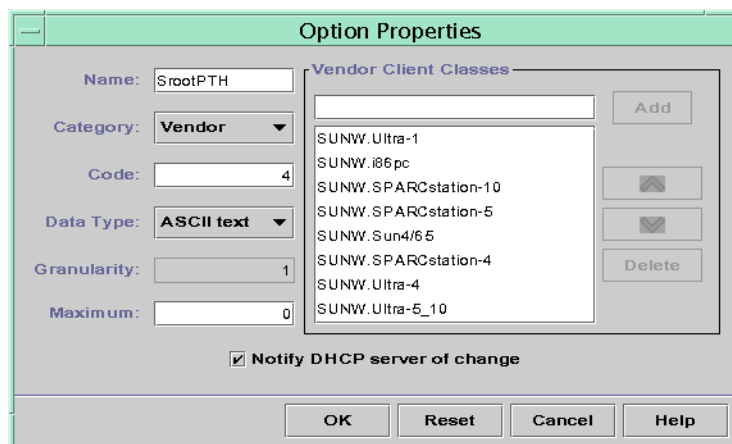
Modificación de opciones DHCP

Si ha creado opciones para el servicio DHCP, puede cambiar las propiedades de dichas opciones. Puede utilizar el comando `dhtadm -M -s` o el cuadro de diálogo Propiedades de opción del Administrador de DHCP para modificar las opciones.

Tenga en cuenta que debe modificar la información de opción del cliente DHCP para reflejar la misma modificación realizada en el servicio DHCP. Consulte [“Modificar la información de opciones de cliente DHCP” en la página 415](#).

La figura siguiente muestra el cuadro de diálogo Propiedades de opción del Administrador de DHCP.

FIGURA 15-18 Cuadro de diálogo Option Properties del Administrador de DHCP



▼ Cómo modificar las propiedades de opciones DHCP (Administrador de DHCP)

- 1 En el Administrador de DHCP, seleccione la ficha Options.

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.

- 2 Seleccione la opción que desea modificar.

- 3 Elija Properties en el menú Edit.

Se abrirá el cuadro de diálogo Option Properties.

4 Edite las propiedades según precise.

Consulte la [Tabla 15-5](#) para obtener información sobre las propiedades, o visualice la ayuda del Administrador de DHCP.

5 Seleccione Notify DHCP Server of Change cuando haya terminado de configurar las opciones.

El cambio se realiza en la tabla `dhcptab`. El servidor DHCP vuelve a leer la tabla `dhcptab` para aplicar los cambios.

6 Haga clic en Aceptar.

▼ **Cómo modificar las propiedades de opciones DHCP (dhtadm)**

1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte “Configuración del acceso de usuario a los comandos de DHCP” en la [página 349](#).

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “Configuración de RBAC (mapa de tareas)” de *Guía de administración del sistema: servicios de seguridad*.

2 Modifique una opción escribiendo un comando con el siguiente formato:

```
# dhtadm -M -s option-name -d 'category,code,data-type,granularity,maximum' -g
```

nombre_opción Especifica el nombre de la opción que se desea modificar.

categoría Puede ser Site, Extend o Vendor=*lista_clases*. *lista_clases* es una lista separada por espacios de clases de cliente de proveedor a la que se aplica la opción. Por ejemplo, SUNW.Sun-Blade-100 SUNW.Ultra-80 SUNWi86pc.

código Especifica un valor numérico apropiado para la categoría de opción, tal como se explica en la [Tabla 15-5](#).

tipo_datos Especifica una palabra clave que indica el tipo de datos que se transfiere con la opción, tal como se describe en la [Tabla 15-5](#).

granularidad Es un número no negativo, como se explica en la [Tabla 15-5](#).

máximo Es un número no negativo, como se explica en la [Tabla 15-5](#).

Debe especificar todas las propiedades de opciones DHCP con el conmutador `-d`, no sólo las propiedades que se desea modificar.

Ejemplo 15-4 Modificación de una opción DHCP con dhtadm

El comando siguiente modificaría una opción denominada NewOpt . La opción es una opción de categoría Sitio. El código de la opción es 135. El valor de la opción se puede configurar como un único entero de 8 bits sin firmar.

```
# dhtadm -M -s NewOpt -d 'Site,135,UNUMBER8,1,1'
```

El comando siguiente modificaría una opción denominada NewServ, que es una opción de categoría Proveedor. La opción ahora se aplica a los clientes cuyo tipo de equipo es SUNW, Sun-Blade-100 o SUNW, i86pc. El código de la opción es 200. El valor de la opción se puede configurar como una dirección IP.

```
# dhtadm -M -s NewServ -d 'Vendor=SUNW.Sun-Blade-100 \ SUNW.i86pc,200,IP,1,1' -g
```

Eliminación de opciones DHCP

No puede eliminar opciones DHCP estándar. Sin embargo, si ha definido opciones para el servicio DHCP, puede eliminarlas utilizando el Administrador de DHCP o el comando dhtadm.

▼ Cómo eliminar opciones DHCP (Administrador de DHCP)

- 1 En el Administrador de DHCP, seleccione la ficha Options.

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.

- 2 Seleccione la opción que desea eliminar.

- 3 Elija Delete en el menú Edit.

Se abrirá el cuadro de diálogo Delete Option.

- 4 Seleccione Notify DHCP Server of Change cuando haya terminado de eliminar las opciones.

Esta selección indica al servidor DHCP que debe volver a leer la tabla dhcptab para aplicar el cambio inmediatamente después de hacer clic en OK.

- 5 Haga clic en Aceptar.

▼ Cómo eliminar opciones DHCP (dhtadm)

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349.](#)

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

- 2 **Elimine una opción DHCP; para esto, escriba un comando con el formato siguiente:**

```
# dhtadm -D -s option-name -g
```

Modificar la información de opciones de cliente DHCP

Si agrega una nueva opción DHCP al servidor DHCP, debe agregar una entrada complementaria a la información de opción de cada cliente DHCP. Si tiene un cliente que no es un cliente DHCP, consulte la documentación de dicho cliente para obtener información sobre cómo agregar opciones o símbolos.

En un cliente DHCP, debe editar el archivo `/etc/dhcp/inittab` y agregar una entrada para cada opción que agregue al servidor DHCP. Si modifica más adelante la opción en el servidor, también debe modificar la entrada en el archivo `/etc/dhcp/inittab` del cliente.

Consulte la página del comando `man dhcp_inittab(4)` para obtener información más detallada sobre la sintaxis del archivo `/etc/dhcp/inittab`.

Nota – Si ha agregado opciones DHCP al archivo `dhcptags` en una versión anterior de Oracle Solaris, debe agregar las opciones al archivo `/etc/dhcp/inittab`. Consulte [“Información de opciones DHCP” en la página 482](#) para obtener más información.

Instalación en red de Oracle Solaris con el servicio DHCP

Puede utilizar DHCP para instalar Oracle Solaris en determinados sistemas cliente de la red. Sólo pueden utilizar esta función los sistemas basados en sun4u y en x86 que se ajustan a los requisitos de hardware para ejecutar el sistema operativo Oracle Solaris. Para obtener información sobre cómo utilizar DHCP para configurar automáticamente los sistemas clientes

para la red durante el arranque, consulte el [Capítulo 2, “Preconfiguración de la información de configuración del sistema \(tareas\)” de Guía de instalación de Oracle Solaris 10 9/10: instalaciones basadas en red.](#)

DHCP también admite sistemas cliente de Oracle Solaris que se inician e instalan remotamente desde servidores en una red de área extensa (WAN) utilizando HTTP. Este método de inicio e instalación remotos se denomina método de *instalación de inicio WAN*. El inicio WAN permite instalar el sistema operativo Oracle Solaris en sistemas basados en SPARC en una red pública extensa donde puede que la infraestructura de red sea poco fiable. Se puede utilizar el inicio WAN con funciones de seguridad para proteger la confidencialidad de los datos y la integridad de la imagen de instalación.

Antes de poder usar DHCP para iniciar e instalar sistemas cliente de forma remota mediante el inicio WAN, el servidor DHCP debe estar configurado para suministrar la siguiente información a los clientes:

- La dirección IP del servidor proxy
- La ubicación del programa wanboot - cgi

Para obtener detalles sobre cómo configurar el servidor DHCP para proporcionar esta información, consulte el [Capítulo 2, “Preconfiguración de la información de configuración del sistema \(tareas\)” de Guía de instalación de Oracle Solaris 10 9/10: instalaciones basadas en red.](#) Para obtener información sobre cómo iniciar e instalar sistemas cliente con un servidor DHCP a través de una WAN, consulte el [Capítulo 10, “Inicio WAN \(información general\)” de Guía de instalación de Oracle Solaris 10 9/10: instalaciones basadas en red.](#)

Para obtener información sobre los clientes sin disco, consulte [“Inicio remoto y clientes de inicio sin disco \(mapa de tareas\)” en la página 416.](#)

Inicio remoto y clientes de inicio sin disco (mapa de tareas)

El servicio DHCP puede admitir sistemas cliente Oracle Solaris que montan sus archivos de sistema operativo de forma remota desde otra máquina (el servidor de SO). Dichos clientes se denominan normalmente *clientes sin discos*. Los clientes sin discos se pueden considerar clientes de inicio remoto persistentes. Cada vez que se inicia un cliente sin disco, el cliente debe obtener el nombre y la dirección IP del servidor en el que se alojan los archivos del sistema operativo del cliente. A continuación, el cliente sin disco se puede iniciar remotamente desde esos archivos.

Cada cliente sin disco tiene su propia partición raíz en el servidor del sistema operativo, que se comparte con el nombre de host del cliente. El servidor DHCP siempre debe devolver la misma dirección IP a un cliente sin disco. Dicha dirección debe permanecer asignada al mismo

nombre de host del servicio de nombres, como DNS. Si un cliente sin disco recibe una dirección IP coherente, el cliente utiliza un nombre de host coherente, y puede acceder a su partición raíz en el servidor del sistema operativo.

Además de proporcionar la dirección IP y el nombre de host, el servidor DHCP puede proporcionar la ubicación de los archivos del sistema operativo del cliente sin disco. Sin embargo, debe crear opciones y macros para transferir la información en un paquete de mensajes DHCP.

El siguiente mapa de tareas enumera las tareas necesarias para admitir clientes sin disco o cualquier cliente de inicio remoto persistente. El mapa de tareas también contiene vínculos a procedimientos que permiten llevar a cabo las tareas.

Tarea	Descripción	Para obtener instrucciones
Configurar servicios de SO en un servidor Oracle Solaris.	Utilice el comando <code>smosservice</code> para crear archivos de sistema operativo para los clientes.	Capítulo 7, “Administración de clientes sin disco (Tareas)” de <i>Guía de administración del sistema: administración básica</i> Asimismo, consulte la página del comando <code>man smosservice(1M)</code> .
Configurar el servicio DHCP para admitir clientes de inicio de red.	Utilice el Administrador de DHCP o el comando <code>dhtadm</code> para crear macros y opciones del proveedor, que el servidor DHCP puede utilizar para transferir información de inicio a los clientes. Si ya ha creado las opciones para los clientes de instalación de red, sólo debe crear las macros de los tipos de cliente de proveedor de los clientes sin disco.	Capítulo 2, “Preconfiguración de la información de configuración del sistema (tareas)” de <i>Guía de instalación de Oracle Solaris 10 9/10: instalaciones basadas en red</i>
Asignar direcciones IP reservadas a los clientes sin disco.	Utilice el Administrador de DHCP para marcar la dirección como reservada, o utilice el comando <code>pntadm</code> para marcar direcciones como <code>MANUAL</code> para los clientes sin disco.	“Asignación de una dirección IP reservada a un cliente DHCP” en la página 393
Configurar clientes sin disco para el servicio de sistema operativo.	Utilice el comando <code>smdiskless</code> para incluir compatibilidad con el sistema operativo en el servidor de sistema operativo para cada cliente. Especifique las direcciones IP que ha reservado para cada cliente.	Capítulo 7, “Administración de clientes sin disco (Tareas)” de <i>Guía de administración del sistema: administración básica</i> Asimismo, consulte la página del comando <code>man smdiskless(1M)</code> .

Configuración de clientes DHCP sólo para recibir información (mapa de tareas)

En algunas redes, el servicio DHCP sólo puede proporcionar información de configuración a los clientes. Los sistemas cliente que necesitan información, no permisos, pueden utilizar el cliente DHCP para emitir un mensaje INFORM. El mensaje INFORM solicita al servidor DHCP que envíe la información de configuración adecuada al cliente.

Puede configurar el servidor DHCP para admitir clientes que sólo necesiten información. Debe crear una tabla de red vacía que se corresponda a la red que aloja a los clientes. La tabla debe existir para que el servidor DHCP pueda responder a los clientes de dicha red.

El siguiente mapa de tareas enumera las tareas necesarias para admitir clientes sólo de información. El mapa de tareas también incluye vínculos a procedimientos que permiten llevar a cabo las tareas.

Tarea	Descripción	Para obtener instrucciones
Crear una tabla de red vacía.	Utilice el Administrador de DHCP o el comando <code>pntadm</code> para crear una tabla de red para la red de clientes sólo de información.	“Cómo agregar redes DHCP” en la página 369
Crear macros para incluir la información que necesitan los clientes.	Utilice el Administrador de DHCP o el comando <code>dhtadm</code> para crear macros que transfieran la información necesaria a los clientes.	“Creación de macros DHCP” en la página 403
Configurar el cliente DHCP para que emita un mensaje INFORM.	Utilice el comando <code>ifconfig int dhcp inform</code> para que el cliente DHCP emita un mensaje INFORM.	“Inicio de cliente DHCP” en la página 434 “Opciones del comando <code>ifconfig</code> que se utilizan con el cliente DHCP” en la página 439 Página del comando <code>man ifconfig(1M)</code>

Conversión a un nuevo almacén de datos DHCP

DHCP proporciona una utilidad para convertir los datos de configuración de DHCP de un almacén de datos a otro. Existen distintos motivos para convertir a un nuevo almacén de datos. Por ejemplo, puede tener más clientes DHCP, que requieran un mayor rendimiento o más capacidad del servicio DHCP. También puede repartir las tareas del servidor DHCP entre distintos servidores. Consulte [“Selección del almacén de datos DHCP” en la página 323](#) para ver una comparación de las ventajas y desventajas de cada tipo de almacén de datos.

Nota – Si ha actualizado de una versión de Oracle Solaris anterior a Solaris 8 7/01, debe leer esta nota.

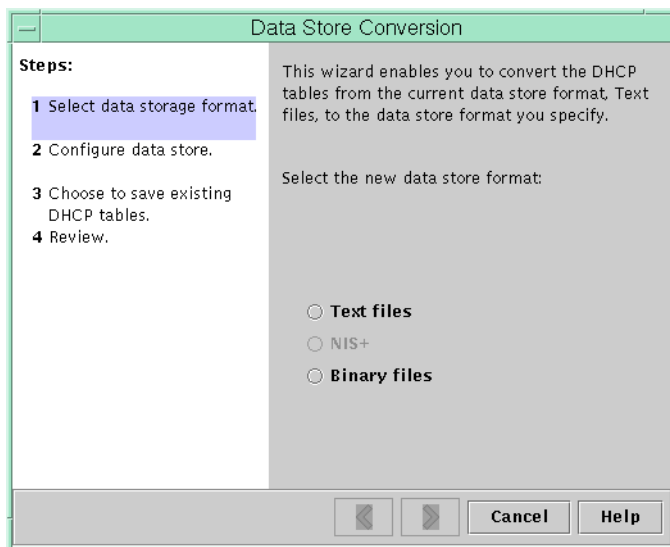
Cuando ejecuta cualquier herramienta de DHCP después de la instalación de Oracle Solaris, se le solicita que realice la conversión a un nuevo almacén de datos. La conversión es necesaria porque el formato de los datos almacenados en ambos archivos y NIS+ ha cambiado en Solaris 8 7/01. Si no convierte al nuevo almacén de datos, el servidor DHCP seguirá leyendo las tablas de datos antiguas. Sin embargo, el servidor sólo puede otorgar permisos para los clientes existentes. No puede registrar nuevos clientes DHCP ni utilizar herramientas de administración de DHCP con las tablas de datos antiguas.

La utilidad de conversión también resulta útil para los sitios que convierten de un almacén de datos proporcionado por Sun a un almacén de datos de otro proveedor. La utilidad de conversión busca entradas en el almacén de datos existente y agrega nuevas entradas que contienen los mismos datos al nuevo almacén de datos. El acceso al almacén de datos se implementa en módulos separados para cada almacén de datos. Este enfoque modular permite a la utilidad de conversión convertir datos DHCP de cualquier formato de almacén de datos a otro diferente. Cada almacén de datos debe tener un módulo que pueda utilizar el servicio DHCP. Consulte [Solaris DHCP Service Developer's Guide](#) para obtener más información sobre cómo escribir un módulo para que admita un almacén de datos de terceros.

La conversión del almacén de datos se puede llevar a cabo con el Administrador de DHCP mediante el asistente Data Store Conversion o con el comando `dhcpconfig -C`.

La figura siguiente muestra el cuadro de diálogo inicial del asistente Data Store Conversion.

FIGURA 15–19 Cuadro de diálogo Data Store Conversion del Administrador de DHCP



Antes de que comience la conversión, debe especificar si desea guardar las tablas de los antiguos almacenes de datos (dhcptab y tablas de red). La utilidad de conversión detiene el servidor DHCP, convierte el almacén de datos y reinicia el servidor cuando la conversión se ha completado correctamente. Si no ha especificado que se guarden las tablas antiguas, la utilidad elimina las tablas después de determinar que la conversión se ha realizado correctamente. El proceso de conversión puede requerir mucho tiempo. La conversión se ejecuta en segundo plano e incluye una indicación del progreso.

▼ **Cómo convertir el almacén de datos DHCP (Administrador de DHCP)**

- 1 En el Administrador de DHCP, elija Convert Data Store en el menú Service.**

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la [página 348](#) para obtener información sobre el Administrador de DHCP.

Se abrirá el asistente Data Store Conversion.

- 2 Responda a las preguntas del asistente.**

Si no conoce la información que se le solicita, haga clic en Help para ver información detallada sobre cada cuadro de diálogo.

3 Revise sus selecciones y haga clic en **Finish** para convertir el almacén de datos.

El servidor DHCP se reinicia cuando finaliza la conversión. El servidor utiliza de inmediato el nuevo almacén de datos.

▼ **Cómo convertir el almacén de datos DHCP** **(dhcpconfig -C)**

1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349.](#)

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

2 Convierta el almacén de datos escribiendo un comando con el formato siguiente:

```
# /usr/sbin/dhcpconfig -C -r resource -p path
```

recurso Es el nuevo tipo de almacén de datos, como SUNWbinfiles

ruta Es la ruta a los datos, como /var/dhcp

Si desea conservar los datos originales del antiguo almacén de datos tras la conversión, especifique la opción -k. Por ejemplo, para convertir el almacén de datos a SUNWbinfiles y guardar el anterior, escriba:

```
# /usr/sbin/dhcpconfig -C -r SUNWbinfiles -p /var/dhcp -k
```

Consulte la página del comando man [dhcpconfig\(1M\)](#) para obtener más información sobre la utilidad dhcpconfig.

Transferencia de datos de configuración entre servidores DHCP (mapa de tareas)

El Administrador de DHCP y la utilidad dhcpconfig permiten transferir todos o parte de los datos de configuración de DHCP de un servidor DHCP a otro servidor. Puede transferir redes completas y todas las direcciones IP, macros y opciones asociadas con las redes. También puede seleccionar direcciones IP específicas, macros y opciones que transferir. También puede copiar macros y opciones sin eliminarlas del primer servidor.

Es posible transferir datos si va a realizar alguna de las tareas siguientes:

- Agregar un servidor para compartir las tareas de DHCP.
- Reemplazar el sistema del servidor DHCP.
- Cambiar la ruta del almacén de datos, mientras se sigue utilizando el mismo almacén de datos.

El siguiente mapa de tareas identifica los procedimientos que debe seguir al transferir datos de configuración de DHCP. El mapa incluye vínculos a procedimientos para realizar las tareas.

Tarea	Descripción	Para obtener instrucciones
1. Exportar los datos del primer servidor.	Selecciona los datos que desea transferir a otro servidor y crea un archivo con los datos exportados.	“Cómo exportar datos de un servidor DHCP (Administrador de DHCP)” en la página 424 “Cómo exportar datos de un servidor DHCP (dhcpconfig -X)” en la página 424
2. Importar los datos al segundo servidor.	Copia los datos exportados a otro almacén de datos del servidor DHCP.	“Cómo importar datos en un servidor DHCP (Administrador de DHCP)” en la página 426 “Cómo importar datos en un servidor DHCP (dhcpconfig -I)” en la página 426
3. Modificar los datos importados para el nuevo entorno de servidor.	Cambia los datos de configuración específicos del servidor para que coincidan con la información del nuevo servidor.	“Cómo modificar datos de DHCP importados (Administrador de DHCP)” en la página 427 “Cómo modificar datos DHCP importados (pntadm, dhtadm)” en la página 428

En el Administrador de DHCP, utilice el asistente Export Data y el asistente Import Data para transferir los datos de un servidor a otro. A continuación, modifique las macros en la ficha Macros. Las siguientes figuras muestran los cuadros de diálogo iniciales de los asistentes.

FIGURA 15-20 Cuadro de diálogo del asistente Export Data del Administrador de DHCP

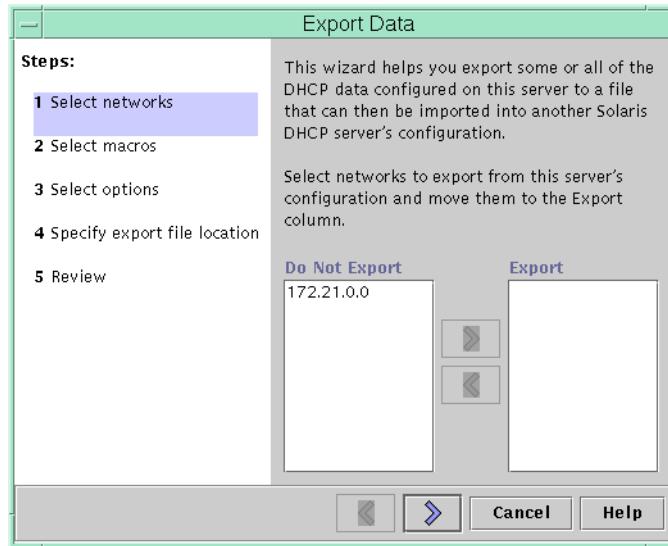
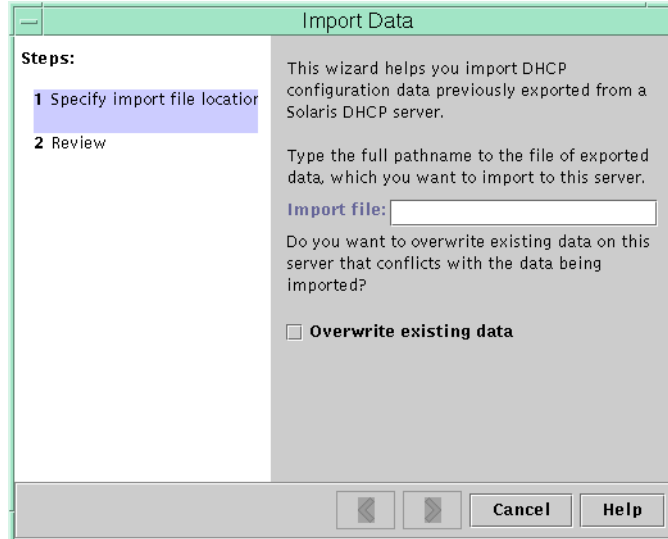


FIGURA 15-21 Cuadro de diálogo del asistente Import Data del Administrador de DHCP



▼ **Cómo exportar datos de un servidor DHCP (Administrador de DHCP)**

- 1 **Inicie el Administrador de datos de DHCP en el servidor desde el que desea transferir o copiar los datos.**

Consulte “[Cómo iniciar y detener el Administrador de DHCP](#)” en la página 348 para obtener información sobre el Administrador de DHCP.

- 2 **Elija Export Data en el menú Service.**

Se abrirá el asistente Export Data tal como se muestra en la [Figura 15–20](#).

- 3 **Responda a las preguntas del asistente.**

Si no conoce la respuesta, haga clic en Help para obtener información detallada sobre las preguntas.

- 4 **Transfiera el archivo de exportación a un sistema de archivos al que pueda acceder el servidor DHCP que debe importar los datos.**

Véase también Importe los datos tal como se describe en “[Cómo importar datos en un servidor DHCP \(Administrador de DHCP\)](#)” en la página 426.

▼ **Cómo exportar datos de un servidor DHCP (dhcpconfig -X)**

- 1 **Inicie sesión en el servidor desde el que desea transferir o copiar los datos.**

- 2 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte “[Configuración del acceso de usuario a los comandos de DHCP](#)” en la página 349.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

3 Exporte los datos.

Puede exportar todos los datos de DHCP o partes específicas de los datos.

- **Para exportar direcciones, macros y opciones específicas, escriba un comando que utilice el formato siguiente:**

```
# dhcpconfig -X filename -a network-addresses -m macros -o options
```

nombre_archivo es el nombre de ruta completo que desea utilizar para almacenar los datos exportados comprimidos. Las direcciones de red, macros DHCP y opciones DHCP concretas se especifican en listas separadas con comas. El ejemplo siguiente muestra cómo exportar redes, macros y opciones específicas.

```
# dhcpconfig -X /var/dhcp/0dhcp1065_data \ -a 10.63.0.0,10.62.0.0 \ -m 10.63.0.0,10
```

- **Para exportar todos los datos de DHCP, escriba un comando que utilice la palabra clave ALL.**

```
# dhcpconfig -X filename -a ALL -m ALL -o ALL
```

nombre_archivo es el nombre de ruta completo que desea utilizar para almacenar los datos exportados comprimidos. La palabra clave ALL puede utilizarse con las opciones de comandos para exportar todas las opciones, macros y direcciones de red. El ejemplo siguiente muestra cómo utilizar la palabra clave ALL.

```
# dhcpconfig -X /var/dhcp/dhcp1065_data -a ALL -m ALL -o ALL
```

Consejo – Puede omitir la exportación de un tipo de datos concreto si no especifica la opción de comando `dhcpconfig` para ese tipo de datos. Por ejemplo, si no especifica la opción `-m`, no se exportará ninguna macro DHCP.

Consulte la página del comando `man dhcpconfig(1M)` para obtener más información sobre el comando `dhcpconfig`.

- ### 4 Transfiera el archivo de exportación a una ubicación a la que pueda acceder el servidor que debe importar los datos.

Véase también Importe los datos de acuerdo con lo descrito en “Cómo importar datos en un servidor DHCP (`dhcpconfig -I`)” en la página 426.

▼ **Cómo importar datos en un servidor DHCP (Administrador de DHCP)**

- 1 Inicie el Administrador de DHCP en el servidor al que desee transferir los datos que exportó previamente de un servidor DHCP.**
Consulte [“Cómo iniciar y detener el Administrador de DHCP”](#) en la página 348 para obtener información sobre el Administrador de DHCP.
- 2 Elija Import Data en el menú Service.**
Se abrirá el asistente Import Data tal como se muestra en la [Figura 15–21](#).
- 3 Responda a las preguntas del asistente.**
Si no conoce la respuesta, haga clic en Help para obtener información detallada sobre las preguntas.
- 4 Modifique los datos importados, si es preciso.**
Consulte [“Cómo modificar datos de DHCP importados \(Administrador de DHCP\)”](#) en la página 427

▼ **Cómo importar datos en un servidor DHCP (dhcpconfig -I)**

- 1 Inicie sesión en el servidor al que desea importar los datos.**
- 2 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**
Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP”](#) en la página 349.
Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.
- 3 Importe los datos escribiendo un comando con el formato siguiente:**

```
# dhcpconfig -I filename
```

nombre_archivo es el nombre del archivo que contiene los datos exportados.
- 4 Modifique los datos importados, si es preciso.**
Consulte [“Cómo modificar datos DHCP importados \(pntadm, dhtadm\)”](#) en la página 428.

▼ **Cómo modificar datos de DHCP importados (Administrador de DHCP)**

1 Inicie el Administrador de DHCP en el servidor al que importó los datos.

Consulte [“Cómo iniciar y detener el Administrador de DHCP” en la página 348](#) para obtener información sobre el Administrador de DHCP.

2 Busque en los datos importados información específica de la red que se deba modificar.

Por ejemplo, si ha movido redes, debe abrir la ficha Addresses y cambiar el servidor propietario de las direcciones en las redes importadas. También puede abrir la ficha Macros para especificar los nombres de dominio correctos para NIS, NIS+ o DNS en algunas macros.

3 Abra la ficha Addresses y seleccione una red que haya importado.

4 Para seleccionar todas las direcciones, haga clic en la primera dirección, mantenga pulsada la tecla Mayús y elija la última dirección.

5 En el menú Edit, elija Properties.

Se abrirá el cuadro de diálogo Modify Multiple Addresses.

6 En el indicador Managing Server, seleccione el nombre del nuevo servidor.

7 En el indicador Configuration Macro, seleccione la macro que se vaya a utilizar para todos los clientes de esta red y haga clic en OK.

8 Abra la ficha Macros.

9 Utilice el botón Find para buscar las opciones que probablemente se deban modificar.

El botón Find se encuentra en la parte inferior de la ventana.

DNSdmain, DNSserv, NISservs, NIS+serv y NISdmain son ejemplos de opciones que pueden requerir modificaciones en el nuevo servidor.

10 Cambie las opciones de las macros deseadas.

Consulte [“Cómo modificar las propiedades de opciones DHCP \(Administrador de DHCP\)” en la página 412](#) para conocer el procedimiento que debe seguir para cambiar opciones.

▼ **Cómo modificar datos DHCP importados (pntadm, dhtadm)**

- 1 Inicie sesión en el servidor al que ha importado los datos.**
- 2 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de administración de DHCP.**

Para obtener más información acerca del perfil de administración de DHCP, consulte [“Configuración del acceso de usuario a los comandos de DHCP” en la página 349.](#)

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

- 3 Busque en las tablas de red los datos que se deben modificar.**

Si ha transferido redes, utilice el comando `pntadm -P dirección_red` para imprimir las tablas de red para las redes que se han transferido.

- 4 Modifique la información de la dirección IP con el comando pntadm.**

El servidor propietario y la macro de configuración se pueden cambiar para las direcciones importadas. Por ejemplo, para cambiar el servidor propietario (10.60.3.4) y la macro (dhcpsrv-1060) for address 10.63.0.2, utilice el comando siguiente:

```
pntadm -M 10.63.0.2 -s 10.60.3.4 -m dhcpsrv-1060 10.60.0.0
```

Si tiene una gran cantidad de direcciones, debe crear un archivo de secuencia que contenga los comandos para modificar cada dirección. Ejecute la secuencia con el comando `pntadm -B`, que ejecuta `pntadm` en modo de ejecución por lotes. Consulte la página del comando [man pntadm\(1M\)](#).

- 5 Busque en las macros dhcptab opciones con valores que necesiten modificarse.**

Utilice el comando `dhtadm -P` para imprimir la tabla `dhcptab` completa en pantalla. Utilice `grep` u otra herramienta para buscar opciones o valores que desee cambiar.

- 6 Si es preciso, modifique las opciones de las macros utilizando el comando dhtadm -M.**

Por ejemplo, puede modificar algunas macros para especificar los servidores y nombres de dominio correctos para NIS, NIS+ o DNS. Por ejemplo, el siguiente comando cambia los valores de `DNSdmain` y `DNSserv` en la macro `mymacro`:

```
dhtadm -M -m mymacro -e 'DNSserv=dnsrv2:DNSdmain=example.net' -g
```

Configuración y administración del cliente DHCP

Este capítulo trata sobre el cliente Dynamic Host Configuration Protocol (DHCP) que es parte de Oracle Solaris. En el capítulo se explica el funcionamiento de los protocolos DHCPv4 y DHCPv6 del cliente y la forma de modificar el comportamiento de este.

Uno de los protocolos, DHCPv4, forma parte del sistema operativo Oracle Solaris desde hace tiempo, y permite a los servidores DHCP pasar parámetros de configuración como direcciones de red IPv4 a nodos IPv4.

El otro, DHCPv6, permite a los servidores DHCP pasar parámetros de configuración, como direcciones de red IPv6, a nodos IPv6. DHCPv6 es una contrapartida con estado a “IPv6 Stateless Address Autoconfiguration” (RFC 2462), y se puede utilizar de forma independiente o conjuntamente con la sin estado para obtener parámetros de configuración.

Este capítulo contiene la información siguiente:

- [“Acerca del cliente DHCP” en la página 429](#)
- [“Activación y desactivación de un cliente DHCP” en la página 437](#)
- [“Administración del cliente DHCP” en la página 439](#)
- [“Sistemas cliente DHCP con varias interfaces de red” en la página 441](#)
- [“Nombres de host de cliente DHCPv4” en la página 442](#)
- [“Sistemas cliente DHCP y servicios de nombres” en la página 443](#)
- [“Secuencias de eventos de cliente DHCP” en la página 448](#)

Acerca del cliente DHCP

El cliente DHCP es el daemon `dhcpgent`, parte de Oracle Solaris. Al instalar Oracle Solaris se le solicitará que utilice DHCP para configurar las interfaces de red. Si especifica Sí para DHCPv4, el protocolo se activa en su sistema durante la instalación de Oracle Solaris. No hay opciones de instalación específicas para DHCPv6. Pero hay una cuestión relacionada acerca de IPv6. Si activa IPv6, DHCPv6 se activará también en una red local compatible con DHCPv6.

No es necesario hacer nada más con el cliente de Oracle Solaris para utilizar DHCP. La configuración del servidor DHCP determina la información que se proporciona a los sistemas cliente DHCP que utilizan el servicio DHCP.

Si un sistema cliente ya está ejecutando Oracle Solaris pero no utiliza DHCP, se puede reconfigurar para que lo utilice. También se puede reconfigurar un sistema cliente DHCP de modo que deje de utilizar DHCP y utilice la información de red estática que proporcione. Consulte [“Activación y desactivación de un cliente DHCP” en la página 437](#) para obtener más información.

Servidor DHCPv6

No hay ningún servidor DHCPv6 disponible a través de Sun Microsystems para Oracle Solaris. Los servidores de terceros son compatibles con el DHCPv6 de Sun y, si hay un servidor DHCPv6 en la red, el cliente DHCPv6 de Sun lo utilizará.

Consulte [“El servidor DHCP” en la página 306](#) para obtener más información sobre el servidor DHCPv4 de Sun.

Diferencias entre DHCPv4 y DHCPv6

Las dos principales diferencias entre DHCPv4 y DHCPv6 son las siguientes:

- **El modelo de administración**
 - DHCPv4: el administrador activa DHCP para cada interfaz. La administración se efectúa por interfaz lógica.
 - DHCPv6—No es necesaria una configuración explícita. Este protocolo se activa en una interfaz física determinada.
- **Detalles del protocolo**
 - DHCPv4—El servidor DHCP proporciona la máscara de subred de cada dirección. La opción de nombre de host establece el nombre de nodo en todo el sistema.
 - DHCPv6: la máscara de subred la proporcionan los anuncios de enrutador, no el servidor DHCPv6. No existe la opción de nombre de host DHCPv6.

El modelo administrativo

DHCPv4 requiere una configuración de cliente explícita. Debe configurar el sistema DHCPv4 para la asignación de direcciones cuando lo desee; esto se suele llevar a cabo durante la instalación inicial del sistema o de forma dinámica mediante las opciones de `ifconfig(1M)`.

DHCPv6 no requiere una configuración de cliente explícita. Por el contrario, el uso de DHCP es una propiedad de la red, y la señal para utilizarlo se encuentra en los mensajes de anuncio de los enrutadores locales. El cliente DHCP crea y destruye automáticamente las interfaces lógicas según sea necesario.

El mecanismo de DHCPv6 es muy parecido, desde el punto de vista administrativo, a la configuración de direcciones sin estado IPv6 (automática) actual. Para la configuración de direcciones sin estado se activaría un indicador en el enrutador local con el fin de indicar que, para un conjunto de prefijos determinado, cada cliente deberá configurar automáticamente una dirección propia utilizando el prefijo anunciado, así como un símbolo o número aleatorio de interfaz local. Para DHCPv6 se requieren los mismos prefijos, pero las direcciones se obtienen y gestionan mediante un servidor DHCPv6 en lugar de asignarse de forma "aleatoria."

Dirección MAC e ID de cliente

DHCPv4 utiliza la dirección MAC y un ID de cliente opcional para identificar al cliente y así asignarle una dirección. Cada vez que el mismo cliente llega a la red, obtiene la misma dirección, si es posible.

DHCPv6 utiliza básicamente el mismo esquema, pero hace que el ID de cliente sea obligatorio y le impone una estructura. El ID de cliente de DHCPv6 consta de dos partes: un Identificador único de DHCP (DUID) y un Identificador de identidad de asociación (IAID). El DUID identifica el **sistema** cliente (no solo una interfaz, como en DHCPv4), y el IAID identifica la interfaz en ese sistema.

Tal como se describe en RFC 3315, una asociación de identidad es el método que utilizan el servidor y el cliente para identificar, agrupar y gestionar un conjunto de direcciones IPv6 relacionadas. Un cliente debe asociar al menos una asociación de identidad (IA) con cada una de sus interfaces de red, y a continuación utiliza las IA asignadas para obtener información de configuración de un servidor de esa interfaz. Para obtener información adicional sobre IA, consulte la siguiente sección, "Detalles de protocolo."

DUID+IAID pueden también emplearse con DHCPv4. Se pueden concatenar de forma no ambigua para actuar como ID de cliente. Por motivos de compatibilidad, en las interfaces IPv4 habituales no suele hacerse. Sin embargo, para interfaces lógicas (hme0:1), DUID+IAID se utiliza si no se ha configurado ningún ID de cliente.

A diferencia de DHCPv4, DHCPv6 no ofrece una opción de "nombre de cliente", así que no hay modo de asignar nombres a sus sistemas basándose únicamente en DHCPv6. Si necesita saber el nombre DNS que corresponde a una dirección proporcionada por DHCPv6, utilice la técnica de determinación inversa de DNS (consulta de dirección-nombre a través de la función `getaddrinfo(3SOCKET)`) para averiguar la información de nombre correspondiente. Esto implica que, si solo utiliza DHCPv6 y desea que un nodo tenga un nombre específico, deberá configurar `/etc/nodename` en su sistema.

Detalles del protocolo

Con DHCPv4, el servidor DHCP proporciona la máscara de subred que se debe utilizar con la dirección asignada. Con DHCPv6, la máscara de subred (que se denomina también “longitud de prefijo”) la asignan los anuncios de enrutador, y no la controla el servidor DHCP.

DHCPv4 incorpora la opción de Nombre de host, que se utiliza para asignar el nombre del nodo en todo el sistema. DHCPv6 no dispone de esa opción.

Para configurar un ID de cliente para DHCPv6 se debe especificar un DUID, en lugar de dejar que el sistema lo elija automáticamente. Esta operación se puede hacer globalmente para el daemon, por cada interfaz. Utilice el formato siguiente para configurar la DUID global (tenga en cuenta el punto inicial):

.v6.CLIENT_ID=DUID

Para configurar una interfaz determinada para que use un DUID específico (y que un servidor DHCPv6 perciba el sistema como varios clientes independientes):

hme0.v6.CLIENT ID=DUID

Cada asociación de identidad (IA) acepta un tipo de dirección. Por ejemplo, una asociación de identidad para direcciones temporales (IA_TA) acepta direcciones temporales, mientras que una para direcciones no temporales (IA_NA) lleva asignadas direcciones permanentes. La versión de DHCPv6 que se describe en esta guía solo proporciona asociaciones IA_NA.

Oracle Solaris asigna exactamente un IAID a cada interfaz cuando se le solicita, y el IAID se guarda en un archivo en el sistema de archivos raíz para que sea constante durante toda la vida del sistema.

Interfaces lógicas

En el cliente DHCPv4, cada interfaz lógica es independiente y es una unidad administrativa. Aparte de la interfaz lógica cero (cuyo identificador predeterminado es la dirección MAC de la interfaz), el usuario puede configurar interfaces específicas para ejecutar DHCP; para ello debe especificar un CLIENT_ID en el archivo de configuración `dhcagent`. Por ejemplo:

hme0:1.CLIENT_ID=orangutan

DHCPv6 funciona de otra forma. La interfaz lógica cero en una interfaz IPv6 es siempre, a diferencia de IPv4, una dirección local. La dirección local se utiliza para asignar automáticamente una dirección IP a un dispositivo de una red IP cuando no se dispone de otro método de asignación, como un servidor DHCP. La interfaz lógica cero no puede estar bajo control de DHCP, de modo que, aunque DHCPv6 se ejecute en esa interfaz (que se denomina también interfaz “física”), solo asigna direcciones a interfaces lógicas que no sean la cero.

En respuesta a una solicitud de cliente DHCPv6, el servidor DHCPv6 devuelve una lista de direcciones para que el cliente las configure.

Negociación de opciones

DHCPv6 dispone de la opción Solicitud de opciones, que ofrece al servidor una pista de lo que el cliente prefiere ver. Si se han enviado todas las posibles opciones desde el servidor al cliente, se podría enviar tanta información que parte de ella debería perderse en el camino al cliente. El servidor podría utilizar esa pista para elegir qué opciones debe incluir en la respuesta. Otra posibilidad es que el servidor haga caso omiso de la pista y elija los elementos que se incluyen. En Oracle Solaris, por ejemplo, las opciones preferibles podrían incluir el dominio de direcciones DNS de Oracle Solaris o el dominio de direcciones NIS, pero posiblemente no se incluiría el servidor de netbios.

DHCPv4 proporciona el mismo tipo de sugerencia, pero sin la opción especial de Solicitud de opciones. En cambio, DHCPv4 utiliza `PARAM_REQUEST_LIST` en `/etc/default/dhclient`.

Sintaxis de configuración

Configure el cliente DHCPv6 de forma similar al actual cliente DHCPv4, mediante `/etc/default/dhclient`.

La sintaxis se aumenta con un marcador “.v6” entre el nombre de la interfaz (si lo hay) y el parámetro que se debe configurar. Por ejemplo, la lista de solicitud de opciones IPv4 global se configura así:

```
PARAM_REQUEST_LIST=1,3,6,12,15,28,43
```

Se puede configurar una interfaz individual para omitir la opción de nombre de host, de este modo:

```
hme0.PARAM_REQUEST_LIST=1,3,6,15,28,43
```

Para configurar una lista de solicitud global para DHCPv6, tenga en cuenta el punto precedente:

```
.v6.PARAM_REQUEST_LIST=23,24
```

O, para configurar una interfaz individual, siga este ejemplo:

```
hme0.v6.PARAM_REQUEST_LIST=21,22,23,24
```

Utilice como referencia para configuración de DHCPv6 este archivo `/etc/default/dhclient`:

```
# The default DHCPv6 parameter request list has preference (7), unicast (12),
# DNS addresses (23), DNS search list (24), NIS addresses (27), and
# NIS domain (29). This may be changed by altering the following parameter-
# value pair. The numbers correspond to the values defined in RFC 3315 and
# the IANA dhcpv6-parameters registry.
.v6.PARAM_REQUEST_LIST=7,12,23,24,27,29
```

Inicio de cliente DHCP

En la mayor parte de casos, no es necesario hacer nada para que se inicie el cliente DHCPv6. El daemon `in.ndpd` inicia DHCPv6 automáticamente cuando se necesita. Es posible que necesite `/etc/hostname6.$IFNAME` para configurar una interfaz que se debe sondear para IPv6 durante el arranque. Sin embargo, el instalador ya efectúa esta operación si se habilita IPv6 en el sistema durante la instalación.

Sin embargo, para DHCPv4 se debe solicitar el inicio del cliente, si no se hizo durante la instalación de Oracle Solaris. Consulte [“Cómo habilitar el cliente DHCP” en la página 437](#).

El daemon `dhcpgent` obtiene la información de configuración necesaria por otros procesos implicados en el inicio del sistema. Por ello, las secuencias de inicio del sistema se inician `dhcpgent` en las primeras fases del proceso de inicio y esperan hasta que llega la información de configuración de red del servidor DHCP.

Aunque el comportamiento predeterminado es ejecutar DHCPv6, puede optar por no ejecutarlo. Una vez que DHCPv6 se está ejecutando, se puede detener con el comando `ifconfig`. También se puede deshabilitar DHCPv6 para que no se inicie al reiniciar el sistema; para ello se debe modificar el archivo `/etc/inet/ndpd.conf`.

El siguiente ejemplo muestra cómo cerrar inmediatamente DHCPv6 en la interfaz denominada `hme0`.

```
ex# echo ifdefault StatefulAddrConf false >> /etc/inet/ndpd.conf
ex# pkill -HUP -x in.ndpd
ex# ifconfig hme0 inet6 dhcp release
```

La presencia del archivo `/etc/dhcp.interfaz` (por ejemplo, `/etc/dhcp.ce0` en un sistema Sun Fire 880) indica a las secuencias de inicio que DHCPv4 se debe utilizar en la interfaz especificada. Cuando encuentran un archivo `dhcp.interfaz`, las secuencias de inicio ejecutan `dhcpgent`.

Al ejecutarse, `dhcpgent` espera hasta recibir instrucciones para configurar una interfaz de red. Las secuencias de inicio emiten el comando `ifconfig interfaz dhcp start`, que indica a `dhcpgent` que inicie DHCPv4 como se describe en [“Funcionamiento de DHCP” en la página 303](#). Si hay comandos en el archivo `dhcp.interfaz`, se agregan a la opción `dhcp start` de `ifconfig`. Consulte la página de comando `man ifconfig(1M)` para obtener información sobre las opciones del comando `ifconfig interfaz dhcp`.

Comunicación con DHCPv6

A diferencia de DHCPv4, que se invoca mediante configuración manual, DHCPv6 se invoca mediante anuncios de enrutador (RA). En función de la configuración del enrutador, el sistema llama automáticamente a DHCPv6 en la interfaz en la que se ha recibido el mensaje de anuncio de enrutador y utiliza DHCP para obtener una dirección y otros parámetros, o el sistema solicita sólo datos que no sean la dirección (por ejemplo, servidores DNS) con DHCPv6.

El daemon `in.ndpd` recibe el mensaje de anuncio del enrutador. Lo hace automáticamente en todas las interfaces sondeadas para IPv6 en el sistema. Cuando `in.ndpd` ve un RA que especifica que se debe ejecutar DHCPv6, lo llama.

Para impedir que `in.ndpd` inicie DHCPv6 se puede modificar el archivo `/etc/inet/ndpd.conf`.

También se puede detener DHCPv6 una vez iniciado mediante una de las siguientes versiones de `ifconfig`:

```
ifconfig <interfaz> inet6 dhcp drop
```

o:

```
ifconfig <interfaz> inet6 dhcp release
```

Cómo gestionan los protocolos del cliente DHCP la información de configuración de red

Los protocolos de los clientes DHCPv4 y DHCPv6 gestionan la información de configuración de red de forma distinta. La principal diferencia es que, con DHCPv4, la negociación es por el permiso de uso de una sola dirección y algunas opciones para acompañarla. Con DHCPv6, la negociación implica un lote de direcciones y de opciones.

Para acceder a información básica sobre la interacción entre el cliente y el servidor DHCPv4, consulte el [Capítulo 12, “Acerca de DHCP \(descripción general\)”](#).

Cómo gestiona el cliente DHCPv4 la información de configuración de red

Una vez obtenido el paquete de información de un servidor DHCP, `dhcpage` configura la interfaz de red y la muestra. El daemon controla la interfaz durante la duración del permiso de la dirección IP y mantiene los datos de configuración en una tabla interna. Las secuencias de inicio del sistema utilizan el comando `dhcpinfo` para extraer valores de opciones de configuración de la tabla interna. Los valores se utilizan para configurar el sistema y permitirle comunicarse a través de la red.

El daemon `dhcpage` espera de forma pasiva a que transcurra un cierto período de tiempo, generalmente la mitad del tiempo de permiso. A continuación, el daemon solicita una ampliación del permiso a un servidor DHCP. Si el sistema notifica a `dhcpage` que la interfaz está cerrada o que la dirección IP ha cambiado, el daemon no controla la interfaz hasta que el comando `ifconfig` le indica que lo haga. Si `dhcpage` obtiene que la interfaz está en marcha y que la dirección IP no ha cambiado, envía una solicitud al servidor para una renovación del permiso. Si no se puede renovar el permiso, `dhcpage` cierra la interfaz al finalizar el período de permiso.

Cada vez que dhcpgent efectúa una acción relacionada con el permiso, el daemon busca un archivo ejecutable denominado `/etc/dhcp/eventhook`. Si se halla un archivo ejecutable con ese nombre, dhcpgent llama a dicho archivo. Consulte [“Secuencias de eventos de cliente DHCP” en la página 448](#) para obtener más información acerca del uso del ejecutable de eventos.

Cómo gestiona el cliente DHCPv6 la información de configuración de red

La comunicación DHCPv6 entre cliente y servidor se inicia con el envío de un mensaje de solicitud por parte del cliente con el objetivo de localizar servidores. En respuesta, todos los servidores disponibles para el servicio DHCP envían un mensaje de anuncio. El mensaje del servidor contiene varios registros IA_NA (Asociación de identidad - Dirección no temporal), así como otras opciones (como direcciones de servidores DNS) que puede proporcionar el servidor.

Un cliente puede solicitar direcciones específicas (y múltiplos de ellas) si incluye sus propios registros IA_NA/IAADDR en el mensaje de solicitud. Generalmente, un cliente solicita direcciones específicas si tiene direcciones antiguas registradas y quiere que el servidor le proporcione las mismas direcciones si es posible. Independientemente de lo que haga el cliente (incluso si no solicita dirección alguna), el servidor puede proporcionarle cualquier número de direcciones para una única transacción DHCPv6.

Este es el diálogo de mensajes entre los clientes y los servidores.

- Un cliente envía un mensaje de solicitud para localizar servidores.
- Los servidores envían un mensaje de anuncio para indicar que están disponibles para el servicio DHCP.
- Un cliente envía un mensaje de solicitud para pedir parámetros de configuración, incluidas direcciones IP, a los servidores con los valores de preferencia más altos. Los valores de preferencia de los servidores los asigna el administrador, y pueden ir desde 0, la mínima preferencia, a 255, la máxima.
- El servidor envía un mensaje de respuesta que contiene los permisos de direcciones y los datos de configuración.

Si el valor de preferencia en el mensaje de anuncio es de 255, el cliente DHCPv6 selecciona inmediatamente ese servidor. Si el servidor con la preferencia más alta no responde o no envía satisfactoriamente un mensaje de respuesta al mensaje de solicitud, el cliente sigue buscando servidores por orden de preferencia hasta que se queda sin mensajes de anuncio. En ese momento, el cliente vuelve a empezar reenviando mensajes de solicitud.

El servidor elegido envía un mensaje de respuesta que contiene las direcciones y parámetros de configuración asignados en respuesta a un mensaje de solicitud de tipo Request o Solicit.

Cierre del cliente DHCP

Al cerrarse, el cliente envía un mensaje de liberación al servidor para indicarle que ya no utilizará una o varias de las direcciones asignadas. Cuando el sistema que ejecuta el cliente DHCPv4 se cierra normalmente, `dhcpagent` escribe la información de configuración actual en el archivo `/etc/dhcp/interfaz.dhc o`, para DHCPv6, en `/etc/dhcp/interfaz.dh6`. De forma predeterminada, el permiso se suele guardar en vez de liberarse, de modo que el servidor DHCP no sabe que la dirección IP no se está usando de forma activa, lo que permite al cliente recuperar fácilmente la dirección en el siguiente inicio. Esta acción predeterminada es equivalente al comando `ifconfig <interfaz> dhcp drop`.

Si el permiso en ese archivo aún es válido cuando el sistema se reinicia, `dhcpagent` envía una solicitud abreviada para utilizar la misma dirección IP e información de configuración de red. Para DHCPv4, es un mensaje de solicitud de tipo Request. Para DHCPv6, es un mensaje de confirmación.

Si el servidor DHCP permite esta solicitud, `dhcpagent` puede utilizar la información que escribió en el disco cuando el sistema se cerró. Si el servidor no da permiso al cliente para utilizar la información, `dhcpagent` inicia la secuencia del protocolo DHCP que se describe en [“Funcionamiento de DHCP” en la página 303](#). El resultado es que el cliente obtiene nueva información de configuración de red.

Activación y desactivación de un cliente DHCP

Para habilitar el cliente DHCP en un sistema que ya está ejecutando Oracle Solaris y no utiliza DHCP, primero debe desconfigurar el sistema. Cuando el sistema se inicie, deberá emitir algunos comandos para configurarlo y activar el cliente DHCP.

Nota – En numerosas implementaciones es habitual que partes esenciales de la infraestructura se configuren con direcciones IP estáticas, en lugar de utilizar DHCP. La determinación de qué dispositivos de la red (como enrutadores y ciertos servidores) deben ser clientes excede el ámbito de esta guía.

▼ Cómo habilitar el cliente DHCP

Este procedimiento sólo debe efectuarse si no se activó DHCPv4 durante la instalación de Oracle Solaris. Nunca es necesario para DHCPv6.

- 1 **Asígnese los permisos de superusuario en el sistema cliente.**

- 2 Si el sistema utiliza preconfiguración en lugar de configuración interactiva, edite el archivo `sysidcfg`. Agregue la subclave `dhcp` a la palabra clave `interfaz_red` en el archivo `sysidcfg`. Por ejemplo, `interfaz_red=hme0 {dhcp}`. Consulte la página del comando `man sysidcfg(4)` para obtener más información.
- 3 **Desconfigure y cierre el sistema.**
`# sys-unconfig`
Consulte la página de comando `man sys-unconfig(1M)` para saber más datos sobre la información de configuración que elimina este comando.
- 4 **Reinicio del sistema una vez completado el cierre.**
Si el sistema utiliza preconfiguración, la subclave `dhcp` del archivo `sysidcfg` configura el sistema para que utilice el cliente DHCP durante el inicio.

Si el sistema no utiliza preconfiguración, `sysidtool` le pedirá información de configuración cuando el sistema reinicie. Para más información consulte la página de comando `man sysidtool(1M)`.
- 5 Cuando se le solicite si se debe usar DHCP para configurar las interfaces de red, especifique **Sí**.

▼ Cómo deshabilitar un cliente DHCP

- 1 **Asígnese los permisos de superusuario en el sistema cliente.**
- 2 Si ha utilizado un archivo `sysidcfg` para preconfigurar el sistema, elimine la subclave `dhcp` de la palabra clave `network_interface`.
- 3 **Desconfigure y cierre el sistema.**
`# sys-unconfig`
Consulte la página de comando `man sys-unconfig(1M)` para saber más datos sobre la información de configuración que elimina este comando.
- 4 **Reinicio del sistema una vez completado el cierre.**
Si el sistema utiliza preconfiguración, no se le solicitará información de configuración y el cliente DHCP no se configura.

Si el sistema no utiliza preconfiguración, `sysidtool` le pedirá información de configuración cuando el sistema se reinicie. Para más información consulte la página de comando `man sysidtool(1M)`.
- 5 Cuando se le solicite si se debe usar DHCP para configurar las interfaces de red, especifique **No**.

Administración del cliente DHCP

El software de cliente DHCP no requiere administración si el sistema se utiliza normalmente. El daemon `dhcpcagent` se inicia automáticamente cuando el sistema se inicia, renegocia los permisos y se detiene cuando se cierra el sistema. Normalmente no se debe iniciar y detener de forma manual el daemon `dhcpcagent` directamente. En vez de eso, como superusuario del sistema cliente, puede utilizar el comando `ifconfig` para modificar la gestión que `dhcpcagent` efectúa de la interfaz de red, si es necesario.

Opciones del comando `ifconfig` que se utilizan con el cliente DHCP

En esta sección se resumen las opciones del comando, documentadas en la página de comando [man ifconfig\(1M\)](#). La única diferencia entre las versiones de DHCPv4 y de DHCPv6 de estos comandos es la palabra clave “inet6”. Incluya la palabra clave “inet6” para DHCPv6, pero no lo haga si ejecuta DHCPv4.

El comando `ifconfig` le permite efectuar las siguientes tareas:

- **Iniciar el cliente DHCP** – El comando `ifconfig interfaz [inet6] dhcp start` inicia la interacción entre `dhcpcagent` y el servidor DHCP para obtener una dirección IP y un nuevo conjunto de opciones de configuración. Este comando resulta útil cuando se modifica información que desea que un cliente utilice de forma inmediata, como cuando se agregan direcciones IP o se cambia la máscara de subred.
- **Sólo solicitar información de configuración de red** – El comando `ifconfig interfaz [inet6] dhcp inform` hace que `dhcpcagent` emita una solicitud de parámetros de configuración de red, con la excepción de la dirección IP. Este comando resulta útil cuando la interfaz de red tiene una dirección IP estática, pero el sistema necesita actualizar las opciones de red. Por ejemplo, este comando es práctico si no se utiliza DHCP para la gestión de direcciones IP, pero sí para configurar los hosts de la red.
- **Solicitar una ampliación del permiso** – El comando `ifconfig interfaz [inet6] dhcp extendipadm refresh-addr dhcp-addrobj` hace que `dhcpcagent` emita una solicitud de renovación del permiso. El cliente solicita automáticamente la renovación de permisos. Sin embargo, puede ser conveniente utilizar este comando si cambia el tiempo de permiso y quiere que los clientes utilicen este nuevo tiempo inmediatamente, en lugar de esperar al siguiente intento de renovación.
- **Liberar la dirección IP** – El comando `ifconfig interfaz [inet6] dhcp release` hace que `dhcpcagent` renuncie a la dirección IP que utiliza la interfaz de red. La liberación de la dirección IP se lleva a cabo automáticamente cuando caduca el permiso. Es conveniente emitir este comando, por ejemplo, desde un equipo portátil si quiere salir de una red y tiene previsto iniciarlo en una red distinta. Consulte también la propiedad `RELEASE_ON_SIGTERM` del archivo de configuración `/etc/default/dhcpcagent`.

- **Abandonar la dirección IP** – El comando `ifconfig interfaz [inet6] dhcp drop` hace que dhcpagent cierre la interfaz de red sin informar al servidor DHCP y reserve el permiso en el sistema de archivos. Este comando permite al cliente utilizar la misma dirección IP al reiniciar.
- **Hacer un ping de la interfaz de red** – El comando `ifconfig interfaz [inet6] dhcp ping` permite determinar si la interfaz está bajo el control de DHCP.
- **Ver el estado de configuración DHCP de la interfaz de red** – El comando `ifconfig interfaz [inet6] dhcp status` muestra el estado actual del cliente DHCP. En la pantalla se muestran los siguientes elementos:
 - Si se ha asociado una dirección IP al cliente
 - El número de solicitudes enviadas, recibidas y rechazadas
 - Si esta interfaz es la principal
 - Veces que se ha obtenido el permiso, cuándo caduca y cuándo está programado el inicio de los intentos de renovación

Por ejemplo:

```
# ifconfig hme0 dhcp status
Interface State      Sent Recv Declined Flags
hme0      BOUND      1    1    0      [PRIMARY]
(Began,Expires,Renew)=(08/16/2005 15:27, 08/18/2005 13:31, 08/17/2005 15:24)

# ifconfig hme0 inet6 dhcp status
Interface State      Sent Recv Declined Flags
hme0      BOUND      1    0    0      [PRIMARY]
(Began,Expires,Renew)=(11/22/2006 20:39, 11/22/2006 20:41, 11/22/2006 20:40)
```

Asignación de los parámetros de configuración del cliente DHCP

El archivo `/etc/default/dhcpagent` del sistema cliente contiene parámetros ajustables para dhcpagent. Puede utilizar un editor de texto para modificar diversos parámetros que afectan al funcionamiento del cliente. El archivo `/etc/default/dhcpagent` está bien documentado; si necesita más información, consulte el propio archivo, así como la página de comando `man dhcpagent(1M)`.

El archivo `/etc/dhcp.interfaz` es otra de las ubicaciones en las que se definen los parámetros que afectan al cliente DHCP. Los parámetros configurados en este archivo se utilizan en las secuencias de inicio del sistema con el comando `ifconfig`. Pero esto solo afecta a DHCPv4. No hay un equivalente para DHCPv6.

De forma predeterminada, el cliente DHCP se configura del siguiente modo:

Para DHCPv4

- El sistema cliente no precisa de un nombre de host específico.
Si quiere que un cliente solicite un nombre de host determinado, consulte [“Nombres de host de cliente DHCPv4” en la página 442](#).
- Las solicitudes predeterminadas del cliente se especifican en `/etc/default/dhcpagent`, e incluyen el servidor DNS, el dominio DNS y la dirección de difusión.
Se puede configurar el archivo de parámetros del cliente DHCP para que solicite más opciones en la palabra clave `PARAM_REQUEST_LIST` del archivo `/etc/default/dhcpagent`. Se puede configurar el servidor DHCP para que ofrezca opciones que no se hayan solicitado de forma explícita. Consulte [“Acerca de macros DHCP” en la página 313](#) y [“Cómo usar macros DHCP \(mapa de tareas\)” en la página 395](#) para obtener información sobre el uso de las macros del servidor DHCP para enviar información a los clientes.

Para DHCPv4 y DHCPv6

- El sistema cliente utiliza DHCP en una interfaz de red física.
Si desea utilizar DHCP en más de una interfaz de red física, consulte [“Sistemas cliente DHCP con varias interfaces de red” en la página 441](#).
- El cliente no se configura automáticamente como cliente de servicio de nombres si se ha configurado después de la instalación de Oracle Solaris.
Consulte [“Sistemas cliente DHCP y servicios de nombres” en la página 443](#) para obtener información acerca del uso de servicios de nombres con clientes DHCP.

Sistemas cliente DHCP con varias interfaces de red

El cliente DHCP puede gestionar simultáneamente varias interfaces distintas en un sistema. Las interfaces pueden ser físicas o lógicas. Cada interfaz tiene su propia dirección IP y tiempo de permiso. Si se configura más de una interfaz de red para DHCP, el cliente emite solicitudes independientes para configurarlas. El cliente mantiene un conjunto independiente de parámetros de configuración de red para cada interfaz. Aunque los parámetros se almacenan de forma independiente, algunos de ellos son de naturaleza global. Los parámetros globales se aplican al sistema en su conjunto, en lugar de a una interfaz de red específica.

El nombre de host, el nombre de dominio NIS y la zona horaria son ejemplos de parámetros globales. Los parámetros globales suelen tener valores distintos para cada interfaz. Sin embargo, solo se puede utilizar un valor para cada parámetro global asociado con cada sistema. Para garantizar que la consulta de un parámetro global recibe una respuesta única, solo se utilizan los parámetros globales de la interfaz de red principal. Puede insertar la palabra `primary` en el archivo `/etc/dhcp.interfaz` de la interfaz que desea tratar como principal. Si no se utiliza la palabra clave `primary`, la primera interfaz en orden alfabético es la que se considerará interfaz principal.

El cliente DHCP gestiona los permisos de las interfaces lógicas y físicas de la misma forma, salvo por la siguiente limitación de las interfaces lógicas:

- El cliente DHCP no gestiona las rutas predeterminadas asociadas con interfaces lógicas.

El núcleo de Oracle Solaris asocia rutas con interfaces físicas, no lógicas. Cuando se establece la dirección IP de una interfaz física, se deben establecer las rutas predeterminadas necesarias en la tabla de enrutamiento. Si a continuación se utiliza DHCP para configurar una interfaz lógica asociada con esa interfaz física, las rutas necesarias ya deben estar establecidas. La interfaz lógica utiliza las mismas rutas.

Cuando caduca un permiso de una interfaz física, el cliente DHCP elimina las rutas predeterminadas asociadas con la interfaz. Cuando caduca un permiso de una interfaz lógica, el cliente DHCP no elimina las rutas predeterminadas asociadas con la interfaz. La interfaz física asociada, y quizá otras interfaces lógicas, pueden tener que utilizar esas mismas rutas.

Si necesita agregar o eliminar rutas predeterminadas asociadas con una interfaz controlada por DHCP, utilice el mecanismo de secuencias de eventos del cliente DHCP. Consulte [“Secuencias de eventos de cliente DHCP” en la página 448](#).

Nombres de host de cliente DHCPv4

De forma predeterminada, el cliente DHCPv4 no proporciona su propio nombre de host, ya que el cliente espera que sea el servidor DHCP el que lo haga. El servidor DHCPv4 está configurado de forma predeterminada para proporcionar nombres de host a los clientes DHCPv4. Cuando se utilizan en conjunto el servidor y el cliente DHCPv4, esta configuración predeterminada funciona perfectamente. Sin embargo, si se utiliza el cliente DHCPv4 con servidores DHCP de terceros, es posible que el cliente no reciba un nombre de host del servidor. Si el cliente DHCP no recibe un nombre de host a través de DHCP, el sistema cliente busca un nombre para utilizar como nombre de host en el archivo `/etc/nodename`. Si el archivo está vacío, se asigna el nombre de host `unknown` (desconocido).

Si el servidor DHCP proporciona un nombre en la opción de DHCP `Hostname`, el cliente utiliza ese nombre de host, aunque se asigne un valor distinto en el archivo `/etc/nodename`. Si quiere que el cliente utilice un nombre de host específico, puede habilitar al cliente para que lo solicite. Consulte el procedimiento siguiente.

Nota – El procedimiento siguiente no funciona con todos los servidores DHCP. Mediante este proceso solicita al cliente que envíe un nombre de host específico al servidor DHCP y que espere el mismo nombre como respuesta.

Sin embargo, el servidor DHCP no tiene por qué satisfacer esta solicitud y, de hecho, muchos no lo hacen. Se limitan a devolver un nombre distinto.

▼ Cómo habilitar un cliente DHCPv4 para que solicite un nombre de host específico

- 1 En el sistema cliente, edite el archivo `/etc/default/dhcpagent` como superusuario.
- 2 Busque la palabra clave `REQUEST_HOSTNAME` en el archivo `/etc/default/dhcpagent` y modifíquela del siguiente modo:
`REQUEST_HOSTNAME=yes`
 Si delante de `REQUEST_HOSTNAME` aparece un signo de comentario (`#`), bórralo. Si no aparece la palabra clave `REQUEST_HOSTNAME`, insértela.
- 3 Edite el archivo `/etc/hostname.interfaz` en el sistema cliente para agregar la línea siguiente:
`inet nombre_host`
`nombre_host` es el nombre que quiere que el cliente utilice.
- 4 Escriba los comandos siguientes para que el cliente efectúe una negociación DHCP completa al reiniciar:

```
# ifconfig interface dhcp release
# reboot
```

Los datos de DHCP reservados en el cliente se eliminan. El cliente reinicia el protocolo para solicitar nueva información de configuración, incluido un nuevo nombre de host. El servidor DHCP se asegura en primer lugar de que otro sistema de la red no utiliza ese nombre de host. El servidor asigna entonces el nombre de host al cliente. Si se configura para ello, el servidor DHCP puede actualizar los servicios de nombres con el nombre de host del cliente.

Si desea modificar el nombre de host más adelante, repita el [Paso 3](#) y el [Paso 4](#).

Sistemas cliente DHCP y servicios de nombres

Los sistemas Oracle Solaris admiten los siguientes servicios de nombres: DNS, NIS, NIS+ y un almacén en un archivo local (`/etc/inet/hosts`). Cada servicio de nombres requiere configurar algunos aspectos antes de poder utilizarse. El archivo de configuración de cambios del servicio de nombres (ver [nsswitch.conf\(4\)](#)) debe también configurarse de forma adecuada para indicar los servicios de nombres que se deben utilizar.

Antes de que un cliente DHCP puede utilizar un servicio de nombres, se debe configurar el sistema como cliente del servicio. De forma predeterminada y a menos que se indique lo contrario durante la instalación del sistema, solo se utilizan archivos locales.

En la tabla siguiente se resumen las cuestiones relacionadas con cada servicio de nombres y DHCP. La tabla contiene también vínculos a documentación que pueden ayudarle a configurar clientes para cada servicio de nombres.

TABLA 16-1 Información de cliente de servicio de nombres para sistemas cliente DHCP

Servicio de nombres	Información de configuración de cliente
NIS	<p>Si utiliza DHCP para enviar información de la instalación de red de Oracle Solaris a un sistema cliente, puede utilizar una macro de configuración que contiene las opciones NISservs y NISdmain. Estas opciones pasan las direcciones IP de los servidores NIS y el nombre de dominio NIS al cliente. El cliente se convierte automáticamente en cliente NIS.</p> <p>Si un sistema cliente DHCP ya está ejecutando Oracle Solaris, el cliente NIS no se configura automáticamente en ese sistema cuando el servidor DHCP envía información NIS al cliente.</p> <p>Si el servidor DHCP se configura para enviar información NIS al sistema cliente DHCP, puede ver los valores proporcionados al cliente utilizando el comando <code>dhcpcinfo</code> en el cliente, de la siguiente forma:</p> <pre># /sbin/dhcpcinfo NISdmain # /sbin/dhcpcinfo NISservs</pre> <p>Nota – Para DHCPv6, incluya <code>-v6</code> y palabras clave de protocolo distintas en el comando.</p> <pre># /sbin/dhcpcinfo -v6 NISDomain # /sbin/dhcpcinfo -v6 NISServers</pre> <p>Utilice los valores devueltos para el nombre del dominio NIS y los servidores NIS al configurar el sistema como cliente NIS.</p> <p>Para configurar un cliente NIS para un sistema cliente DHCP, utilice el método estándar documentado en el Capítulo 5, “Instalación y configuración del servicio NIS” de <i>Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)</i>.</p> <p>Consejo – Puede escribir una secuencia de comandos que utilice <code>dhcpcinfo</code> e <code>ypinit</code> para automatizar la configuración de clientes NIS en sistemas cliente DHCP.</p>
NIS+	<p>Si el cliente NIS+ para un sistema cliente DHCP se configura de la forma convencional, es posible que el servidor DHCP proporcione de vez en cuando al cliente direcciones distintas. Esto provoca problemas de seguridad, ya que la seguridad de NIS+ incluye la dirección IP como parte de la configuración. Para garantizar que el cliente tenga la misma dirección cada vez, configure el cliente NIS+ para un sistema cliente DHCP de forma no estándar, según se documenta en “Configuración de clientes DHCP como clientes NIS+” en la página 445.</p> <p>Si se ha asignado manualmente una dirección IP al sistema cliente DHCP, la dirección del cliente será siempre la misma. El cliente NIS+ se puede configurar de la forma estándar, descrita en “Setting Up NIS+ Client Machines” de <i>System Administration Guide: Naming and Directory Services (NIS+)</i>.</p>

TABLA 16-1 Información de cliente de servicio de nombres para sistemas cliente DHCP
(Continuación)

Servicio de nombres	Información de configuración de cliente
/etc/inet/hosts	Deberá configurar el archivo /etc/inet/hosts para un sistema cliente DHCP que vaya a utilizar /etc/inet/hosts para su servicio de nombres. El nombre de host del sistema cliente DHCP se agrega a su propio archivo /etc/inet/hosts mediante las herramientas de DHCP. Sin embargo, se debe agregar manualmente el nombre de host al archivo /etc/inet/hosts de otros sistemas de la red. Si el sistema servidor DHCP utiliza /etc/inet/hosts para la resolución de nombres, deberá agregar también manualmente el nombre de host del cliente al sistema.
DNS	Si el sistema cliente DHCP recibe el nombre de dominio DNS a través de DHCP, el archivo /etc/resolv.conf del sistema cliente se configura automáticamente. El archivo /etc/nsswitch.conf se actualiza también automáticamente para agregar dns a la línea hosts a continuación de otros servicios de nombres en el orden de búsqueda. Para obtener más información acerca de DNS, consulte la Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP) .

Configuración de clientes DHCP como clientes NIS+

Puede utilizar el servicio de nombres NIS+ en sistemas Oracle Solaris que sean clientes DHCP. Sin embargo, si su servidor DHCP puede proporcionar direcciones distintas en momentos distintos, este hecho burla parcialmente una de las opciones de mejora de seguridad de NIS+: la creación de credenciales de Estándar de cifrado de datos (DES). Por seguridad, configure el servidor DHCP para que proporcione siempre la misma dirección. Cuando se configura un cliente NIS+ que *no* utiliza DHCP, se agregan al servidor NIS+ credenciales DES únicas para el cliente. Hay varias formas de crear credenciales, como el uso de la secuencia `niscient` o el comando `nissaddcred`.

La generación de credenciales NIS+ requiere que un cliente tenga un nombre de host estático para crear y almacenar las credenciales. Si quiere utilizar NIS+ y DHCP, deberá crear credenciales idénticas que se utilizarán para todos los nombres de host de los clientes DHCP. De este modo, no importa qué dirección IP y nombre de host asociado reciba un cliente DHCP, porque el cliente podrá utilizar las mismas credenciales DES.

El procedimiento siguiente muestra cómo se crean credenciales idénticas para todos los nombres de host DHCP. El procedimiento es válido únicamente si se conocen los nombres de host que utilizan los clientes DHCP. Por ejemplo, cuando el servidor DHCP genera los nombres de host, se saben los posibles nombres de host que puede recibir un cliente.

▼ Cómo configurar clientes DHCP como clientes NIS+

Un sistema cliente DHCP que vaya a ser cliente NIS+ deberá utilizar credenciales que pertenezcan a otro sistema cliente NIS+ del dominio NIS+. Este procedimiento genera únicamente credenciales para el sistema, que se aplican solo al superusuario que ha iniciado

sesión en el sistema. Otros usuarios que inicien sesión en el sistema cliente DHCP deberán disponer de sus propias credenciales únicas en el servidor NIS+. Estas credenciales se crean mediante el procedimiento descrito en la [System Administration Guide: Naming and Directory Services \(NIS+\)](#).

- 1 Para crear las credenciales para un cliente, escriba el siguiente comando en el servidor NIS+:**

```
# nisgrep nisplus-client-name cred.org_dir > /tmp/file
```

Este comando escribe la entrada de la tabla `cred.org_dir` correspondiente al cliente NIS+ en un archivo temporal.

- 2 Utilice el comando `cat` para ver el contenido de este archivo.**

También puede utilizar un editor de texto.

- 3 Copie las credenciales para utilizar para los clientes DHCP.**

Deberá copiar la clave pública y la privada, que son largas secuencias de números y letras separadas por dos puntos (:). Las credenciales se deberán pegar en el comando que se emitirá en el siguiente paso.

- 4 Agregue credenciales para un cliente DHCP mediante el siguiente comando:**

```
# nistbladm -a cname="dhcp-client-name@nisplus-domain" auth_type=DES \
auth_name="unix.dhcp-client-name@nisplus-domain" \
public_data=copied-public-key \
private_data=copied-private-key
```

En *clave_pública_copiada*, pegue la información de clave pública que ha copiado del archivo temporal. En *clave_privada_copiada*, pegue la información de clave privada que ha copiado del archivo temporal.

- 5 Copie de forma remota los archivos desde el sistema cliente NIS+ al sistema cliente DHCP emitiendo los siguientes comandos en el sistema cliente DHCP:**

```
# rcp nisplus-client-name:/var/nis/NIS_COLD_START /var/nis
# rcp nisplus-client-name:/etc/.rootkey /etc
# rcp nisplus-client-name:/etc/defaultdomain /etc
```

Si recibe un mensaje de “permission denied” (permiso denegado), es posible que los sistemas no estén configurados para permitir la copia remota. En tal caso, puede copiar los archivos como usuario normal a una ubicación intermedia. Como superusuario, copie los archivos desde la ubicación intermedia a la ubicación apropiada en el sistema cliente DHCP.

- 6 Copie el archivo de cambios del servicio de nombres correcto para NIS+ mediante el siguiente comando en el sistema cliente DHCP:**

```
# cp /etc/nsswitch.nisplus /etc/nsswitch.conf
```

- 7 Reinicie el sistema cliente DHCP.**

Ahora, el sistema cliente DHCP ya podrá utilizar los servicios NIS+.

Ejemplo 16-1 Configuración de un sistema cliente DHCP como cliente NIS+

En el ejemplo siguiente se supone que cuenta con un sistema `nisei`, el cual es un cliente NIS+ en el dominio NIS+ `dev.example.net`. También tiene un sistema cliente DHCP, `dhow`, y quiere que `dhow` sea un cliente NIS+.

```
(First log in as superuser on the NIS+ server)
# nistgrep nisei cred.org_dir > /tmp/nisei-cred
# cat /tmp/nisei-cred
nisei.dev.example.net.:DES:unix.nisei@dev.example.net:46199279911a84045b8e0
c76822179138173a20edbd8eab4:90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830
c05bc1c724b
# nistbladm -a cname="dhow@dev.example.net." \
auth_type=DES auth_name="unix.dhow@dev.example.net" \
public_data=46199279911a84045b8e0c76822179138173a20edbd8eab4 \
private_data=90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830\
c05bc1c724b
# rlogin dhow
(Log in as superuser on dhow)
# rcp nisei:/var/nis/NIS_COLD_START /var/nis
# rcp nisei:/etc/.rootkey /etc
# rcp nisei:/etc/defaultdomain /etc
# cp /etc/nsswitch.nisplus /etc/nsswitch.conf
# reboot
```

El sistema cliente DHCP `dhow` podrá ahora utilizar los servicios NIS+.

Ejemplo 16-2 Adición de credenciales mediante una secuencia de comandos

Si quiere configurar una gran cantidad de clientes DHCP como clientes NIS+, puede escribir una secuencia. Una secuencia puede agregar rápidamente las entradas a la tabla NIS+ `cred.org_dir`. A continuación se muestra un ejemplo de secuencia.

```
#!/usr/bin/ksh
#
# Copyright (c) by Sun Microsystems, Inc. All rights reserved.
#
# Sample script for cloning a credential. Hosts file is already populated
# with entries of the form dhcp-[0-9][0-9][0-9]. The entry we're cloning
# is dhcp-001.
#
#
PUBLIC_DATA=6e72878d8dc095a8b5aea951733d6ea91b4ec59e136bd3b3
PRIVATE_DATA=3a86729b685e2b2320cd7e26d4f1519ee070a60620a93e48a8682c5031058df4
HOST="dhcp-"
DOMAIN="mydomain.example.com"

for
i in 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019
do
```

```
print - ${HOST}${i}
#nistbladm -r [cname="${HOST}${i}.${DOMAIN}."]cred.org_dir
nistbladm -a cname="${HOST}${i}.${DOMAIN}." \
    auth_type=DES auth_name="unix.${HOST}${i}@${DOMAIN}" \
    public_data=${PUBLIC_DATA} private_data=${PRIVATE_DTA} cred.org_Dir
done
exit 0
```

Secuencias de eventos de cliente DHCP

El cliente DHCP se puede configurar para que ejecute un programa o secuencia que lleve a cabo cualquier acción adecuada para el sistema cliente. El programa o secuencia, que se denomina, *secuencia de eventos*, se ejecuta automáticamente cuando tienen lugar determinados eventos de permiso de DHCP. La secuencia de eventos se puede utilizar para ejecutar otros comandos, programas o secuencias en respuesta a eventos de permiso específicos. Para utilizar esta función deberá proporcionar su propia secuencia.

dhcpgent utiliza las siguientes palabras clave para referirse a eventos de permisos de DHCP:

Palabra clave de evento	Descripción
BOUND y BOUND6	La interfaz está configurada para DHCP. El cliente recibe el mensaje de confirmación (DHCPv4 ACK) o (DHCPv6 Reply) del servidor DHCP en el que se concede la solicitud de permiso para una dirección IP. Se llama a la secuencia de eventos inmediatamente después de la configuración satisfactoria de la interfaz.
EXTEND y EXTEND6	El cliente ha realizado correctamente una concesión. Se llama a la secuencia de eventos inmediatamente después de que el cliente recibe el mensaje de confirmación del servidor DHCP por la solicitud de renovación.
EXPIRE y EXPIRE6	El permiso caduca cuando se agota su tiempo. Para DHCPv4, la secuencia de eventos se llama inmediatamente después de que la dirección permitida se elimina de la interfaz y se marca esta como desconectada. Para DHCPv6, la secuencia de eventos se llama justo antes de que las últimas direcciones permitidas se eliminen de la interfaz.
DROP y DROP6	El cliente usa la concesión para eliminar la interfaz desde el control DHCP. Se llama a la secuencia de eventos inmediatamente antes de la interfaz se retire del control de DHCP.
RELEASE y RELEASE6	El cliente deja de usar la dirección IP. Se llama a la secuencia de eventos inmediatamente antes de que el cliente libere la dirección en la interfaz y envíe el paquete DHCPv4 RELEASE o DHCPv6 Release al servidor DHCP.

INFORM e INFORM6	Una interfaz obtiene información de configuración nueva o actualizada de un servidor DHCP a través del mensaje DHCPv4 INFORM o DHCPv6 Information-Request. Estos eventos tienen lugar cuando el cliente DHCP solo obtiene parámetros de configuración del servidor, pero no obtiene un permiso de dirección IP.
LOSS6	Durante la caducidad del permiso, cuando aún quedan uno o más permisos válidos, se llama a la secuencia de eventos justo antes de eliminar las direcciones caducadas. Las direcciones que se van a eliminar se marcan con el indicador IFF_DEPRECATED.

Con cada uno de estos eventos, dhcpagent llama al comando siguiente:

```
/etc/dhcp/eventhook interface event
```

donde *interfaz* es la interfaz que utiliza DHCP y *evento* es una de las palabras clave de evento descritas anteriormente. Por ejemplo, cuando la interfaz `ce0` se configura por primera vez para DHCP, dhcpagent llama a la secuencia de eventos de la siguiente forma:

```
/etc/dhcp/eventhook ce0 BOUND
```

Para utilizar la función de secuencia de eventos, haga lo siguiente:

- Asigne al archivo ejecutable el nombre `/etc/dhcp/eventhook`.
- Establezca el propietario del archivo en `root`.
- Establezca los permisos en `755 (rwxr-xr-x)`.
- Escriba la secuencia o programa que debe llevar a cabo una serie de acciones en respuesta a alguno de los eventos documentados. Se puede agregar nuevos eventos, de modo que el programa debe hacer caso omiso de los eventos no reconocidos o que no requieren acción. Por ejemplo, el programa o secuencia puede escribir un archivo de registro cuando el evento es `RELEASE`, y no hacer caso de los demás eventos.
- El programa o secuencia no debe ser interactivo. Antes de llamar a la secuencia de eventos, `stdin`, `stdout` y `stderr` se conectan a `/dev/null`. Para ver la salida de errores, deberá redirigirla a un archivo.

La secuencia de eventos hereda su entorno de programa de dhcpagent, y se ejecuta con privilegios de `root`. Si es necesario, la secuencia puede utilizar la utilidad `dhcpinfo` para obtener más información acerca de la interfaz. Para más información consulte la página de comando `man dhcpinfo(1)`.

El daemon dhcpagent espera la salida de la secuencia de eventos para todos los eventos. Si la secuencia de eventos no sale transcurridos 55 segundos, dhcpagent envía una señal `SIGTERM` al proceso de la secuencia. Si el proceso sigue sin salir pasados otros tres segundos, el daemon envía una señal `SIGKILL` para cerrar el proceso.

En la página de comando man [dhcpageant\(1M\)](#) se muestra un ejemplo de secuencia de eventos.

El [Ejemplo 16-3](#) muestra la forma de utilizar una secuencia de eventos DHCP para mantener actualizado el contenido del archivo `/etc/resolv.conf`. Cuando tienen lugar los eventos BOUND y EXTEND, la secuencia sustituye los nombres del servidor de dominios y del servidor de nombres. Cuando tienen lugar los eventos EXPIRE, DROP y RELEASE, la secuencia elimina del archivo los nombres del servidor de dominios y del servidor de nombres.

Nota – La secuencia de ejemplo supone que DHCP es el origen de autoridad del servidor de dominios y del servidor de nombres. También supone que todas las interfaces bajo control de DHCP devuelven información coherente y actualizada. Es posible que estas hipótesis no reflejen las condiciones reales de su sistema.

EJEMPLO 16-3 Secuencia de eventos para actualizar el archivo `/etc/resolv.conf`

```
#!/bin/ksh -p

PATH=/bin:/sbin export PATH
umask 0222

# Refresh the domain and name servers on /etc/resolv.conf

insert ()
{
    dnsservers='dhcpinfo -i $1 DNSserv'
    if [ -n "$dnsservers" ]; then
        # remove the old domain and name servers
        if [ -f /etc/resolv.conf ]; then
            rm -f /tmp/resolv.conf.$$
            sed -e '/^domain/d' -e '/^nameserver/d' \
                /etc/resolv.conf > /tmp/resolv.conf.$$
        fi

        # add the new domain
        dnsdomain='dhcpinfo -i $1 DNSdmain'
        if [ -n "$dnsdomain" ]; then
            echo "domain $dnsdomain" >> /tmp/resolv.conf.$$
        fi

        # add new name servers
        for name in $dnsservers; do
            echo nameserver $name >> /tmp/resolv.conf.$$
        done
        mv -f /tmp/resolv.conf.$$ /etc/resolv.conf
    fi
}

# Remove the domain and name servers from /etc/resolv.conf

remove ()
{
    if [ -f /etc/resolv.conf ]; then
        rm -f /tmp/resolv.conf.$$
    fi
}
```

EJEMPLO 16-3 Secuencia de eventos para actualizar el archivo `/etc/resolv.conf` (Continuación)

```
        sed -e '/^domain/d' -e '/^nameserver/d' \
            /etc/resolv.conf > /tmp/resolv.conf.$$
        mv -f /tmp/resolv.conf.$$ /etc/resolv.conf
    fi
}

case $2 in
BOUND | EXTEND)
    insert $1
    exit 0
    ;;
EXPIRE | DROP | RELEASE)
    remove
    exit 0
    ;;
*)
    exit 0
    ;;
esac
```


Solución de problemas de DHCP (referencia)

En este capítulo se ofrece información para ayudarle a resolver problemas que pueden aparecer al configurar un servidor o cliente DHCP. También puede servir de ayuda con posibles problemas de uso de DHCP una vez finalizada la configuración.

Este capítulo contiene la información siguiente:

- [“Solución de problemas del servidor DHCP” en la página 453](#)
- [“Solución de problemas de configuración del cliente DHCP” en la página 459](#)

Consulte el [Capítulo 14, “Configuración del servicio DHCP \(tareas\)”](#) para obtener información sobre la configuración del servidor DHCP. Consulte [“Activación y desactivación de un cliente DHCP” en la página 437](#) para obtener información sobre la configuración de su cliente DHCP.

Solución de problemas del servidor DHCP

Los posibles problemas de configuración del servidor se pueden dividir en las categorías siguientes:

- [“Problemas de NIS+ y el almacén de datos DHCP” en la página 453](#)
- [“Errores de asignación de dirección IP en DHCP” en la página 457](#)

Problemas de NIS+ y el almacén de datos DHCP

Si utiliza NIS+ como almacén de datos DHCP, los posibles problemas se dividen en las siguientes categorías:

- [“No se puede seleccionar NIS+ como almacén de datos DHCP” en la página 454](#)
- [“NIS+ no está bien configurado como almacén de datos DHCP” en la página 454](#)
- [“Problemas de acceso de NIS+ para el almacén de datos DHCP” en la página 455](#)

No se puede seleccionar NIS+ como almacén de datos DHCP

Si intenta utilizar NIS+ como almacén de datos, es posible que DHCP Manager no ofrezca NIS+ como opción de almacén de datos. Si utiliza el comando `dhcpconfig`, quizá se muestre un mensaje indicando que NIS+ no parece estar instalado y en ejecución. Estos dos síntomas significan que NIS+ no se ha configurado para este servidor, aunque puede que NIS+ se esté utilizando en la red. Antes de poder seleccionar NIS+ como almacén de datos, el sistema servidor se debe configurar como cliente NIS+.

Antes de configurar el sistema servidor DHCP como cliente NIS+ se deben cumplir las siguientes condiciones:

- El dominio ya debe estar configurado.
- El servidor maestro del dominio NIS+ se debe estar ejecutando.
- Las tablas del servidor maestro deben estar llenas.
- La tabla de hosts debe contener una entrada para el nuevo sistema cliente, el sistema servidor DHCP.

“Setting Up NIS+ Client Machines” de *System Administration Guide: Naming and Directory Services (NIS+)* ofrece información detallada acerca de la configuración de un cliente NIS+.

NIS+ no está bien configurado como almacén de datos DHCP

Si ya ha utilizado satisfactoriamente NIS+ con DHCP, puede encontrarse con errores si se efectúan cambios en NIS+. Los cambios pueden provocar problemas de configuración. Utilice las siguientes descripciones de problemas y sus soluciones para ayudarle a determinar la causa de los problemas de configuración.

Problema: El objeto raíz no existe en el dominio NIS+.

Solución: Escriba el siguiente comando:

```
/usr/lib/nis/nisstat
```

Este comando muestra las estadísticas del dominio. Si el objeto raíz no existe, no se devuelve estadística alguna.

Configure el dominio NIS+ siguiendo las indicaciones de la *System Administration Guide: Naming and Directory Services (NIS+)*.

Problema: NIS+ no se utiliza para la información de `passwd` y `publickey`.

Solución: Escriba el comando siguiente para ver el archivo de configuración del cambio de servicio de nombres:

```
cat /etc/nsswitch.conf
```

Compruebe si en las entradas `passwd` y `publickey` aparece la palabra clave “nisplus”. Consulte la *System Administration Guide: Naming and Directory Services (NIS+)* para obtener información acerca de la configuración del cambio de servicio de nombres.

Problema: El nombre de dominio está vacío.

Solución: Escriba el siguiente comando:

```
domainname
```

Si el comando muestra una cadena vacía, no se ha establecido ningún nombre para el dominio. Utilice archivos locales como almacén de datos o configure un dominio NIS+ para su red. Consulte la [System Administration Guide: Naming and Directory Services \(NIS+\)](#).

Problema: El archivo NIS_COLD_START no existe.

Solución: Escriba el comando siguiente en el sistema servidor para determinar si el archivo existe:

```
cat /var/nis/NIS_COLD_START
```

Utilice archivos locales como almacén de datos o cree un cliente NIS+. Consulte la [System Administration Guide: Naming and Directory Services \(NIS+\)](#).

Problemas de acceso de NIS+ para el almacén de datos DHCP

Los problemas de acceso de NIS+ pueden provocar mensajes de error sobre credenciales DES incorrectas, o permisos inadecuados para actualizar objetos y tablas NIS+. Utilice las siguientes descripciones de problemas y soluciones para determinar la causa de los errores de acceso de NIS+ recibidos.

Problema: El sistema servidor DHCP no tiene acceso de creación para el objeto `org_dir` en el dominio NIS+.

Solución: Escriba el siguiente comando:

```
nisls -ld org_dir
```

Los derechos de acceso se muestran en la forma `r---rmdrmdr---`, donde los permisos se aplican respectivamente a `nobody` (nadie), `owner` (propietario), `group` (grupo) y `world` (todos). El propietario del objeto se indica a continuación.

Normalmente, el objeto de directorio `org_dir` proporciona todos los derechos al propietario y al grupo. "Todos los derechos" significa derechos de leer, modificar, crear y destruir. El objeto de directorio `org_dir` proporciona únicamente acceso de lectura a las clases `world` y `nobody`.

El nombre del servidor DHCP debe figurar como propietario del objeto `org_dir` o bien como principal en el grupo. El grupo debe tener acceso de creación. Utilice el comando siguiente para ver el grupo:

```
nisls -ldg org_dir
```

Utilice el comando `nischmod` para cambiar los permisos de `org_dir`, si es necesario. Por ejemplo, para agregar al grupo acceso de creación, escriba el siguiente comando:

```
nischmod g+c org_dir
```

Para más información consulte la página de comando `man nischmod(1)`.

Problema: El servidor DHCP no tiene derechos de acceso para crear una tabla en el objeto `org_dir`.

Normalmente, este problema significa que el nombre principal del sistema servidor no es miembro del grupo propietario del objeto `org_dir`, o que no existe un grupo propietario.

Solución: Escriba este comando para averiguar el nombre del grupo propietario:

niscat -o org_dir

Busque una línea similar a la siguiente:

Group : "admin.example.com."

Para ver los nombres de principales del grupo, utilice el comando:

nisgrpadm -l groupname

Por ejemplo, este comando muestra los nombres de principales del grupo `admin.example.com`:

`nisgrpadm -l admin.example.com`

El nombre del sistema servidor debe aparecer como miembro explícito del grupo o estar incluido como miembro implícito de él. Si es necesario, agregue el nombre del sistema servidor al grupo mediante el comando `nisgrpadm`.

Por ejemplo, para agregar el servidor de nombres `pacific` al grupo `admin.example.com`, utilice el siguiente comando:

`nisgrpadm -a admin.example.com pacific.example.com`

Para más información consulte la página de comando `man nisgrpadm(1)`.

Problema: El servidor DHCP no tiene credenciales de Estándar de cifrado de datos (DES) válidas en la tabla `cred` de NIS+.

Solución: En caso de problema de credenciales, un mensaje de error indica que el usuario no dispone de credenciales DES en el servicio de nombres NIS+.

Utilice el comando `nisaddcred` para agregar credenciales de seguridad para un sistema servidor DHCP.

En el ejemplo siguiente se muestra la forma de agregar credenciales DES para el sistema `mercury` en el dominio `example.com`:

`nisaddcred -p unix.mercury@example.com \
-P mercury.example.com. DES example.com.`

El comando solicita la contraseña de usuario `root`, necesaria para generar una clave secreta cifrada.

Para más información consulte la página de comando `man nisaddcred(1M)`.

Errores de asignación de dirección IP en DHCP

Cuando un cliente intenta obtener o verificar una dirección IP, es posible que se registren problemas en `syslog` o en la salida del modo de depuración del servidor. En la siguiente lista de mensajes de error comunes se indican las posibles causas y las soluciones.

No existe la tabla de red dhcp *n.n.n.n* para la red DHCP del cliente

Causa: Un cliente solicita una dirección IP específica o intenta ampliar un permiso para su dirección IP actual. El servidor DHCP no puede encontrar la tabla de red DHCP para esa dirección.

Solución: Es posible que la tabla de red DHCP se haya eliminado por error. Se puede recrear la tabla de red agregando la red de nuevo mediante el Administrador de DHCP o mediante el comando `dhcpconfig`.

Respuesta de ICMP ECHO al candidato de OFFER: *n.n.n.n*, desactivando

Causa: La dirección IP que se iba a ofrecer a un cliente DHCP ya se está utilizando. Este problema puede surgir si hay más de un servidor DHCP propietario de la dirección. También puede ocurrir si se ha configurado manualmente una dirección para un cliente de red no DHCP.

Solución: Determine el verdadero propietario de la dirección. Corrija la base de datos del servidor DHCP o la configuración de red del host.

Respuesta de ICMP ECHO al candidato de OFFER: *n.n.n.n*. No hay registro de red dhcp correspondiente.

Causa: La dirección IP que se iba a ofrecer a un cliente DHCP no tiene un registro en una tabla de red. Este error indica que el registro de la dirección IP se eliminó de la tabla de red DHCP después de seleccionar la dirección. Este error solo puede suceder durante el breve intervalo antes de terminar de comprobar la dirección duplicada.

Solución: Utilice DHCP Manager o el comando `pntadm` para ver la tabla de red DHCP. Si falta la dirección IP, créela con DHCP Manager eligiendo Crear en el menú Edición de la tabla Dirección. También puede crear la dirección IP con el comando `pntadm`.

Registro de red DHCP para *n.n.n.n* no disponible, solicitud ignorada.

Causa: El registro de la dirección IP solicitada no está en la tabla de red DHCP, de modo que el servidor abandona la solicitud.

Solución: Utilice DHCP Manager o el comando `pntadm` para ver la tabla de red DHCP. Si falta la dirección IP, créela con DHCP Manager eligiendo Crear en el menú Edición de la tabla Dirección. También puede crear la dirección IP con el comando `pntadm`.

n.n.n.n actualmente marcada como no utilizable.

Causa: La dirección IP solicitada no se puede ofrecer porque se ha marcado como no utilizable en la tabla de red.

Solución: Utilice DHCP Manager o el comando `pntadm` para marcar la dirección como utilizable.

n.n.n.n se ha asignado manualmente. No se asignará ninguna dirección dinámica.

Causa: Se ha asignado manualmente una dirección al ID de cliente, y se ha marcado la dirección como no utilizable. El servidor no puede asignar a este cliente una dirección distinta.

Solución: Utilice DHCP Manager o el comando `pntadm` para hacer que la dirección sea utilizable, o asigne manualmente al cliente una dirección distinta.

La asignación manual (*n.n.n.n*, *ID de cliente*) tiene otros *n* registros. Debería tener 0.

Causa: Se ha asignado manualmente más de una dirección IP al cliente con el ID especificado. Solo se debe asignar una dirección por cliente. El servidor selecciona la última dirección asignada que encuentra en la tabla de red.

Solución: Utilice DHCP Manager o el comando `pntadm` para modificar direcciones IP y eliminar las asignaciones manuales adicionales.

No hay más direcciones IP en la red *n.n.n.n*.

Causa: Se han asignado todas las direcciones IP actualmente gestionadas por DHCP en la red especificada.

Solución: Utilice DHCP Manager o el comando `pntadm` para crear nuevas direcciones IP para esta red.

El permiso del cliente: *ID_cliente* en *n.n.n.n* ha caducado.

Causa: El permiso no era negociable y ha caducado.

Solución: El cliente deberá iniciar automáticamente el protocolo para obtener un nuevo permiso.

Ha caducado la oferta para el cliente: *n.n.n.n*

Causa: El servidor ha hecho una oferta de dirección IP al cliente, pero el cliente ha tardado demasiado en responder y la oferta ha caducado.

Solución: El cliente deberá emitir automáticamente otro mensaje de descubrimiento. Si este mensaje caduca también, aumente el tiempo de caducidad de ofertas del servidor DHCP. En el Administrador de DHCP, elija Modify en el menú Service.

El permiso del cliente: *ID_cliente* le falta la opción de IP solicitada.

Causa: La solicitud del cliente no especificaba la dirección IP ofrecida, de modo que el servidor DHCP ha hecho caso omiso de la solicitud. Este problema puede presentarse si se utiliza un cliente DHCP de otro fabricante que no sea compatible con el protocolo DHCP actualizado, RFC 2131.

Solución: Actualice el software cliente.

El permiso del cliente: *ID_cliente* está intentando renovar *n.n.n.n*, una dirección IP a la que no ha dado permiso.

Causa: La dirección IP de este cliente en la tabla de red DHCP no coincide con la dirección IP especificada en su solicitud de renovación. El servidor DHCP no renueva el permiso. Este problema se puede presentar al borrar un registro del cliente mientras este está aún utilizando la dirección IP.

Solución: Utilice DHCP Manager o el comando `pntadm` para examinar la tabla de red y corregir el registro del cliente en caso necesario. El ID del cliente debe estar vinculado a la dirección IP especificada. Si no está vinculado a ella, edite las propiedades de la dirección para agregar el ID del cliente.

El permiso del cliente: *ID_cliente* está intentando verificar la dirección no registrada: *n.n.n.n*, ignorada.

Causa: El cliente especificado no se ha registrado en la tabla de red DHCP con esta dirección, de modo que este servidor DHCP hace caso omiso de la solicitud.

Es posible que otro servidor DHCP de la red haya asignado la dirección al cliente. Sin embargo, puede que haya eliminado también el registro del cliente mientras este aún estaba utilizando la dirección IP.

Solución: Utilice DHCP Manager o el comando `pntadm` para examinar la tabla de red de este servidor y otros servidores DHCP de la red. Efectúe las correcciones necesarias.

También puede no hacer nada y permitir que el permiso caduque. El cliente solicitará automáticamente un nuevo permiso de dirección.

Si quiere que el cliente obtenga un nuevo permiso inmediatamente, reinicie el protocolo DHCP en el cliente mediante los comandos siguientes:

```
ifconfig interface dhcp release  
ifconfig interface dhcp start
```

Solución de problemas de configuración del cliente DHCP

Los problemas que pueden aparecer con un cliente DHCP pertenecen a alguna de las siguientes categorías:

- “Problemas de comunicación con el servidor DHCP” en la página 460
- “Problemas por información de configuración DHCP incorrecta” en la página 468

Problemas de comunicación con el servidor DHCP

En esta sección se describen los problemas que se pueden presentar al agregar clientes DHCP a la red.

Después de activar el software cliente y reiniciar el sistema, el cliente intentará conectar con el servidor DHCP para obtener su configuración de red. Si el cliente no puede acceder al servidor, es posible que se muestren mensajes de error similares a los siguientes:

DHCP or BOOTP server not responding

Antes de poder determinar el problema, deberá reunir información de diagnóstico del cliente y del servidor. Para recopilar esta información, efectúe las siguientes tareas:

1. “Cómo ejecutar el cliente DHCP en modo de depuración” en la página 460
2. “Cómo ejecutar el servidor DHCP en modo de depuración” en la página 461
3. “Cómo utilizar snoop para supervisar el tráfico DHCP en la red” en la página 461

Puede llevar a cabo estos procesos de forma independiente o simultánea.

La información recogida puede ayudarle a determinar si el problema es del cliente, del servidor o de un agente de reenvío. Esto le permitirá hallar una solución.

▼ Cómo ejecutar el cliente DHCP en modo de depuración

Si no es un cliente DHCP, consulte la documentación del cliente para obtener información sobre cómo ejecutarlo en modo de depuración.

Si tiene un cliente DHCP, siga estos pasos.

1 Asígnese los privilegios de superusuario en el sistema del cliente DHCP.

2 Finalice el daemon del cliente DHCP.

```
# pkill -x dhcpcd
```

3 Reinicie el daemon en modo de depuración.

```
# /sbin/dhcpcd -d -f &
```

La opción `-d` pone el cliente DHCP en modo de depuración con detalle de nivel 1. La opción `-f` hace que la salida se envíe a la consola en lugar de a `syslog`.

4 Configure la interfaz para que inicie la negociación DHCP.

```
# ifconfig interface dhcp start
```

Sustituya *interface* por el nombre de la interfaz de red del cliente, por ejemplo `ge0`.

Cuando se ejecuta en modo de depuración, el daemon del cliente muestra mensajes en pantalla mientras atiende las solicitudes de DHCP. Consulte [“Salida del cliente DHCP en modo de depuración” en la página 462](#) para obtener información sobre la salida del cliente en dicho modo.

▼ **Cómo ejecutar el servidor DHCP en modo de depuración**

- 1 **Conviértase en superusuario en el sistema del servidor.**

- 2 **Detenga temporalmente el servidor DHCP.**

```
# svcadm disable -t svc:/network/dhcp-server
```

También puede utilizar DHCP Manager o dhcpconfig para detener el servidor.

- 3 **Reinicie el daemon en modo de depuración.**

```
# /usr/lib/inet/in.dhcpd -d -v
```

Deberá utilizar también las opciones de línea de comandos de `in.dhcpd` que utiliza normalmente al ejecutar el daemon. Por ejemplo, si ejecuta el daemon como agente de reenvío BOOTP, incluya la opción `-r` en el comando `in.dhcpd -d -v`.

Cuando se ejecuta en modo de depuración, el daemon muestra mensajes en pantalla mientras procesa las solicitudes de DHCP o BOOTP. Consulte [“Salida del servidor DHCP en modo de depuración” en la página 463](#) para obtener información sobre la depuración del servidor.

▼ **Cómo utilizar snoop para supervisar el tráfico DHCP en la red**

- 1 **Asígnese los privilegios de superusuario en el sistema del servidor DHCP.**

- 2 **Inicie snoop para empezar a rastrear el tráfico de red que pasa por la interfaz de red del servidor.**

```
# /usr/sbin/snoop -d interface -o snoop-output-filename udp port 67 or udp port 68
```

Por ejemplo, escriba el comando siguiente:

```
# /usr/sbin/snoop -d hme0 -o /tmp/snoop.output udp port 67 or udp port 68
```

snoop sigue supervisando la interfaz hasta que detenga snoop pulsando Control-C cuando ya tenga la información que necesita.

- 3 **Inicie el sistema cliente o reinicie dhcpageant en él.**

En [“Cómo ejecutar el cliente DHCP en modo de depuración” en la página 460](#) se indica cómo reiniciar dhcpageant.

- 4 **En el sistema servidor, utilice snoop para mostrar el archivo de salida con el contenido de los paquetes de red:**

```
# /usr/sbin/snoop -i snoop-output-filename -x0 -v
```

Por ejemplo, escriba el comando siguiente:

```
# /usr/sbin/snoop -i /tmp/snoop.output -x0 -v
```

Véase también Consulte “[Salida de snoop en DHCP](#)” en la página 466 para obtener información de interpretación de la salida.

Salida del cliente DHCP en modo de depuración

En el ejemplo siguiente se muestra una salida normal cuando un cliente DHCP en modo de depuración envía su solicitud DHCP y recibe su información de configuración de un servidor DHCP.

EJEMPLO 17-1 Salida normal del cliente DHCP en modo de depuración

```
/sbin/dhcppagent: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhcppagent: debug: init_ifs: init interface hme0
/sbin/dhcppagent: debug: insert_ifs: hme0: sdumax 1500, optmax 1260, hwtype 1, hwlen 6
/sbin/dhcppagent: debug: insert_ifs: inserted interface hme0
/sbin/dhcppagent: debug: register_acknak: registered acknak id 5
/sbin/dhcppagent: debug: unregister_acknak: unregistered acknak id 5
/sbin/dhcppagent: debug: set_packet_filter: set filter 0x26018 (ARP reply filter)
/sbin/dhcppagent: info: setting IP netmask on hme0 to 255.255.192.0
/sbin/dhcppagent: info: setting IP address on hme0 to 10.23.3.233
/sbin/dhcppagent: info: setting broadcast address on hme0 to 10.23.63.255
/sbin/dhcppagent: info: added default router 10.23.0.1 on hme0
/sbin/dhcppagent: debug: set_packet_filter: set filter 0x28054 (blackhole filter)
/sbin/dhcppagent: debug: configure_if: bound ifsp->if sock_ip_fd
/sbin/dhcppagent: info: hme0 acquired lease, expires Tue Aug 10 16:18:33 2006
/sbin/dhcppagent: info: hme0 begins renewal at Tue Aug 10 15:49:44 2006
/sbin/dhcppagent: info: hme0 begins rebinding at Tue Aug 10 16:11:03 2006
```

Si el cliente no puede acceder al servidor DHCP, es posible que la salida del modo de depuración sea similar a este ejemplo.

EJEMPLO 17-2 Salida del cliente DHCP en modo de depuración que indica que hay algún problema

```
/sbin/dhcppagent: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhcppagent: debug: init_ifs: init interface hme0
/sbin/dhcppagent: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhcppagent: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhcppagent: debug: select_best: no valid OFFER/BOOTP reply
```

Si se muestra este mensaje, la solicitud del cliente no ha llegado al servidor o el servidor no puede enviar una respuesta al cliente. Ejecute snoop en el servidor según se describe en “[Cómo utilizar snoop para supervisar el tráfico DHCP en la red](#)” en la página 461 para determinar si los paquetes del cliente han llegado al servidor.

Salida del servidor DHCP en modo de depuración

Una salida normal del servidor en modo de depuración contiene información de configuración del servidor y, a continuación, información acerca de cada una de las interfaces de red a medida que el daemon se inicia. Tras el inicio del daemon, la salida del modo de depuración contiene información acerca de las solicitudes procesadas por el daemon. El [Ejemplo 17-3](#) muestra la salida del modo de depuración de un servidor DHCP que se acaba de iniciar. El servidor amplía el permiso para un cliente que utiliza una dirección propiedad de otro servidor DHCP que no responde.

EJEMPLO 17-3 Salida normal de un servidor DHCP en modo de depuración

```

Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
Run mode is: DHCP Server Mode.
Datastore: nisplus
Path: org_dir.dhcp.test...dhcp.test...$
DHCP offer TTL: 10
Ethers compatibility enabled.
BOOTP compatibility enabled.
ICMP validation timeout: 1000 milliseconds, Attempts: 2.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.21.255.255
Netmask: 255.255.0.0
Address: 10.21.0.2
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 10.22.255.255
Netmask: 255.255.0.0
Address: 10.22.0.1
Monitor (0007/qfe0) started...
Thread Id: 0007 - Monitoring Interface: qfe0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.23.63.255
Netmask: 255.255.192.0
Address: 10.23.0.1
Read 33 entries from DHCP macro database on Tue Aug 10 15:10:27 2006
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A maps to IP: 10.23.3.233
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
DHCP EXTEND 0934312543 0934316143 10.23.3.233 10.21.0.2
                0800201DBA3A SUNW.Ultra-5_10 0800201DBA3A

```

El [Ejemplo 17-4](#) muestra la salida del modo de depuración de un daemon DHCP que se inicia como agente de reenvío BOOTP. El agente reenvía solicitudes de un cliente a un servidor DHCP, y reenvía las respuestas del servidor al cliente.

EJEMPLO 17-4 Salida normal de agente de reenvío BOOTP en modo de depuración

```
Relay destination: 10.21.0.4 (blue-srvr2)      network: 10.21.0.0
Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
Run mode is: Relay Agent Mode.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.21.255.255
Netmask: 255.255.0.0
Address: 10.21.0.2
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 10.22.255.255
Netmask: 255.255.0.0
Address: 10.22.0.1
Monitor (0007/qfe0) started...
Thread Id: 0007 - Monitoring Interface: qfe0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.23.63.255
Netmask: 255.255.192.0
Address: 10.23.0.1
Relaying request 0800201DBA3A to 10.21.0.4, server port.
BOOTP RELAY-SRVR 0934297685 0000000000 0.0.0.0 10.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 10.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
BOOTP RELAY-CLNT 0934297688 0000000000 10.23.0.1 10.23.3.233 0800201DBA3A
N/A 0800201DBA3A
Relaying request 0800201DBA3A to 10.21.0.4, server port.
BOOTP RELAY-SRVR 0934297689 0000000000 0.0.0.0 10.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 10.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
```

Si hay algún problema con DHCP, la salida del modo de depuración puede contener advertencias o mensajes de error. Utilice la siguiente lista de mensajes de error del servidor DHCP para encontrar soluciones.

Respuesta de ICMP ECHO al candidato de OFFER: *dirección_ip* desactivando

Causa: Antes de que el servidor DHCP ofrezca una dirección IP a un cliente, el servidor envía un ping a la dirección para comprobar que no se está utilizando. Si algún cliente responde, la dirección se está utilizando.

Solución: Asegúrese de que las direcciones configuradas no se están utilizando. Puede utilizar para ello el comando ping. Consulte la página de comando [man ping\(1M\)](#) para obtener más información.

No hay más direcciones IP en la red *dirección_red*.

Causa: No hay direcciones IP disponibles en la tabla de red DHCP asociada con la red del cliente.

Solución: Cree más direcciones IP mediante DHCP Manager o el comando `pntadm`. Si el daemon de DHCP está supervisando varias subredes, compruebe que las direcciones adicionales son para la subred en la que se encuentra el cliente. Para más información consulte [“Cómo agregar direcciones IP al servicio DHCP” en la página 383](#).

No hay mas direcciones IP para la red *dirección_red* cuando se ejecuta el daemon de DHCP en modo de compatibilidad con BOOTP.

Causa: BOOTP no utiliza tiempos de permiso, de modo que el servidor DHCP busca direcciones libres con el indicador BOOTP activado para asignar a clientes BOOTP.

Solución: Utilice DHCP Manager para asignar direcciones BOOTP. Para más información consulte [“Clientes BOOTP con el servicio DHCP \(mapa de tareas\)” en la página 376](#).

Solicitud de acceso a base de datos por red inexistente: *nombre_base_datos* en almacén de datos: *almacén_datos*.

Causa: Durante la configuración del servidor DHCP no se ha creado una tabla de red DHCP para una subred.

Solución: Utilice DHCP Manager o el comando `pntadm` para crear la tabla de red DHCP y nuevas direcciones IP. Consulte [“Cómo agregar redes DHCP” en la página 369](#).

No existe la tabla de red DHCP *nombre_tabla* para la red del cliente DHCP.

Causa: Durante la configuración del servidor DHCP no se ha creado una tabla de red DHCP para una subred.

Solución: Utilice DHCP Manager o el comando `pntadm` para crear la tabla de red DHCP y nuevas direcciones IP. Consulte [“Cómo agregar redes DHCP” en la página 369](#).

El cliente utiliza una cookie de BOOTP no compatible con RFC1048.

Causa: Un dispositivo de la red está intentando acceder a una implementación incompatible de BOOTP.

Solución: Haga caso omiso de este mensaje a menos que tenga necesidad de configurar el dispositivo. Si quiere que el dispositivo sea compatible, consulte [“Clientes BOOTP con el servicio DHCP \(mapa de tareas\)” en la página 376](#) para más información.

Salida de snoop en DHCP

En la salida de snoop podrá ver los paquetes intercambiados entre el sistema cliente DHCP y el sistema servidor DHCP. La dirección IP de cada sistema está indicada en el paquete. También se incluyen las direcciones IP de los enrutadores o agentes de reenvío que se encuentran en la ruta del paquete. Si los sistemas no intercambian paquetes, es posible que el sistema cliente no pueda ponerse en contacto con el sistema servidor. El problema se encuentra en un nivel inferior.

Para evaluar la salida de snoop deberá saber cuál es el comportamiento esperado. Deberá saber, por ejemplo, si la solicitud debe pasar por un agente de reenvío BOOTP. También deberá saber las direcciones MAC e IP de los sistemas implicados para poder determinar si se trata de los valores esperados. Si hay más de una interfaz de red, deberá conocer también las direcciones de las interfaces de red.

En el ejemplo siguiente se muestra una salida normal de snoop para un mensaje de reconocimiento (ACK) de DHCP enviado desde el servidor en blue-srvr2 a un cliente cuya dirección MAC es 8:0:20:8e:f3:7e. En el mensaje, el servidor asigna al cliente la dirección IP 192.168.252.6 y el nombre de host white-6. El mensaje incluye también diversas opciones de red estándar y varias opciones de cliente específicas del proveedor.

EJEMPLO 17-5 Ejemplo de salida de snoop para un paquete

```
ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 26 arrived at 14:43:19.14
ETHER:  Packet size = 540 bytes
ETHER:  Destination = 8:0:20:8e:f3:7e, Sun
ETHER:  Source      = 8:0:20:1e:31:c1, Sun
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:  ----- IP Header -----
IP:
IP:  Version = 4
IP:  Header length = 20 bytes
IP:  Type of service = 0x00
IP:      xxx. .... = 0 (precedence)
IP:      ...0 .... = normal delay
IP:      .... 0... = normal throughput
IP:      .... .0.. = normal reliability
IP:  Total length = 526 bytes
IP:  Identification = 64667
IP:  Flags = 0x4 IP:      .1.. .... = do not fragment
IP:      ..0. .... = last fragment
IP:  Fragment offset = 0 bytes
IP:  Time to live = 254 seconds/hops
IP:  Protocol = 17 (UDP)
IP:  Header checksum = 157a
IP:  Source address = 10.21.0.4, blue-srvr2
IP:  Destination address = 192.168.252.6, white-6
IP:  No options
IP:  UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 67
UDP:  Destination port = 68 (BOOTPC)
```

EJEMPLO 17-5 Ejemplo de salida de snoop para un paquete (Continuación)

```

UDP: Length = 506
UDP: Checksum = 5D4C
UDP:
DHCP: ----- Dynamic Host Configuration Protocol -----
DHCP:
DHCP: Hardware address type (htype) = 1 (Ethernet (10Mb))
DHCP: Hardware address length (hlen) = 6 octets
DHCP: Relay agent hops = 0
DHCP: Transaction ID = 0x2e210f17
DHCP: Time since boot = 0 seconds
DHCP: Flags = 0x0000
DHCP: Client address (ciaddr) = 0.0.0.0
DHCP: Your client address (yiaddr) = 192.168.252.6
DHCP: Next server address (siaddr) = 10.21.0.2
DHCP: Relay agent address (giaddr) = 0.0.0.0
DHCP: Client hardware address (chaddr) = 08:00:20:11:E0:1B
DHCP:
DHCP: ----- (Options) field options -----
DHCP:
DHCP: Message type = DHCPACK
DHCP: DHCP Server Identifier = 10.21.0.4
DHCP: Subnet Mask = 255.255.255.0
DHCP: Router at = 192.168.252.1
DHCP: Broadcast Address = 192.168.252.255
DHCP: NISPLUS Domainname = dhcp.test
DHCP: IP Address Lease Time = 3600 seconds
DHCP: UTC Time Offset = -14400 seconds
DHCP: RFC868 Time Servers at = 10.21.0.4
DHCP: DNS Domain Name = sem.example.com
DHCP: DNS Servers at = 10.21.0.1
DHCP: Client Hostname = white-6
DHCP: Vendor-specific Options (166 total octets):
DHCP: (02) 04 octets 0x8194AE1B (unprintable)
DHCP: (03) 08 octets "pacific"
DHCP: (10) 04 octets 0x8194AE1B (unprintable)
DHCP: (11) 08 octets "pacific"
DHCP: (15) 05 octets "xterm"
DHCP: (04) 53 octets "/export/s2/base.s2s/latest/Solaris_8/Tools/Boot"
DHCP: (12) 32 octets "/export/s2/base.s2s/latest"
DHCP: (07) 27 octets "/platform/sun4u/kernel/unix"
DHCP: (08) 07 octets "EST5EDT"
    0: 0800 208e f37e 0800 201e 31c1 0800 4500 .. .ó~.. .1...E.
   16: 020e fc9b 4000 fe11 157a ac15 0004 c0a8 ....@....z.....
   32: fc06 0043 0044 01fa 5d4c 0201 0600 2e21 ...C.D..]L.....!
   48: 0f17 0000 0000 0000 0000 c0a8 fc06 ac15 .....
   64: 0002 0000 0000 0800 2011 e01b 0000 0000 .....
   80: 0000 0000 0000 0000 0000 0000 0000 0000 .....
   96: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  112: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  128: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  144: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  160: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  176: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  192: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  208: 0000 0000 0000 0000 0000 0000 0000 0000 .....
  224: 0000 0000 0000 0000 0000 0000 0000 0000 .....

```

EJEMPLO 17-5 Ejemplo de salida de snoop para un paquete (Continuación)

```
240: 0000 0000 0000 0000 0000 0000 0000 0000 .....
256: 0000 0000 0000 0000 0000 0000 0000 0000 .....
272: 0000 0000 0000 6382 5363 3501 0536 04ac .....c.Sc5..6..
288: 1500 0401 04ff ffff 0003 04c0 a8fc 011c .....
304: 04c0 a8fc ff40 0964 6863 702e 7465 7374 .....@.dhcp.test
320: 3304 0000 0e10 0204 ffff c7c0 0404 ac15 3.....
336: 0004 0f10 736e 742e 6561 7374 2e73 756e ....sem.example.
352: 2e63 6f6d 0604 ac15 0001 0c07 7768 6974 com.....whit
368: 652d 362b a602 0481 94ae 1b03 0861 746c e-6+.....pac
384: 616e 7469 630a 0481 94ae 1b0b 0861 746c ific.....pac
400: 616e 7469 630f 0578 7465 726d 0435 2f65 ific...xterm.5/e
416: 7870 6f72 742f 7332 382f 6261 7365 2e73 xport/sx2/bcvf.s
432: 3238 735f 776f 732f 6c61 7465 7374 2f53 2xs_btf/latest/S
448: 6f6c 6172 6973 5f38 2f54 6f6f 6c73 2f42 olaris_x/Tools/B
464: 6f6f 740c 202f 6578 706f 7274 2f73 3238 oot. /export/s2x
480: 2f62 6173 652e 7332 3873 5f77 6f73 2f6c /bcvf.s2xs_btf/l
496: 6174 6573 7407 1b2f 706c 6174 666f 726d atest../platform
512: 2f73 756e 346d 2f6b 6572 6e65 6c2f 756e /sun4u/kernel/un
528: 6978 0807 4553 5435 4544 54ff ix..EST5EDT.
```

Problemas por información de configuración DHCP incorrecta

Si un cliente DHCP recibe información de configuración de red incorrecta, examine los datos del servidor DHCP. Deberá examinar los valores de las opciones en las macros que el servidor DHCP procesa para este cliente. Información incorrecta puede ser, por ejemplo, un nombre de dominio NIS o una dirección IP de enrutador erróneos.

Utilice las siguientes pautas generales para determinar el origen de la información incorrecta:

- Examine las macros definidas en el servidor tal como se describe en “[Cómo visualizar las macros definidas en un servidor DHCP \(Administrador de DHCP\)](#)” en la página 397. Revise la información en “[Orden del procesamiento de macros](#)” en la página 315 y determine qué macros se procesan automáticamente para este cliente.
- Examine la tabla de red para determinar si se asigna alguna macro a la dirección IP del cliente como macro de configuración y, en su caso, cuál es. Para más información consulte “[Uso de direcciones IP en el servicio DHCP \(mapa de tareas\)](#)” en la página 379.
- Anote las opciones que aparecen en más de una macro. Asegúrese de que el valor deseado para una opción se configura en la última macro procesada.
- Edite la macro o macros necesarias para garantizar que se pasa el valor correcto al cliente. Consulte “[Modificación de macros DHCP](#)” en la página 398.

Problemas con el nombre de host proporcionado por el cliente DHCP

En esta sección se describen los posibles problemas con clientes DHCP que proporcionan sus propios nombres de host para registrarse con DNS.

El cliente DHCP no solicita un nombre de host

Si su cliente no es un cliente DHCP, consulte la documentación para determinar la forma de configurar el cliente para que solicite un nombre de host. Para los clientes DHCP, consulte [“Cómo habilitar un cliente DHCPv4 para que solicite un nombre de host específico” en la página 443](#).

El cliente DHCP no obtiene el nombre de host solicitado

En la lista siguiente se describen los problemas que puede experimentar un cliente para obtener el nombre de host solicitado, y las soluciones que se sugieren.

Problema: El cliente ha aceptado una oferta de un servidor DHCP que no emite actualizaciones de DNS.

Solución: Si el cliente tiene disponibles dos servidores DHCP, ambos se deben configurar para proporcionar actualizaciones de DNS. Consulte [“Habilitación de las actualizaciones DNS dinámicas por parte del servidor DHCP” en la página 360](#) para obtener información sobre la configuración del servidor DHCP y del servidor DNS.

Para determinar si el servidor DHCP está configurado para proporcionar actualizaciones de DNS:

1. Determine la dirección IP del servidor DHCP del cliente. En el sistema cliente, utilice snoop u otra aplicación para capturar paquetes de red. Consulte [“Cómo utilizar snoop para supervisar el tráfico DHCP en la red” en la página 461](#) y efectúe el procedimiento en el cliente en lugar de hacerlo en el servidor. En la salida de snoop, busque el identificador del servidor DHCP para obtener la dirección IP del servidor.
2. Inicie sesión en el sistema servidor DHCP para comprobar que esté configurado para efectuar actualizaciones de DNS. Escriba el siguiente comando como superusuario:

dhcpconfig -P

Si aparece UPDATE_TIMEOUT como parámetro de servidor, el servidor DHCP está configurado para efectuar actualizaciones de DNS.

3. En el servidor DNS, examine el archivo /etc/named.conf. Busque la palabra clave allow-update en la sección zone del dominio apropiado. Si el servidor permite que el servidor DHCP efectúe actualizaciones de DNS, la dirección IP del servidor DHCP aparecerá en la palabra clave allow-update.

Problema: El cliente utiliza la opción FQDN para especificar el nombre de host. DHCP no es actualmente compatible con la opción FQDN porque no es una opción oficial del protocolo DHCP.

Solución: En el servidor, utilice snoop u otra aplicación para capturar paquetes de red. Consulte [“Cómo utilizar snoop para supervisar el tráfico DHCP en la red” en la página 461](#) En la salida de snoop, busque la opción FQDN en un paquete del cliente.

Configure el cliente para que especifique el nombre de host con la opción Hostname. Hostname tiene el código de opción 12. Consulte la documentación de cliente para obtener instrucciones.

Para un cliente Oracle Solaris, consulte [“Cómo habilitar un cliente DHCPv4 para que solicite un nombre de host específico” en la página 443](#).

Problema: El servidor DHCP que efectúa una oferta de dirección al cliente no conoce el dominio DNS de este.

Solución: En el servidor DHCP, busque la opción DNSdomain con un valor válido. Configure la opción DNSdomain con el dominio DNS correcto en una macro procesada para este cliente. DNSdomain suele estar incluida en la macro de red. Consulte [“Modificación de macros DHCP” en la página 398](#) para obtener información sobre cómo cambiar los valores de las opciones de una macro.

Problema: El nombre de host solicitado por el cliente corresponde a una dirección IP no gestionada por el servidor DHCP. El servidor DHCP no efectúa actualizaciones de DNS para direcciones IP que no gestiona.

Solución: Examine syslog y busque uno de los siguientes mensajes del servidor DHCP:

- There is no *n.n.n.n* dhcp-network table for DHCP client's network.
- DHCP network record for *n.n.n.n* is unavailable, ignoring request.

Configure el cliente para que solicite un nombre distinto. Consulte [“Cómo habilitar un cliente DHCPv4 para que solicite un nombre de host específico” en la página 443](#). Elija un nombre asignado a una de las direcciones gestionadas por el servidor DHCP. Puede acceder a las asignaciones de direcciones en la ficha Direcciones de DHCP Manager. También puede elegir una dirección que no esté asignada a ninguna dirección IP.

Problema: El nombre de host solicitado por el cliente corresponde a una dirección IP no disponible actualmente. Es posible que la dirección se esté utilizando, se haya asignado a otro cliente o se haya ofrecido a otro cliente.

Solución: Examine syslog y busque el siguiente mensaje del servidor DHCP: ICMP ECHO reply to OFFER candidate: *n.n.n.n*.

Configure el cliente para que elija un nombre que corresponda a una dirección IP distinta. También puede recuperar la dirección del cliente que la está utilizando.

Problema: El servidor DNS no está configurado para aceptar actualizaciones del servidor DHCP.

Solución: Examine el archivo `/etc/named.conf` del servidor DNS. Busque la dirección IP del servidor DHCP con la palabra clave `allow-update` en la sección `zone` apropiada del dominio del servidor DHCP. Si no encuentra la dirección IP, el servidor DNS no está configurado para aceptar actualizaciones del servidor DHCP.

Consulte [“Cómo activar la actualización de DNS dinámica para los clientes DHCP” en la página 361](#) para obtener información sobre la configuración del servidor DNS.

Si el servidor DHCP tiene varias interfaces, quizá deba configurar el servidor DNS para que acepte actualizaciones de todas las direcciones del servidor DHCP. Active el modo de depuración en el servidor DNS para ver si le están llegando las actualizaciones. Si el servidor DNS ha recibido solicitudes de actualización, examine la salida del modo de depuración para determinar por qué no se han producido las actualizaciones. Consulte la página de comando `man in.named.1M` para obtener información sobre el modo de depuración de DNS.

Problema: Es posible que las actualizaciones de DNS no se hayan completado en el tiempo asignado. Los servidores DHCP no devuelven nombres de host a los clientes si las actualizaciones de DNS no se han completado antes del límite de tiempo configurado. Sin embargo, los intentos de completar las actualizaciones de DNS no se interrumpen.

Solución: Utilice el comando `nslookup` para determinar si las actualizaciones se han completado satisfactoriamente. Consulte la página de comando `man nslookup(1M)`.

Por ejemplo, supongamos que el dominio DNS es `hills.example.org` y la dirección IP del servidor DNS es `10.76.178.11`. El nombre de host que el cliente desea registrar es `cathedral`. Puede utilizar el comando siguiente para determinar si `cathedral` se ha registrado con ese servidor DNS:

```
nslookup cathedral.hills.example.org 10.76.178.11
```

Si las actualizaciones se han efectuado satisfactoriamente, pero no en el tiempo asignado, deberá aumentar el tiempo. Consulte [“Cómo activar la actualización de DNS dinámica para los clientes DHCP” en la página 361](#). En este procedimiento deberá aumentar el número de segundos durante los que se debe esperar una respuesta del servidor DNS antes de que se agote el tiempo.

Comandos y archivos DHCP (referencia)

En este capítulo se explican las relaciones entre los comandos DHCP y los archivos DHCP. En él no se explica el uso de los comandos.

El capítulo contiene la información siguiente:

- “Comandos DHCP” en la página 473
- “Archivos que utiliza el servicio DHCP” en la página 480
- “Información de opciones DHCP” en la página 482

Comandos DHCP

En la tabla siguiente se enumeran los comandos que se pueden utilizar para gestionar DHCP en la red.

TABLA 18–1 Comandos utilizados en DHCP

Orden	Descripción	Página de comando man
dhtadm	Se emplea para efectuar cambios en las opciones y macros de dhcptab. Este comando resulta útil en secuencias creadas para automatizar los cambios en la información DHCP. Utilice dhtadm con la opción -P y redirija la salida al comando grep para buscar de forma rápida valores específicos de opciones en la tabla dhcptab.	dhtadm(1M)
pntadm	Se utiliza para efectuar cambios en las tablas de red DHCP que asignan ID de cliente a direcciones IP y, de forma opcional, asocian información de configuración con direcciones IP.	pntadm(1M)
dhcpcfig	Se usa para configurar y desconfigurar servidores DHCP y agentes de reenvío BOOTP. También se utiliza para convertir a un formato de almacén de datos distinto y para importar y exportar datos de configuración DHCP.	dhcpcfig(1M)

TABLA 18-1 Comandos utilizados en DHCP (Continuación)

Orden	Descripción	Página de comando man
in.dhcpd	Daemon del servidor DHCP. El daemon se inicia al iniciarse el sistema. No es conveniente iniciar el daemon del servidor directamente. Utilice DHCP Manager, el comando svcadm o dhcpconfig para iniciar y detener el daemon. El daemon solo se debe llamar directamente para ejecutar el servidor en modo de depuración y para resolver problemas.	in.dhcpd(1M)
dhcpgmr	El Administrador de DHCP, una interfaz gráfica de usuario (GUI), se utiliza para la configuración y gestión del servicio DHCP. El Administrador de DHCP es la herramienta de administración recomendada para DHCP.	dhcpgmr(1M)
ifconfig	Se utiliza en el inicio del sistema para asignar direcciones IP a interfaces de red, configurar parámetros de red o ambas funciones. En un cliente DHCP, ifconfig inicia DHCP para obtener los parámetros (incluida la dirección IP) necesarios para configurar una interfaz de red.	ifconfig(1M)
dhcpcinfo	Lo utilizan las secuencias de inicio de los sistemas cliente de Oracle Solaris para obtener información (como el nombre de host) para el daemon del cliente DHCP, dhcpcagent. También se puede utilizar dhcpcinfo en secuencias o en la línea de comandos para obtener valores de parámetros específicos.	dhcpcinfo(1)
snoop	Se utiliza para capturar y mostrar el contenido de paquetes que circulan por la red. snoop resulta útil para resolver problemas del servicio DHCP.	snoop(1M)
dhcpcagent	El daemon del cliente DHCP, que implementa el extremo cliente del protocolo DHCP.	dhcpcagent(1M)

Ejecución de comandos DHCP en secuencias

Los comandos `dhcpconfig`, `dhtadm` y `pntadm` están optimizados para su uso en secuencias. En particular, el comando `pntadm` es útil para crear una gran cantidad de entradas de dirección IP en una tabla de red DHCP. En la siguiente secuencia de ejemplo se utiliza `pntadm` en modo de proceso por lotes para crear direcciones IP.

EJEMPLO 18-1 Secuencia `addclient.ksh` con el comando `pntadm`

```
#!/usr/bin/ksh
#
# This script utilizes the pntadm batch facility to add client entries
# to a DHCP network table. It assumes that the user has the rights to
# run pntadm to add entries to DHCP network tables.
#
# Based on the nsswitch setting, query the netmasks table for a netmask.
# Accepts one argument, a dotted IP address.
#
get_netmask()
{
```

EJEMPLO 18-1 Secuencia addclient.ksh con el comando pntadm (Continuación)

```

MTMP='getent netmasks ${1} | awk '{ print $2 }'
if [ ! -z "${MTMP}" ]
then
    print - ${MTMP}
fi
}

#
# Based on the network specification, determine whether or not network is
# subnetted or supernetted.
# Given a dotted IP network number, convert it to the default class
# network.(used to detect subnetting). Requires one argument, the
# network number. (e.g. 10.0.0.0) Echoes the default network and default
# mask for success, null if error.
#
get_default_class()
{
    NN01=${1%.*}
    tmp=${1#*.}
    NN02=${tmp%.*}
    tmp=${tmp#*.}
    NN03=${tmp%.*}
    tmp=${tmp#*.}
    NN04=${tmp%.*}
    RETNET=""
    RETMASK=""

    typeset -i16 ONE=10#${1%.*}
    typeset -i10 X=$(( ${ONE}&16#f0 ))
    if [ ${X} -eq 224 ]
    then
        # Multicast
        typeset -i10 TMP=$(( ${ONE}&16#f0 ))
        RETNET="${TMP}.0.0.0"
        RETMASK="240.0.0.0"
    fi
    typeset -i10 X=$(( ${ONE}&16#80 ))
    if [ -z "${RETNET}" -a ${X} -eq 0 ]
    then
        # Class A
        RETNET="${NN01}.0.0.0"
        RETMASK="255.0.0.0"
    fi
    typeset -i10 X=$(( ${ONE}&16#c0 ))
    if [ -z "${RETNET}" -a ${X} -eq 128 ]
    then
        # Class B
        RETNET="${NN01}.${NN02}.0.0"
        RETMASK="255.255.0.0"
    fi
    typeset -i10 X=$(( ${ONE}&16#e0 ))
    if [ -z "${RETNET}" -a ${X} -eq 192 ]
    then
        # Class C
        RETNET="${NN01}.${NN02}.${NN03}.0"
        RETMASK="255.255.255.0"
    fi
}

```

EJEMPLO 18-1 Secuencia addclient.ksh con el comando pntadm (Continuación)

```

fi
print - ${RETNET} ${RETMASK}
unset NNO1 NNO2 NNO3 NNO4 RETNET RETMASK X ONE
}

#
# Given a dotted form of an IP address, convert it to its hex equivalent.
#
convert_dotted_to_hex()
{
    typeset -i10 one=${1%*.*}
    typeset -i16 one=${one}
    typeset -Z2 one=${one}
    tmp=${1#*.*}

    typeset -i10 two=${tmp%*.*}
    typeset -i16 two=${two}
    typeset -Z2 two=${two}
    tmp=${tmp#*.*}

    typeset -i10 three=${tmp%*.*}
    typeset -i16 three=${three}
    typeset -Z2 three=${three}
    tmp=${tmp#*.*}

    typeset -i10 four=${tmp%*.*}
    typeset -i16 four=${four}
    typeset -Z2 four=${four}

    hex='print - ${one}${two}${three}${four} | sed -e 's/#/0/g''
    print - 16#${hex}
    unset one two three four tmp
}

#
# Generate an IP address given the network address, mask, increment.
#
get_addr()
{
    typeset -i16 net='convert_dotted_to_hex ${1}'
    typeset -i16 mask='convert_dotted_to_hex ${2}'
    typeset -i16 incr=10#${3}

    # Maximum legal value - invert the mask, add to net.
    typeset -i16 mhosts=~${mask}
    typeset -i16 maxnet=${net}+${mhosts}

    # Add the incr value.
    let net=${net}+${incr}

    if [ ((${net} < ${maxnet})) -eq 1 ]
    then
        typeset -i16 a=${net}\&16#ff000000
        typeset -i10 a="{a}>>24"

        typeset -i16 b=${net}\&16#ff0000

```

EJEMPLO 18-1 Secuencia `addclient.ksh` con el comando `prntadm` (Continuación)

```

typeset -i10 b="${b}>>16"

typeset -i16 c=${net}\&16#ff00
typeset -i10 c="${c}>>8"

typeset -i10 d=${net}\&16#ff
print - "${a}.${b}.${c}.${d}"
fi
unset net mask incr mhosts maxnet a b c d
}

# Given a network address and client address, return the index.
client_index()
{
    typeset -i NNO1=${1%*. *}
    tmp=${1#*. *}
    typeset -i NNO2=${tmp%*. *}
    tmp=${tmp#*. *}
    typeset -i NNO3=${tmp%*. *}
    tmp=${tmp#*. *}
    typeset -i NNO4=${tmp%*. *}

    typeset -i16 NNF1
    let NNF1=${NNO1}
    typeset -i16 NNF2
    let NNF2=${NNO2}
    typeset -i16 NNF3
    let NNF3=${NNO3}
    typeset -i16 NNF4
    let NNF4=${NNO4}
    typeset +i16 NNF1
    typeset +i16 NNF2
    typeset +i16 NNF3
    typeset +i16 NNF4
    NNF1=${NNF1#16\#}
    NNF2=${NNF2#16\#}
    NNF3=${NNF3#16\#}
    NNF4=${NNF4#16\#}
    if [ ${#NNF1} -eq 1 ]
    then
        NNF1="0${NNF1}"
    fi
    if [ ${#NNF2} -eq 1 ]
    then
        NNF2="0${NNF2}"
    fi
    if [ ${#NNF3} -eq 1 ]
    then
        NNF3="0${NNF3}"
    fi
    if [ ${#NNF4} -eq 1 ]
    then
        NNF4="0${NNF4}"
    fi
    typeset -i16 NN
    let NN=16#${NNF1}${NNF2}${NNF3}${NNF4}

```

EJEMPLO 18-1 Secuencia addclient.ksh con el comando pntadm *(Continuación)*

```

unset NNF1 NNF2 NNF3 NNF4

typeset -i NNO1=${2%*. *}
tmp=${2#*. *}
typeset -i NNO2=${tmp%*. *}
tmp=${tmp#*. *}
typeset -i NNO3=${tmp%*. *}
tmp=${tmp#*. *}
typeset -i NNO4=${tmp%*. *}
typeset -i16 NNF1
let NNF1=${NNO1}
typeset -i16 NNF2
let NNF2=${NNO2}
typeset -i16 NNF3
let NNF3=${NNO3}
typeset -i16 NNF4
let NNF4=${NNO4}
typeset +i16 NNF1
typeset +i16 NNF2
typeset +i16 NNF3
typeset +i16 NNF4
NNF1=${NNF1#16\#}
NNF2=${NNF2#16\#}
NNF3=${NNF3#16\#}
NNF4=${NNF4#16\#}
if [ $#NNF1 -eq 1 ]
then
    NNF1="0${NNF1}"
fi
if [ $#NNF2 -eq 1 ]
then
    NNF2="0${NNF2}"
fi
if [ $#NNF3 -eq 1 ]
then
    NNF3="0${NNF3}"
fi
if [ $#NNF4 -eq 1 ]
then
    NNF4="0${NNF4}"
fi
typeset -i16 NC
let NC=16#${NNF1}${NNF2}${NNF3}${NNF4}
typeset -i10 ANS
let ANS=$((NC)-${NN})
print - $ANS
}

#
# Check usage.
#
if [ "$#" != 3 ]
then
    print "This script is used to add client entries to a DHCP network"
    print "table by utilizing the pntadm batch facility.\n"
    print "usage: $0 network start_ip entries\n"

```

EJEMPLO 18-1 Secuencia `addclient.ksh` con el comando `pntadm` (Continuación)

```

    print "where: network is the IP address of the network"
    print "        start_ip is the starting IP address \n"
    print "        entries is the number of the entries to add\n"
    print "example: $0 10.148.174.0 10.148.174.1 254\n"
    return
fi

#
# Use input arguments to set script variables.
#
NETWORK=$1
START_IP=$2
typeset -i STRTNUM=client_index ${NETWORK} ${START_IP}
let ENDNUM=${STRTNUM}+3
let ENTRYNUM=${STRTNUM}
BATCHFILE=/tmp/batchfile.$$
MACRO='uname -n'

#
# Check if mask in netmasks table. First try
# for network address as given, in case VLSM
# is in use.
#
NETMASK='get_netmask ${NETWORK}'
if [ -z "${NETMASK}" ]
then
    get_default_class ${NETWORK} | read DEFNET DEFMASK
    # use the default.
    if [ "${DEFNET}" != "${NETWORK}" ]
    then
        # likely subnetted/supernetted.
        print - "\n\n###\tWarning\t###\n"
        print - "Network ${NETWORK} is netmasked, but no entry was found \n
                in the 'netmasks' table; please update the 'netmasks' \n
                table in the appropriate nameservice before continuing. \n
                (See /etc/nsswitch.conf.) \n" >&2
        return 1
    else
        # use the default.
        NETMASK="${DEFMASK}"
    fi
fi

#
# Create a batch file.
#
print -n "Creating batch file "
while [ ${ENTRYNUM} -lt ${ENDNUM} ]
do
    if [ (($({ENTRYNUM}-${STRTNUM}))%50 -eq 0 )
    then
        print -n "."
    fi

    CLIENTIP='get_addr ${NETWORK} ${NETMASK} ${ENTRYNUM}'
    print "pntadm -A ${CLIENTIP} -m ${MACRO} ${NETWORK}" >> ${BATCHFILE}
done

```

EJEMPLO 18-1 Secuencia `addclient.ksh` con el comando `pntadm` (Continuación)

```

    let ENTRYNUM=${ENTRYNUM}+1
done
print " done.\n"

#
# Run pntadm in batch mode and redirect output to a temporary file.
# Progress can be monitored by using the output file.
#
print "Batch processing output redirected to ${BATCHFILE}"
print "Batch processing started."

pntadm -B ${BATCHFILE} -v > /tmp/batch.out 2 >&1

print "Batch processing completed."
```

Archivos que utiliza el servicio DHCP

En la tabla siguiente se enumeran los archivos asociados con DHCP.

TABLA 18-2 Archivos y tablas utilizados por los daemons y comandos DHCP

Nombre de archivo o tabla	Descripción	Página de comando man
dhcptab	Término genérico para la tabla que contiene la información o configuración de DHCP registrada en forma de opciones con valores asignados y luego agrupadas en forma de macros. El nombre de la tabla <code>dhcptab</code> y su ubicación los determinan el almacén de datos que se utiliza para la información DHCP.	dhcptab(4)
Tabla de red DHCP	Asigna direcciones IP a ID de cliente y opciones de configuración. Las tablas de red DHCP se nombran según la dirección IP de la red, como <code>10.21.32.0</code> . No hay ningún archivo llamado <code>dhcp_network</code> . El nombre y la ubicación de las tablas de red DHCP los determina el almacén de datos utilizado para la información de DHCP.	dhcp_network(4)
dhcpsvc.conf	Almacena opciones de inicio para el daemon DHCP e información para el almacén de datos. Este archivo no debe editarse de forma manual. Utilice el comando <code>dhcpconfig</code> para modificar las opciones de inicio.	dhcpsvc.conf(4)
nsswitch.conf	Especifica la ubicación de las bases de datos de servicios de nombres y el orden en que se debe buscar en los servidores de nombres diversos tipos de información. El archivo <code>nsswitch.conf</code> se lee para obtener información de configuración precisa al configurar un servidor DHCP. El archivo se encuentra en el directorio <code>/etc</code> .	nsswitch.conf(4)

TABLA 18-2 Archivos y tablas utilizados por los daemons y comandos DHCP (Continuación)

Nombre de archivo o tabla	Descripción	Página de comando man
<code>resolv.conf</code>	Contiene información que se emplea para resolver consultas de DNS. Durante la configuración del servidor DHCP se consulta este archivo para obtener información acerca del dominio DNS y del servidor DNS. El archivo se encuentra en el directorio <code>/etc</code> .	resolv.conf(4)
<code>dhcp.interfaz</code>	Indica que se debe utilizar DHCP en la interfaz de red del cliente especificada en el nombre de archivo <code>dhcp.interfaz</code> . Por ejemplo, la existencia de un archivo denominado <code>dhcp.qe0</code> indica que se debe utilizar DHCP en la interfaz <code>qe0</code> . El archivo <code>dhcp.interfaz</code> puede contener comandos que se pasan como opciones al comando <code>ifconfig</code> , que a su vez se utiliza para iniciar DHCP en el cliente. El archivo se encuentra en el directorio <code>/etc</code> de los sistemas cliente DHCP.	No hay página de comando man específica, consulte dhcp(5)
<code>interfaz.dhc</code>	Contiene los parámetros de configuración obtenidos de DHCP para la interfaz de red especificada. El cliente guarda la información de configuración actual en <code>/etc/dhcp/interfaz.dhc</code> cuando se termina el permiso de la dirección IP actual. Por ejemplo, si se usa DHCP en la interfaz <code>qe0</code> , <code>dhcagent</code> guarda la información de configuración en <code>/etc/dhcp/qe0.dhc</code> . La siguiente vez que se inicia DHCP en la interfaz, el cliente solicita utilizar la información guardada si el permiso no ha caducado. Si el servidor DHCP deniega la solicitud, el cliente inicia el proceso estándar de negociación de permiso DHCP.	No hay página de comando man específica, consulte dhcagent(1M)
<code>dhcagent</code>	Establece valores de parámetros para el daemon de cliente <code>dhcagent</code> . La ruta al archivo es <code>/etc/default/dhcagent</code> . Para más información acerca de los parámetros consulte el archivo <code>/etc/default/dhcagent</code> o la página de comando man dhcagent(1M) .	dhcagent(1M)

TABLA 18–2 Archivos y tablas utilizados por los daemons y comandos DHCP (Continuación)

Nombre de archivo o tabla	Descripción	Página de comando man
DHCP <code>inittab</code>	<p>Define diversos aspectos de códigos de opciones DHCP, como el tipo de datos, y asigna etiquetas mnemónicas. Para más información acerca de la sintaxis del archivo consulte la página de comando <code>man dhcp_inittab(4)</code>.</p> <p>En el cliente, la información del archivo <code>/etc/dhcp/inittab</code> la utiliza <code>dhcpcd</code> para proporcionar información más significativa a los lectores humanos de la información. En el sistema servidor DHCP, este archivo lo utiliza el daemon DHCP y las herramientas de gestión para obtener información de opciones DHCP.</p> <p>El archivo <code>/etc/dhcp/inittab</code> sustituye al archivo <code>/etc/dhcp/dhcptags</code> utilizado en versiones anteriores. En “Información de opciones DHCP” en la página 482 hallará más información acerca de esta sustitución.</p>	<code>dhcp_inittab(4)</code>

Información de opciones DHCP

Historicamente, la información de opciones DHCP se ha guardado en diversos lugares, como la tabla `dhcptab` del servidor, el archivo `dhcptags` del cliente y tablas internas de diversos programas. En la versión 8 de Solaris y posteriores, la información de opciones se ha consolidado en el archivo `/etc/dhcp/inittab`. Consulte la página de comando `man dhcp_inittab(4)` para obtener información detallada acerca del archivo.

El cliente DHCP utiliza el archivo `inittab` de DHCP para sustituir al archivo `dhcptags`. El cliente utiliza este archivo para obtener información acerca de los códigos de opciones recibidos en un paquete DHCP. Los programas `in.dhcpd`, `snoop` y `dhcpcmgr` del servidor DHCP utilizan también el archivo `inittab`.

Cómo determinar si su sitio se ve afectado

La mayor parte de los sitios que utilizan DHCP *no* se ven afectados por el cambio al archivo `/etc/dhcp/inittab`. Su sitio se verá afectado si cumple la totalidad de los criterios siguientes:

- Tiene previsto actualizarse desde una versión de Oracle Solaris más antigua que Solaris 8.
- Ha creado anteriormente nuevas opciones de DHCP.
- Ha modificado el archivo `/etc/dhcp/dhcptags` y desea conservar los cambios.

Al actualizarse, el registro de actualización le notifica que su archivo `dhcptags` se ha modificado y que deberá efectuar cambios en el archivo `inittab` de DHCP.

Diferencias entre los archivos `dhcptags` e `inittab`

El archivo `inittab` contiene más información que el archivo `dhcptags`. Además, `inittab` utiliza una sintaxis distinta.

A continuación se muestra un ejemplo de una entrada de `dhcptags`:

```
33 StaticRt - IPList Static_Routes
```

33 es el código numérico que se pasa en el paquete DHCP. `StaticRt` es el nombre de la opción. `IPList` indica que el tipo de datos de `StaticRt` debe ser una lista de direcciones IP. `Static_Routes` es un nombre más descriptivo.

El archivo `inittab` consta de registros de una línea en los que se describe cada opción. El formato es similar al que define los símbolos en `dhcptab`. En la tabla siguiente se describe la sintaxis del archivo `inittab`.

Opción	Descripción
<i>nombre_opción</i>	Nombre de la opción. El nombre de la opción debe ser único dentro de la categoría de la opción y no superponerse con los nombres de otras opciones en las categorías Standard, Site y Vendor. Por ejemplo, no puede haber dos opciones en Site que se llamen igual, y no se debe crear una opción de Site con el mismo nombre de una opción de Standard.
<i>categoría</i>	Identifica el espacio de nombres al que pertenece la opción. Debe ser uno de los siguientes: Standard, Site, Vendor, Field o Internal.
<i>código</i>	Identifica la opción cuando se envía a la red. En la mayor parte de casos, el código identifica la opción de forma unívoca, sin necesidad de categoría. Sin embargo, en el caso de las categorías internas como Field o Internal, un código se puede utilizar con otra finalidad. Es posible que el código no sea único a nivel global. El código debe ser único dentro de la categoría de la opción, y no superponerse con los códigos en los campos Standard y Site.
<i>type</i>	Describe los datos asociados con esta opción. Los tipos válidos son IP, ASCII, Octet, Boolean, Unnumber8, Unnumber16, Unnumber32, Unnumber64, Snumber8, Snumber16, Snumber32 y Snumber64. Para números, la inicial indica si el número tiene signo (S) o no (U). Los dígitos al final indican cuántos bits hay en el número. Por ejemplo, Unnumber8 es un número sin signo de 8 bits. El tipo no distingue mayúsculas de minúsculas.
<i>granularidad</i>	Describe cuántas unidades de datos componen un valor completo para esta opción.
<i>máximo</i>	Describe cuántos valores completos se permiten para esta opción. 0 indica un número infinito.

<i>consumidores</i>	Describe qué programas pueden utilizar esta información. Consumidores debe establecerse en <code>sdmi</code> , donde:
<code>s</code>	<code>snoop</code>
<code>d</code>	<code>in.dhcpd</code>
<code>m</code>	<code>dhcpgmr</code>
<code>i</code>	<code>dhcpinfo</code>

A continuación se muestra un ejemplo de entrada de `inittab`:

```
StaticRt - Standard, 33, IP, 2, 0, sdmi
```

En esta entrada se describe una opción denominada `StaticRt`. La opción está en la categoría estándar y el código de opción es el 33. Los datos previstos son probablemente una cantidad infinita de pares de direcciones porque el tipo es IP, la granularidad es 2 y el máximo es infinito (0). Los consumidores de esta opción son `sdmi: snoop, in.dhcpd, dhcpgmr` y `dhcpinfo`.

Conversión de entradas de `dhcptags` en entradas de `inittab`

Si ha agregado anteriormente entradas en su archivo `dhcptags`, deberá agregar las entradas correspondientes en el nuevo archivo `inittab` si quiere continuar usando en su sitio las opciones agregadas. En el ejemplo siguiente se muestra cómo expresar una entrada de ejemplo de `dhcptags` en el formato `inittab`.

Supongamos que se ha agregado la siguiente entrada de `dhcptags` para faxes conectados a la red:

```
128 FaxMchn - IP Fax_Machine
```

El código 128 significa que la opción debe estar en la categoría Site. El nombre de la opción es `FaxMchn`, y el tipo de datos es IP.

La entrada correspondiente de `inittab` podría ser:

```
FaxMchn SITE, 128, IP, 1, 1, sdmi
```

La granularidad de 1 y el máximo de 1 indican que en esta opción se espera una sola dirección IP.

P A R T E I V

Seguridad IP

Esta sección se centra en la seguridad de red. La arquitectura de seguridad IP (IPsec) protege la red en el nivel del paquete. El intercambio de claves de Internet (IKE) administra las claves para IPsec. El filtro IP proporciona un cortafuegos.

Arquitectura de seguridad IP (descripción general)

La arquitectura de seguridad IP (IPsec) ofrece protección criptográfica para los datagramas IP en paquetes de redes IPv4 e IPv6.

Este capítulo contiene la información siguiente:

- “Novedades de IPsec” en la página 487
- “Introducción a IPsec” en la página 489
- “Flujo de paquetes IPsec” en la página 491
- “Asociaciones de seguridad IPsec” en la página 494
- “Mecanismos de protección de IPsec” en la página 495
- “Directivas de protección IPsec” en la página 499
- “Modos de transporte y túnel en IPsec” en la página 499
- “Redes privadas virtuales e IPsec” en la página 502
- “Paso a través de IPsec y NAT” en la página 503
- “IPsec y SCTP” en la página 504
- “IPsec y Zonas de Solaris” en la página 504
- “IPsec y dominios lógicos” en la página 504
- “Archivos y utilidades IPsec” en la página 505
- “Cambios en IPsec para la versión Solaris 10” en la página 507

Para implementar IPsec en la red, consulte el [Capítulo 20, “Configuración de IPsec \(tareas\)”](#).

Para obtener información de referencia, consulte el [Capítulo 21, “Arquitectura de seguridad IP \(referencia\)”](#).

Novedades de IPsec

Solaris 10 4/09: a partir de esta versión, la utilidad de gestión de servicios (SMF) administra IPsec como conjunto de servicios.

Por defecto, hay dos servicios de IPsec habilitados en el inicio del sistema:

- `svc:/network/ipsec/policy:default`
- `svc:/network/ipsec/ipsecalgs:default`

Por defecto, los servicios de gestión de claves se deshabilitan en el inicio del sistema:

- `svc:/network/ipsec/manual-key:default`
- `svc:/network/ipsec/ike:default`

Para activar directivas IPsec en SMF, siga estos pasos:

1. Agregue entradas de directivas IPsec al archivo `ipsecinit.conf`.
2. Configure la Internet Key Exchange (IKE) o configure manualmente las claves.
3. Actualice el servicio de directivas IPsec.
4. Habilite el servicio de administración de teclas.

Para obtener más información sobre SMF, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)”](#) de *Guía de administración del sistema: administración básica*. Consulte también las páginas de comando `man smf(5)` y `svcadm(1M)`.

A partir de esta versión, los comandos `ipseconf` e `ipseckey` presentan la opción `-c` para comprobar la sintaxis de sus respectivos archivos de configuración. Asimismo, el perfil de derechos Network IPsec Management se proporciona para administrar IPsec e IKE.

Solaris 10 7/07: a partir de esta versión, IPsec implementa por completo los túneles en modo túnel y se modifican las utilidades que admiten túneles.

- IPsec implementa los túneles en modo túnel para las redes privadas virtuales (VPN). En modo túnel, IPsec admite múltiples clientes detrás de una sola NAT. En modo túnel, IPsec es interoperable con las implementaciones de túneles de IP en IP de otros proveedores. IPsec sigue admitiendo túneles en modo transporte, de modo que es compatible con las versiones anteriores de Oracle Solaris.
- La sintaxis para crear un túnel se simplifica. Para administrar la directiva IPsec, se ha ampliado el comando `ipseconf`. El comando `ifconfig` no se admite para la administración de la directiva IPsec.
- A partir de esta versión, se elimina el archivo `/etc/ipnodes`. Utilice el archivo `/etc/hosts` para configurar las direcciones IPv6 de red.

Solaris 10 1/06: a partir de esta versión, IKE es totalmente compatible con NAT-Traversal, como se describe en RFC 3947 y RFC 3948. Las operaciones IKE usan la biblioteca PKCS #11 de la estructura criptográfica, lo cual mejora el rendimiento.

La estructura criptográfica proporciona un almacén de claves softtoken para las aplicaciones que utilizan la metarranura. Cuando IKE utilice la metarranura, podrá guardar las claves en el disco, en una placa conectada o en el almacén de claves softtoken.

- Para utilizar el almacén de claves softtoken, consulte la página del comando `man cryptoadm(1M)`.

- Para ver una lista completa de las nuevas funciones de Solaris 10 y una descripción de las versiones de Solaris, consulte *Novedades de Oracle Solaris 10 8/11*.

Introducción a IPsec

IPsec protege los paquetes IP autenticándolos, cifrándolos o llevando a cabo ambas acciones. IPsec se lleva a cabo dentro del módulo IP, debajo de la capa de aplicación. Por tanto, una aplicación de Internet puede aprovechar IPsec aunque no esté configurada para el uso de IPsec. Cuando se utiliza correctamente, la directiva IPsec es una herramienta eficaz para proteger el tráfico de la red.

La protección IPsec implica cinco componentes principales:

- **Protocolos de seguridad:** Mecanismo de protección de datagramas IP. El **encabezado de autenticación** (AH) firma los paquetes IP y garantiza la integridad. El contenido del datagrama no está cifrado, pero el receptor tiene la seguridad de que el contenido del paquete no se ha modificado. El receptor también tiene la garantía de que los paquetes los ha enviado el remitente. La **Encapsulating Security Payload (ESP)** cifra los datos IP, con lo cual codifica el contenido durante la transmisión de paquetes. ESP también puede garantizar la integridad de los datos mediante una opción de algoritmo de autenticación.
- **Base de datos de asociaciones de seguridad (SADB):** La base de datos que asocia un protocolo de seguridad con una dirección de destino IP y un número de índice. El número de índice se denomina **índice de parámetros de seguridad**. Estos tres elementos (el protocolo de seguridad, la dirección de destino y el SPI) identifican de forma exclusiva a un paquete IPsec legítimo. La base de datos garantiza que el receptor reconozca un paquete protegido que llega a su destino. El receptor también utiliza información de la base de datos para descifrar la comunicación, verificar que los paquetes no se hayan modificado, volver a ensamblar los paquetes y entregarlos en su destino final.
- **Administración de claves:** La generación y distribución de claves para los algoritmos criptográficos y SPI.
- **Mecanismos de seguridad:** Los algoritmos de autenticación y cifrado que protegen los datos de los datagramas IP.
- **Base de datos de directivas de seguridad (SPD):** La base de datos que especifica el nivel de protección que se aplica a un paquete. SPD filtra el tráfico IP para determinar el modo en que se deben procesar los paquetes. Un paquete puede descartarse, transferirse sin codificar o protegerse con IPsec. Para los paquetes salientes, SPD y SADB determinan el nivel de protección que se aplicará. Para los paquetes entrantes, SPD permite determinar si el nivel de protección del paquete es aceptable. Si el paquete se protege con IPsec, SPD se consulta una vez descifrado y verificado el paquete.

IPsec aplica los mecanismos de seguridad a los datagramas IP que se transfieren a la dirección de destino IP. El receptor utiliza la información de SADB para comprobar que los paquetes que llegan sean legítimos y descifrarlos. Las aplicaciones pueden invocar IPsec para aplicar mecanismos de seguridad a los datagramas IP por socket también.

Los sockets tienen un comportamiento distinto según el puerto:

- Los SA por socket modifican su entrada de puerto correspondiente en SPD.
- Además, si el socket de un puerto está conectado y posteriormente se aplica la directiva IPsec a ese puerto, el tráfico que utiliza ese socket no está protegido mediante IPsec.

Naturalmente, un socket abierto en un puerto *después* de la aplicación de la directiva IPsec en el puerto está protegido con IPsec.

RFC IPsec

Internet Engineering Task Force (IETF) ha publicado una serie de solicitudes de comentarios (RFC) que describen la arquitectura de seguridad para la capa IP. Todas las RFC tienen copyright de la Sociedad de Internet. Encontrará un vínculo a las RFC en la página <http://www.ietf.org/>. La siguiente lista de RFC incluye referencias de seguridad IP generales:

- RFC 2411, "IP Security Document Roadmap", noviembre de 1998.
- RFC 2401, "Security Architecture for the Internet Protocol", noviembre de 1998.
- RFC 2402, "IP Authentication Header", noviembre de 1998.
- RFC 2406, "IP Encapsulating Security Payload (ESP)", noviembre de 1998.
- RFC 2408, "Internet Security Association and Key Management Protocol (ISAKMP)", noviembre de 1998.
- RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP", noviembre de 1998
- RFC 2409, "The Internet Key Exchange (IKE)", noviembre de 1998.
- RFC 3554, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec", julio de 2003 [sin implementar en la versión Solaris 10]

Terminología de IPsec

Las RFC IPsec definen una serie de términos útiles para determinar cuándo debe implementar IPsec en los sistemas. La tabla siguiente enumera los términos de IPsec, proporciona sus acrónimos habituales y aporta una definición. Para ver una lista de la terminología que se utiliza en la negociación de claves, consulte la [Tabla 22-1](#).

TABLA 19-1 Términos, acrónimos y usos de IPsec

Término de IPsec	Acrónimo	Definición
Asociación de seguridad	SA	Conexión exclusiva entre dos nodos de una red. La conexión se define mediante tres elementos: un protocolo de seguridad, un índice de parámetros de seguridad y un destino IP. El destino IP puede ser una dirección IP o un socket.
Base de datos de asociaciones de seguridad	SADB	Base de datos que contiene todas las asociaciones de seguridad activas.
Índice de parámetros de seguridad	SPI	El valor de índice para una asociación de seguridad. Un SPI es un valor de 32 bits que distingue entre las SA que tienen el mismo destino IP y protocolo de seguridad.
base de datos de directivas de seguridad	SPD	Base de datos que determina si los paquetes salientes y entrantes tienen el nivel de protección especificado.
Intercambio de claves		El proceso de generación de claves para los algoritmos criptográficos asimétricos. Los dos métodos principales son los protocolos RSA y el protocolo Diffie-Hellman.
Protocolo Diffie-Hellman	DH	Protocolo de intercambio de claves que implica la generación y la autenticación de claves. A menudo se denomina <i>intercambio de claves autenticadas</i> .
Protocolo RSA	RSA	Protocolo de intercambio de claves que implica la generación y la distribución de claves. El protocolo recibe el nombre de sus tres creadores, Rivest, Shamir y Adleman.
Protocolo de administración de claves y asociaciones de seguridad de Internet	ISAKMP	Estructura habitual para establecer el formato de los atributos SA, así como para negociar, modificar y eliminar SA. ISAKMP es el estándar IETF para administrar SA IPsec.

Flujo de paquetes IPsec

La [Figura 19-1](#) muestra cómo se comporta un paquete de direcciones IP, como parte de un **datagrama IP**, cuando se invoca IPsec en un paquete saliente. El diagrama de flujo muestra dónde se pueden aplicar en el paquete las entidades encabezado de autenticación (AH) y Carga de seguridad encapsuladora (ESP). En las secciones siguientes se describe cómo aplicar estas entidades, así como el modo de seleccionar los algoritmos.

La [Figura 19-2](#) muestra el proceso entrante de IPsec.

FIGURA 19-1 IPsec aplicado al proceso de paquetes salientes

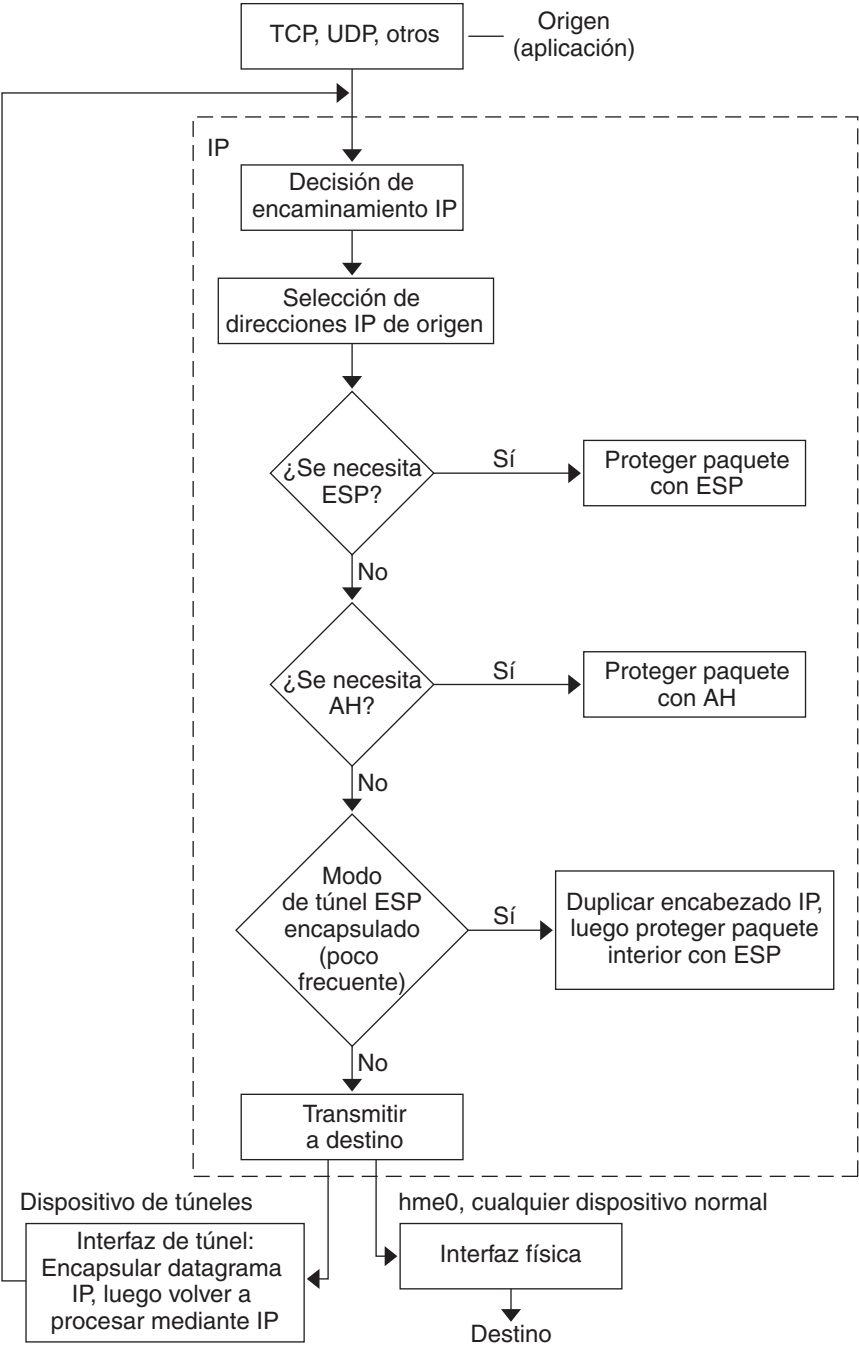
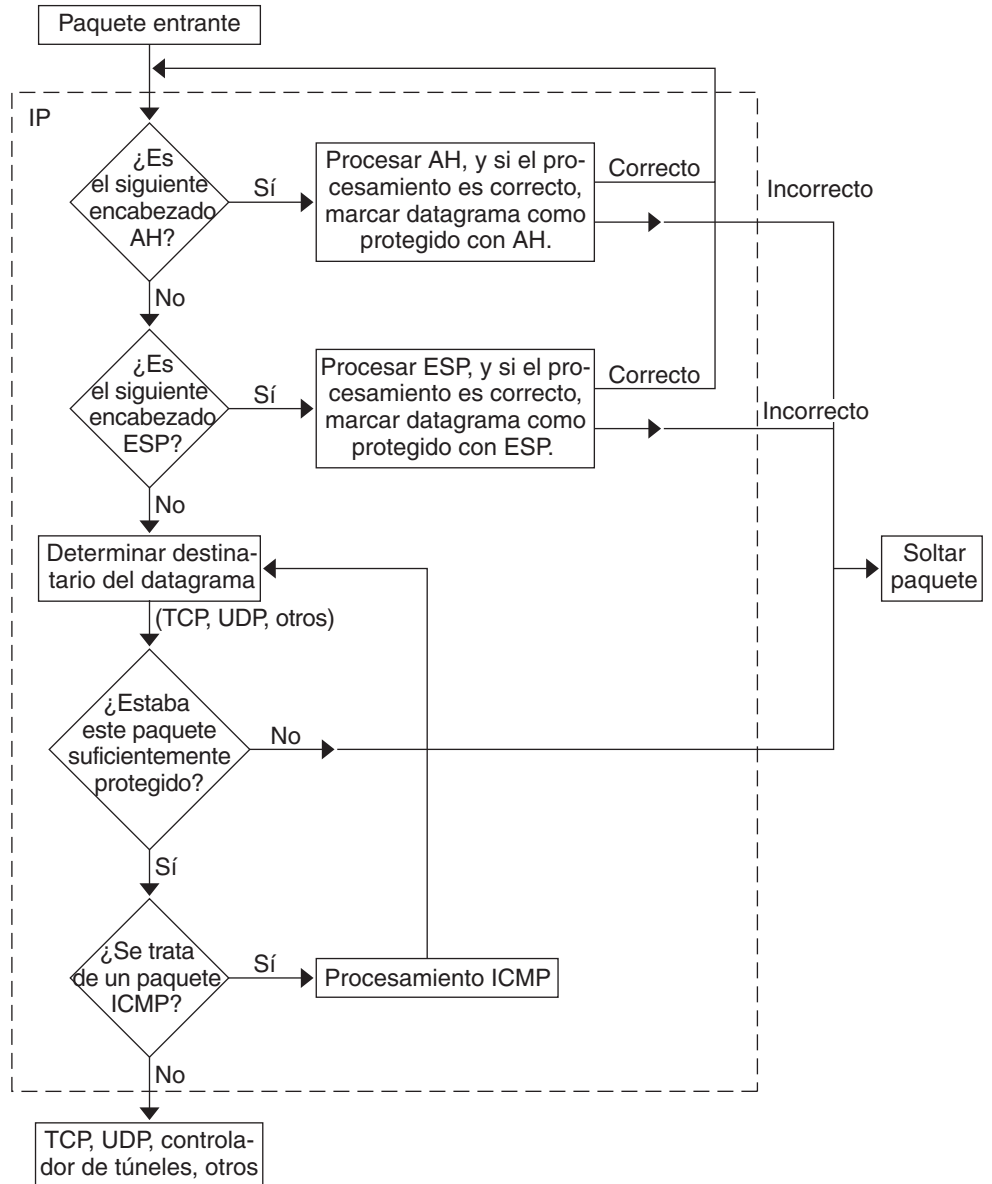


FIGURA 19-2 IPsec aplicado al proceso de paquetes entrantes



Asociaciones de seguridad IPsec

Una *asociación de seguridad* (SA) IPsec especifica las propiedades de seguridad que se reconocen mediante hosts comunicados. Una única SA protege los datos en una dirección. La protección es para un solo host o para una dirección de grupo (multidifusión). Dado que la mayoría de la comunicación es de igual a igual o de cliente-servidor, debe haber dos SA para proteger el tráfico en ambas direcciones.

Los tres elementos siguientes identifican una SA IPsec de modo exclusivo:

- El protocolo de seguridad (AH o ESP)
- La dirección IP de destino
- El [índice de parámetros de seguridad](#)

El SPI, un valor arbitrario de 32 bits, se transmite con un paquete AH o ESP. Las páginas del comando `man ipsec` [\(7P\)](#) y `ipsecesp` [\(7P\)](#) explican la protección que ofrecen AH y ESP. Se utiliza un valor de suma de comprobación de integridad para autenticar un paquete. Si la autenticación falla, se deja el paquete.

Las asociaciones de seguridad se almacenan en una *base de datos de asociaciones de seguridad* (SADB). Un motor de administración basado en sockets, la interfaz PF_KEY, permite a las aplicaciones privilegiadas administrar la base de datos. Por ejemplo, la aplicación IKE y el comando `ipseckey` usan la interfaz de socket PF_KEY.

- Para obtener una descripción completa de SADB IPsec, consulte “[Base de datos de asociaciones de seguridad para IPsec](#)” en la [página 571](#).
- Para obtener más información sobre cómo administrar SADB, consulte la [página del comando `pf_key`](#) [\(7P\)](#).

Administración de claves en IPsec

Las asociaciones de seguridad (SA) requieren materiales para la autenticación y para el cifrado. La administración de este *material de claves* se denomina *administración de claves*. El protocolo de intercambio de claves de Internet (IKE) gestiona automáticamente la administración de claves. También puede administrar las claves manualmente con el comando `ipseckey`.

Las SA de los paquetes IPv4 e IPv6 pueden utilizar cualquier método para administrar las claves. A menos que tenga una razón de peso para utilizar la administración de claves manual, se recomienda la administración automática. Por ejemplo, para interoperar con sistemas que no sean Solaris es posible que precise la administración de claves manual.

En la versión actual, SMF proporciona el siguiente servicio de administración de claves para IPsec:

- `svc:/network/ipsec/ike:default` **service** – es el servicio SMF para la administración automática de claves. El servicio `ike` ejecuta el daemon `in.iked` para proporcionar administración automática de claves. Para ver una descripción de IKE, consulte el [Capítulo 22, “Intercambio de claves de Internet \(descripción general\)”](#). Para obtener más información sobre el daemon `in.iked`, consulte la página de comando `man in.iked(1M)`. Para obtener información sobre el servicio `ike`, consulte [“Utilidad de gestión de servicios de IKE” en la página 629](#).
- `svc:/network/ipsec/manual-key:default` **service** – es el servicio SMF para la administración manual de claves. El servicio `manual-key` ejecuta el comando `ipseckey` con varias opciones para administrar claves manualmente. Para ver una descripción del comando `ipseckey`, consulte [“Utilidades para la generación de claves en IPsec” en la página 571](#). Para obtener más información sobre las opciones del comando `ipseckey`, consulte la página de comando `man ipseckey(1M)`.

En las versiones anteriores a Solaris 10 4/09 los comandos `in.iked` e `ipseckey` administran material de claves.

- El daemon `in.iked` proporciona administración de claves automática. Para ver una descripción de IKE, consulte el [Capítulo 22, “Intercambio de claves de Internet \(descripción general\)”](#). Para obtener más información sobre el daemon `in.iked`, consulte la página de comando `man in.iked(1M)`.
- El comando `ipseckey` proporciona administración de claves manual. Para ver una descripción del comando, consulte [“Utilidades para la generación de claves en IPsec” en la página 571](#). Para obtener más información sobre las opciones del comando `ipseckey`, consulte la página de comando `man ipseckey(1M)`.

Mecanismos de protección de IPsec

IPsec proporciona dos protocolos de seguridad para proteger los datos:

- Encabezado de autenticación (AH)
- Carga de seguridad encapsuladora (ESP)

Un AH protege los datos con un algoritmo de autenticación. Una ESP protege los datos con un algoritmo de cifrado. De modo opcional, una ESP protege los datos con un algoritmo de autenticación. Cada implementación de un algoritmo se denomina *mecanismo*.

Encabezado de autenticación

El **encabezado de autenticación** proporciona autenticación de datos, una integridad sólida y protección de repetición para los datagramas IP. AH protege la mayor parte del datagrama IP. Como muestra la ilustración siguiente, AH se inserta entre el encabezado IP y el encabezado de transporte.

IP Hdr	AH	TCP Hdr	
--------	----	---------	--

El encabezado de transporte puede ser TCP, UDP, SCTP o ICMP. Si se utiliza un **túnel**, el encabezado de transporte puede ser otro encabezado de IP.

Carga de seguridad encapsuladora

El módulo **Encapsulating Security Payload (ESP)** ofrece confidencialidad para los elementos que encapsula ESP. ESP también proporciona los servicios que proporciona AH. Sin embargo, ESP sólo proporciona sus protecciones de la parte del datagrama que encapsula ESP. ESP proporciona servicios de autenticación opcional para asegurar la integridad de los paquetes protegidos. Debido a que ESP utiliza tecnología de habilitación de cifrado, un sistema que proporcione ESP puede estar sujeto a leyes de control de importación y exportación.

ESP encapsula sus datos, de modo que ESP sólo protege los datos que siguen a su inicio en el datagrama, como se muestra en la ilustración siguiente.

IP Hdr	ESP	TCP Hdr	
--------	-----	---------	--

 Cifrado

En un paquete TCP, ESP encapsula únicamente el encabezado TCP y sus datos. Si el paquete se encuentra en un datagrama de IP en IP, ESP protege el datagrama IP interior. La directiva por socket permite la **autoencapsulación**, de modo que ESP puede encapsular las opciones de IP cuando lo necesita.

Si está activada la autoencapsulación, se realiza una copia del encabezado IP para construir un datagrama de IP en IP. Por ejemplo, cuando la autoencapsulación no está activada en un socket TCP, el datagrama se envía con el siguiente formato:

[IP(a -> b) *options* + TCP + data]

Cuando la autoencapsulación está activa en ese socket TCP, el datagrama se envía con el siguiente formato:

```
[ IP(a -> b) + ESP [ IP(a -> b) options + TCP + data ] ]
```

Para más información, consulte “Modos de transporte y túnel en IPsec” en la página 499.

Consideraciones de seguridad para el uso de AH y ESP

La tabla siguiente compara las protecciones que proporcionan AH y ESP.

TABLA 19-2 Protecciones que proporcionan AH y ESP en IPsec

Protocolo	Protección de paquetes	Protección	Contra ataques
AH	Protege el paquete del encabezado IP al encabezado de transporte.	Proporciona integridad sólida, autenticación de datos: <ul style="list-style-type: none">■ Garantiza que el receptor recibe exactamente lo que ha enviado el remitente.■ Es susceptible a los ataques de repetición cuando AH no activa la protección contra repeticiones.	Repetición, cortar y pegar
ESP.	Protege el paquete que sigue a ESP en el datagrama.	Con la opción de cifrado, cifra el datagrama IP. Garantiza la confidencialidad. Con la opción de autenticación, proporciona la misma protección que AH. Con ambas opciones, proporciona integridad sólida, autenticación de datos y confidencialidad.	Intercepción de comunicaciones Repetición, cortar y pegar Repetición, cortar y pegar e intercepción de comunicaciones.

Algoritmos de autenticación y cifrado en IPsec

Los protocolos de seguridad IPsec utilizan dos tipos de algoritmos: de autenticación y de cifrado. El módulo AH utiliza algoritmos de autenticación. El módulo ESP puede utilizar tanto algoritmos de cifrado como de autenticación. Puede obtener una lista de los algoritmos de su sistema y sus propiedades con el comando `ipsecalgs`. Para mas información, consulte la página del comando `man ipsecalgs(1M)` También puede utilizar las funciones que se describen en la página del comando `man getipsecalgbyname(3NSL)` para recuperar las propiedades de los algoritmos.

IPsec en un sistema Solaris utiliza la estructura criptográfica de Solaris para acceder a los algoritmos. La estructura proporciona un depósito central para los algoritmos, además de otros servicios. La estructura permite a IPsec aprovechar los aceleradores de hardware criptográficos de alto rendimiento. La estructura también proporciona funciones de control de recursos. Por ejemplo, la estructura permite limitar la cantidad de tiempo de CPU que se dedica a las operaciones criptográficas en el núcleo.

Para obtener más información, consulte lo siguiente:

- Capítulo 13, “Estructura criptográfica de Oracle Solaris (descripción general)” de *Guía de administración del sistema: servicios de seguridad*
- Capítulo 8, “Introduction to the Oracle Solaris Cryptographic Framework” de *Developer’s Guide to Oracle Solaris Security*

Algoritmos de autenticación en IPsec

Los algoritmos de autenticación producen un valor de suma de comprobación de integridad o *síntesis* que se basa en los datos y una clave. El módulo AH utiliza algoritmos de autenticación. El módulo ESP también puede utilizar algoritmos de autenticación.

Algoritmos de cifrado en IPsec

Los algoritmos de cifrado cifran los datos con una clave. El módulo ESP de IPsec utiliza algoritmos de cifrado. Los algoritmos operan en los datos en unidades del *tamaño de un bloque*.

Diferentes versiones del sistema operativo Solaris 10 proporcionan algoritmos de cifrado predeterminados distintos.



Precaución – A partir de la versión Solaris 10 7/07, no añada Solaris Encryption Kit al sistema. El kit reduce el nivel de revisión para cifrado del sistema. El kit es incompatible con el cifrado del sistema.

- A partir de la versión Solaris 10 7/07, el contenido de Solaris Encryption Kit se instala mediante el disco de instalación de Solaris. En esta versión se añaden los algoritmos de autenticación SHA2: sha256, sha384 y sha512. Las implementaciones SHA2 cumplen la especificación RFC 4868. Esta versión también agrega grupos Diffie-Hellman más grandes: 2048 bits (grupo 14), 3072 bits (grupo 15) y 4096 bits (grupo 16). Tenga en cuenta que los sistemas de Sun con tecnología CoolThreads sólo aceleran los grupos de 2048 bits.
- Antes de la versión Solaris 10 7/07, el disco de instalación de Solaris proporciona algoritmos básicos, además puede añadir algoritmos más complejos desde Solaris Encryption Kit. De modo predeterminado, están instalados los algoritmos DES-CBC, 3DES-CBC, AES-CBC, y Blowfish-CBC. Los tamaños de claves que admiten los algoritmos AES-CBC y Blowfish-CBC están limitados a 128 bits.

Los algoritmos AES-CBC y Blowfish-CBC que admiten tamaños de claves de más de 128 bits están disponibles para IPsec cuando se instala el Solaris Encryption Kit. Sin embargo, no todos los algoritmos de cifrado están disponibles fuera de Estados Unidos. El kit está disponible en un CD independiente que *no* forma parte del paquete de instalación de Solaris 10. En la *Solaris 10 Encryption Kit Installation Guide* se describe cómo instalar el kit. Para obtener más información, visite el [sitio web de descargas de Sun \(http://www.oracle.com/\)](http://www.oracle.com/)

technetwork/indexes/downloads/index.html). Para descargar el kit, haga clic en la ficha Downloads A-Z y, a continuación, haga clic en la letra S. Encontrará Solaris 10 Encryption Kit entre las 20 primeras entradas.

Directivas de protección IPsec

Las directivas de protección IPsec pueden utilizar cualquiera de los mecanismos de seguridad. Las directivas IPsec se pueden aplicar en los niveles siguientes:

- En el sistema
- Por socket

IPsec aplica la directiva en todo el sistema a los datagramas entrantes y salientes. Los datagramas salientes se envían con o sin protección. Si se aplica protección, los algoritmos son específicos o no específicos. Puede aplicar algunas reglas adicionales a los datagramas salientes, dados los datos adicionales que conoce el sistema. Los datagramas entrantes pueden aceptarse o dejarse. La decisión de dejar o aceptar un datagrama entrante se basa en varios criterios, que en ocasiones se pueden superponer o entrar en conflicto. Los conflictos se resuelven determinando qué regla que analiza primero. El tráfico se acepta automáticamente, excepto cuando una entrada de directiva indica que el tráfico debe omitir las demás directivas.

La directiva que normalmente protege un datagrama se puede omitir. Puede especificar una excepción en la directiva del sistema, o solicitar una omisión en la directiva por socket. Para el tráfico de un sistema, se aplican las directivas, pero no se aplican los mecanismos de seguridad reales. En lugar de ello, la directiva saliente de un paquete dentro del sistema se convierte en un paquete entrante al que se han aplicado esos mecanismos.

El archivo `ipsecinit.conf` y el comando `ipsecconf` permiten configurar directivas IPsec. Para ver detalles y ejemplos, consulte la página del comando `man ipsecconf(1M)`.

Modos de transporte y túnel en IPsec

Los estándares IPsec definen dos modos distintos de funcionamiento de IPsec, el *modo transporte* y el *modo túnel*. Dichos modos no afectan a la codificación de paquetes. Los paquetes están protegidos por AH, ESP, o ambos en cada modo. Los modos aplican la directiva de un modo distinto cuando el paquete interior es un paquete IP, como en el caso siguiente:

- En modo transporte, el encabezado exterior determina la directiva IPsec que protege el paquete IP interior.
- En modo túnel, el paquete IP interior determina la directiva IPsec que protege su contenido.

En modo transporte, pueden utilizarse el encabezado exterior, el encabezado siguiente y los puertos que admita el siguiente encabezado para determinar la directiva IPsec. En efecto, IPsec puede aplicar diferentes directivas de modo de transporte entre dos direcciones IP hasta la

granularidad de un único puerto. Por ejemplo, si el siguiente encabezado es TCP, que admite puertos, la directiva IPsec se puede configurar para un puerto TCP de la dirección IP exterior. De modo similar, si el siguiente encabezado es un encabezado IP, se pueden utilizar el encabezado exterior y el encabezado IP interior para determinar la directiva IPsec.

El modo túnel sólo funciona para los datagramas de IP en IP. El uso de túneles en modo túnel puede ser útil cuando los usuarios se conecten desde casa a un equipo central. En modo túnel, la directiva IPsec se aplica en el contenido del datagrama IP interior. Se pueden aplicar diferentes directivas IPsec para distintas direcciones IP interiores. Es decir, el encabezado IP interior, su encabezado siguiente y los puertos que admite el siguiente encabezado pueden aplicar una directiva. A diferencia del modo transporte, en el modo túnel el encabezado IP exterior no dicta la directiva de su datagrama IP interior.

Por tanto, en modo túnel, la directiva IPsec se puede especificar para las subredes de una LAN detrás de un enrutador y para puertos de dichas subredes. La directiva IPsec también se puede especificar para una dirección IP concreta, es decir, hosts de esas subredes. Los puertos de dichos hosts también pueden tener una directiva IPsec específica. Sin embargo, si se ejecuta un protocolo de enrutamiento dinámico por un túnel, no utilice la selección de subredes o la sección de direcciones, porque la vista de la topología de red en la red equivalente podría cambiar. Los cambios invalidarían la directiva IPsec estática. Para ver algunos ejemplos de procedimientos de túnel que incluyen la configuración de rutas estáticas, consulte [“Protección de una VPN con IPsec” en la página 530](#).

En SO Solaris, el modo túnel puede aplicarse sólo en una interfaz de red de túneles IP. El comando `ipseconf` proporciona una palabra clave `tunnel` para seleccionar una interfaz de red de túneles IP. Cuando la palabra clave `tunnel` está presente en una regla, todos los selectores específicos de dicha regla se aplican al paquete interior.

En modo transporte, ESP, AH, o ambos, pueden proteger el datagrama.

La figura siguiente muestra un encabezado IP con un paquete TCP sin proteger.

FIGURA 19-3 Paquete IP sin proteger con información TCP



En modo transporte, ESP protege los datos tal como se muestra en la figura siguiente. El área sombreada muestra la parte cifrada del paquete.

FIGURA 19-4 Paquete IP protegido con información TCP



☐ Cifrado

En modo transporte, AH protege los datos como se muestra en la figura siguiente.

FIGURA 19-5 Paquete protegido por encabezado de autenticación



AH cifra los datos antes de que aparezcan en el datagrama. En consecuencia, la protección que proporciona AH, incluso en el modo transporte, cifra parte del encabezado IP.

En modo túnel, todo el datagrama está *dentro* de la protección de un encabezado IPsec. El datagrama de la [Figura 19-3](#) está protegido en modo túnel por otro encabezado IPsec exterior, en este caso ESP, tal como se muestra en la figura siguiente.

FIGURA 19-6 Paquete IPsec protegido en modo túnel



☐ Cifrado

El comando `ipsecconf` incluye palabras clave para configurar túneles en modo túnel o en modo transporte.

- Para obtener detalles sobre la directiva por socket, consulte la página del comando [man ipsec\(7P\)](#).
- Si desea ver un ejemplo de la directiva por socket, consulte “[Cómo utilizar IPsec para proteger un servidor web del tráfico que no procede de Internet](#)” en la página 515.
- Para más información acerca de los túneles, consulte la página del comando [man ipsecconf\(1M\)](#).
- Para ver un ejemplo de configuración de túnel, consulte “[Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4](#)” en la página 535.

Redes privadas virtuales e IPsec

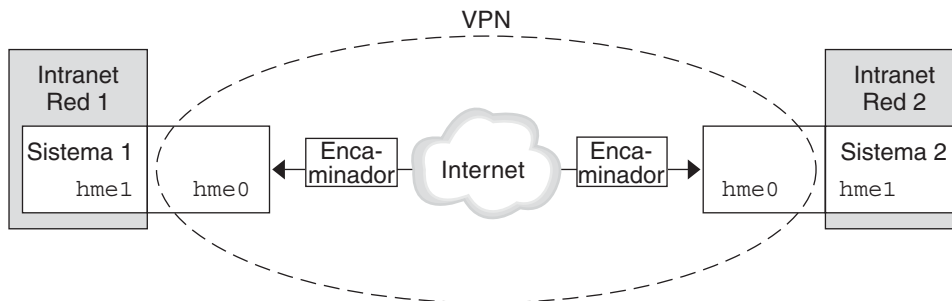
Un túnel configurado es una interfaz de punto a punto. El túnel permite la encapsulación de un paquete IP dentro de otro paquete IP. Un túnel configurado correctamente requiere tanto un origen como un destino. Para obtener más información, consulte la página de comando [man tun\(7M\)](#) y [Configuración de túneles para compatibilidad con IPv6](#).

Un túnel crea una [interfaz física](#) aparente para IP. La integridad del vínculo físico depende de los protocolos de seguridad subyacentes. Si configura las asociaciones de seguridad (SA) de un modo seguro, puede confiar en el túnel. Los paquetes que salen del túnel deben haberse originado en su equivalente especificado en el destino del túnel. Si existe esa confianza, puede utilizar el reenvío de IP por interfaz para crear una [red privada virtual \(VPN\)](#).

Puede utilizar IPsec para construir una VPN. IPsec protege la conexión. Por ejemplo, una organización que utiliza tecnología VPN para conectar oficinas con redes separadas puede implementar IPsec para proteger el tráfico entre las dos oficinas.

La figura siguiente ilustra cómo las dos oficinas utilizan Internet para formar su VPN con IPsec implementado en sus sistemas de red.

FIGURA 19-7 Red privada virtual



Para ver un ejemplo detallado del procedimiento de configuración, consulte [“Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4”](#) en la página 535.

Para ver un ejemplo similar con direcciones IPv6, consulte [“Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv6”](#) en la página 545.

Paso a través de IPsec y NAT

IKE puede negociar las SA IPsec a través de un cuadro NAT. Esta función permite a los sistemas conectarse de forma segura desde una red remota, incluso cuando los sistemas están detrás de un dispositivo NAT. Por ejemplo, los empleados que trabajan desde casa, o que se registran desde un sitio de conferencia pueden proteger su tráfico con IPsec.

NAT significa traducción de direcciones de red. Un cuadro NAT se utiliza para traducir una dirección interna privada en una dirección de Internet exclusiva. Las NAT son muy comunes en los puntos de acceso públicos a Internet, como los hoteles. Para obtener más información, consulte [“Uso de la función NAT del filtro IP” en la página 646](#).

La posibilidad de utilizar IKE cuando un cuadro NAT se encuentra entre sistemas que se comunican, se denomina NAT traversal, o NAT-T. En la versión the Solaris 10, tiene las limitaciones siguientes:

- NAT-T no puede aprovechar la aceleración ESP IPsec que proporciona la placa de Sun Crypto Accelerator 4000. Sin embargo, la aceleración IKE con la placa Sun Crypto Accelerator 4000 funciona.
- El protocolo AH depende de un encabezado de IP inalterable; por lo tanto, AH no funciona con NAT-T. El protocolo ESP se utiliza con NAT-T.
- El cuadro NAT no utiliza reglas de procesamiento especiales. Un cuadro NAT con reglas de procesamiento IPsec especiales podría interferir con la implementación de NAT-T.
- NAT-T sólo funciona cuando el iniciador IKE es el sistema que hay detrás del cuadro NAT. Un contestador IKE no puede estar detrás de un cuadro NAT a menos que el cuadro se haya programado para reenviar paquetes IKE al sistema individual adecuado detrás del cuadro.

En los siguientes documentos RFC se describen las funciones de NAT y los límites de NAT-T. Puede obtener copias de los RFC en <http://www.rfc-editor.org>.

- RFC 3022, "Traditional IP Network Address Translator (Traditional NAT)", enero de 2001.
- RFC 3715, "IPsec-Network Address Translation (NAT) Compatibility Requirements", marzo de 2004.
- RFC 3947, "Negotiation of NAT-Traversal in the IKE", enero de 2005.
- RFC 3948, "UDP Encapsulation of IPsec Packets", enero de 2005.

Para utilizar IPsec en una NAT, consulte [“Configuración de IKE para sistemas portátiles \(mapa de tareas\)” en la página 614](#).

IPsec y Sctp

El SO Solaris admite el protocolo Sctp (Streams Control Transmission Protocol). Se admite el uso del protocolo Sctp y el número de puerto Sctp para especificar la directiva IPsec, pero no es fiable. Las extensiones IPsec para Sctp tal como se especifican en la RFC 3554 todavía no están implementadas. Estas limitaciones pueden generar complicaciones a la hora de crear la directiva IPsec para Sctp.

Sctp puede utilizar varias direcciones de origen y destino en el contexto de una sola asociación Sctp. Cuando la directiva IPsec se aplica a una única dirección de origen o una única dirección de destino, la comunicación puede fallar cuando Sctp cambie la dirección de origen o de destino de dicha asociación. La directiva IPsec sólo reconoce la dirección original. Para obtener información sobre Sctp, consulte las RFC y [“Protocolo Sctp” en la página 42](#).

IPsec y Zonas de Solaris

IPsec se configura desde la zona global para las zonas IP compartidas. El archivo de configuración de la directiva IPsec, `ipsecinit.conf`, se encuentra únicamente en la zona global. El archivo puede tener entradas que se apliquen a zonas no globales, así como entradas que se apliquen a la zona global.

Para zonas de IP exclusiva, IPsec está configurado en la zona no global.

Para obtener información sobre cómo utilizar IPsec con zonas, consulte [“Protección del tráfico con IPsec” en la página 510](#). Para obtener información sobre las zonas, consulte el [Capítulo 16, “Introducción a Solaris Zones” de Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#).

IPsec y dominios lógicos

IPsec funciona con dominios lógicos. El dominio lógico debe ejecutar una versión del SO Solaris que incluya IPsec, como, por ejemplo, Solaris 10.

Para crear dominios lógicos, debe utilizar Oracle VM Server para SPARC, anteriormente denominado Logical Domains. Para obtener más información sobre cómo configurar dominios lógicos, consulte [Logical Domains 1.2 Administration Guide](#) o [Oracle VM Server for SPARC 2.0 Administration Guide](#).

Archivos y utilidades IPsec

La [Tabla 19-3](#) describe los archivos, comandos e identificadores de servicios que se utilizan para configurar y administrar IPsec. Para mayor información, la tabla incluye comandos y archivos de administración de claves.

A partir de Solaris 10 4/09, SMF administra IPsec. Para obtener más información sobre los identificadores de servicios, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)”](#) de *Guía de administración del sistema: administración básica*.

- Si desea obtener instrucciones sobre la implementación de IPsec en la red, consulte “Protección del tráfico con IPsec (mapa de tareas)” en la [página 509](#).
- Para mas información sobre los archivos y las utilidades IPsec, consulte el [Capítulo 21, “Arquitectura de seguridad IP \(referencia\)”](#).

TABLA 19-3 Lista de archivos y utilidades IPsec seleccionados

Utilidad IPsec, archivo o servicio	Descripción	Página de comando man
svc:/network/ipsec/ipsecalgs	En la versión actual, el servicio SMF que administra los algoritmos IPsec.	smf(5) , ipsecalgs(1M)
svc:/network/ipsec/manual-key	En la versión actual, el servicio SMF que gestiona asociaciones de seguridad manuales (SA).	smf(5) , ipseckey(1M)
svc:/network/ipsec/policy	En la versión actual, el servicio SMF que gestiona la directiva IPsec.	smf(5) , ipseconf(1M)
svc: /network/ipsec/ike	En la versión actual, el servicio SMF para la gestión automática de IPsec SA.	smf(5) , in.iked(1M)
Archivo /etc/inet/ipsecinit.conf	archivo de directiva IPsec En las versiones anteriores a Solaris 10 4/09, si el archivo existe, IPsec se activará en el momento del inicio. En la versión actual, el servicio SMF policy utiliza este archivo para configurar la directiva de IPsec durante el inicio del sistema.	ipseconf(1M)
Comando ipseconf	Comando de directiva IPsec. Es útil para visualizar y modificar la directiva IPsec actual, así como para realizar pruebas. En las versiones anteriores a Solaris 10 4/09 las secuencias de comandos de inicio utilizan ipseconf para leer el archivo /etc/inet/ipsecinit.conf y activar IPsec. En la versión actual, ipseconf lo utiliza el servicio SMF policy para configurar la directiva IPsec en el inicio del sistema.	ipseconf(1M)
Interfaz de socket PF_KEY	Interfaz para la base de datos de asociaciones de seguridad (SADB). Controla la administración de claves manual y automática.	pf_key(7P)

TABLA 19-3 Lista de archivos y utilidades IPsec seleccionados (Continuación)

Utilidad IPsec, archivo o servicio	Descripción	Página de comando man
Comando ipseckey	Comando de material de claves de asociaciones de seguridad (SA) de IPsec. ipseckey es un componente frontal de línea de comandos para la interfaz PF_KEY. ipseckey puede crear, destruir o modificar SA.	ipseckey(1M)
Archivo /etc/inet/secret/ipseckey	Claves para SA de IPsec. En las versiones anteriores a Solaris 10 4/09 si existe el archivo ipsecinit.conf, el archivo ipseckey se lee automáticamente en el momento del inicio. En la versión actual, el servicio SMF manual-key utiliza ipseckey para configurar manualmente las asociaciones de seguridad (SA) durante el inicio del sistema.	
Comando ipsecalgs	Comando de algoritmos IPsec. Es útil para visualizar y modificar la lista de algoritmos IPsec y sus propiedades. En la versión actual, se utiliza por parte del servicio SMF ipsecalgs para sincronizar algoritmos IPsec conocidos con el núcleo en el inicio del sistema.	ipsecalgs(1M)
Archivo /etc/inet/ipsecalgs	Contiene los protocolos IPsec configurados y las definiciones de algoritmos. Este archivo lo administra el comando ipsecalgs y nunca se debe editar manualmente.	
Archivo /etc/inet/ike/config	archivo de configuración y directiva de IKE Por defecto, este archivo no existe. En las versiones anteriores a Solaris 10 4/09, si el archivo existe, el daemon IKE (in.iked) proporciona gestión automática de claves. La administración se basa en reglas y parámetros globales del archivo /etc/inet/ike/config. Consulte “Archivos y utilidades IKE” en la página 580. En la versión actual, si el archivo existe, el servicio svc:/network/ipsec/ike inicia el daemon IKE, in.iked, para proporcionar gestión automática de claves.	ike.config(4)

Cambios en IPsec para la versión Solaris 10

Para ver una lista completa de las nuevas funciones de Solaris 10 y una descripción de las versiones de Solaris, consulte [Novedades de Oracle Solaris 10 8/11](#). A partir de la versión Solaris 9, IPsec incluye las siguientes funciones:

- Cuando se conecta una placa Sun Crypto Accelerator 4000, ésta coloca en caché automáticamente las SA IPsec para los paquetes que utilizan la interfaz Ethernet de la placa. La placa también acelera el procesamiento de las SA IPsec.
- IPsec puede aprovechar la administración de claves automática con IKE a través de redes IPv6. Para más información, consulte el [Capítulo 22, “Intercambio de claves de Internet \(descripción general\)”](#).

Para conocer las novedades IKE, consulte [“Cambios de IKE en Solaris 10”](#) en la página 582.

- Encontrará más ayuda en el analizador del comando `ipseckey`. El comando `ipseckey monitor` incluye indicaciones de fecha y hora en cada evento. Para obtener más información, consulte la página del comando `man ipseckey(1M)`.
- Los algoritmos IPsec ahora provienen de una ubicación de almacenamiento central, la estructura criptográfica de Solaris. La página del comando `man ipsecalgs(1M)` describe las características de los algoritmos que hay disponibles. Los algoritmos están optimizados para la arquitectura en la que se ejecutan. Para obtener una descripción de la estructura, consulte el [Capítulo 13, “Estructura criptográfica de Oracle Solaris \(descripción general\)”](#) de *Guía de administración del sistema: servicios de seguridad*.
- IPsec funciona en la zona global. La directiva IPsec se administra en la zona global para una zona no global. El material de claves se crea y administra manualmente en la zona global para una zona no global. IKE no se puede utilizar para generar claves para una zona no global. Para obtener más información sobre las zonas, consulte el [Capítulo 16, “Introducción a Solaris Zones”](#) de *Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris*.
- La directiva IPsec puede funcionar con el protocolo SCTP (Streams Control Transmission Protocol) y el número de puerto SCTP. Sin embargo, la implementación no está completa. Las extensiones IPsec para SCTP que se especifican en la RFC 3554 todavía no están implementadas. Estas limitaciones pueden ocasionar complicaciones a la hora de crear la directiva IPsec para SCTP. Para obtener más información, consulte las RFC. Asimismo, lea [“IPsec y SCTP”](#) en la página 504 y [“Protocolo SCTP”](#) en la página 42.
- IPsec e IKE pueden proteger el tráfico que se origina detrás de un cuadro NAT. Para obtener más detalles e información sobre las limitaciones, consulte [“Paso a través de IPsec y NAT”](#) en la página 503. Para ver los procedimientos, consulte [“Configuración de IKE para sistemas portátiles \(mapa de tareas\)”](#) en la página 614.

Configuración de IPsec (tareas)

Este capítulo incluye los procedimientos para implementar IPsec en la red. Los procedimientos se describen en los siguientes mapas de tareas:

- “Protección del tráfico con IPsec (mapa de tareas)” en la página 509
- “Protección de una VPN con IPsec (mapa de tareas)” en la página 532

Para obtener información general sobre IPsec, consulte el [Capítulo 19, “Arquitectura de seguridad IP \(descripción general\)”](#). Para obtener información de referencia sobre IPsec, consulte el [Capítulo 21, “Arquitectura de seguridad IP \(referencia\)”](#).

Protección del tráfico con IPsec (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos que configuran IPsec entre uno o más sistemas. Las páginas del comando [man ipseconf\(1M\)](#), [ipseckey\(1M\)](#) e [ifconfig\(1M\)](#) también describen procedimientos útiles en sus secciones de ejemplos correspondientes.

Tarea	Descripción	Para obtener instrucciones
Proteger el tráfico entre dos sistemas.	Protege los paquetes de un sistema a otro.	“Cómo proteger el tráfico entre dos sistemas con IPsec” en la página 511
Proteger un servidor web con la directiva IPsec.	Requiere el uso de IPsec por parte del tráfico que no sea de red. Los clientes web se identifican mediante puertos específicos, que omiten las comprobaciones de IPsec.	“Cómo utilizar IPsec para proteger un servidor web del tráfico que no procede de Internet” en la página 515
Visualizar las directivas de IPsec.	Muestra las directivas de IPsec que se están aplicando, en el orden en que se aplican.	“Cómo visualizar las directivas de IPsec” en la página 518

Tarea	Descripción	Para obtener instrucciones
Generar números aleatorios.	Genera números aleatorios para el material de claves para las asociaciones de seguridad creadas manualmente.	“Cómo generar números aleatorios en un sistema Solaris” en la página 519 “Cómo generar una clave simétrica con el comando pktool” de <i>Guía de administración del sistema: servicios de seguridad</i>
Crear o reemplazar asociaciones de seguridad manualmente.	Proporciona los datos básicos para las asociaciones de seguridad: <ul style="list-style-type: none">■ Nombre de algoritmo IPsec y material de claves■ Clave para el índice de parámetros de seguridad■ Direcciones IP de origen y destino	“Cómo crear manualmente asociaciones de seguridad IPsec” en la página 520
Comprobar que IPsec esté protegiendo los paquetes.	Examina el resultado del comando snoop para los encabezados específicos que indica cómo se protegen los datagramas IP.	“Cómo verificar que los paquetes estén protegidos con IPsec” en la página 525
(Opcional) Crear un rol de seguridad de red.	Crea un rol que puede configurar una red segura, pero que puede desempeñar menos funciones que un superusuario.	“Cómo configurar una función para la seguridad de la red” en la página 526
Administrar IPsec y materiales clave como un conjunto de servicios SME.	Describe cómo y cuándo utilizar los comandos que habilitan, deshabilitan, actualizan y reinician los servicios. También describe los comandos que cambian los valores de propiedad de los servicios.	“Cómo administrar servicios de IPsec e IKE” en la página 528
Configurar una red privada virtual protegida (VPN).	Configura IPsec entre dos sistemas separados por Internet.	“Protección de una VPN con IPsec (mapa de tareas)” en la página 532

Protección del tráfico con IPsec

En esta sección se describen los procedimientos que permiten proteger un servidor web y el tráfico entre dos sistemas. Para proteger una VPN, consulte [“Protección de una VPN con IPsec \(mapa de tareas\)” en la página 532](#). Existen procedimientos adicionales que proporcionan los materiales de claves y las asociaciones de seguridad, y además verifican que IPsec esté funcionando de acuerdo con la configuración establecida.

La información siguiente se aplica a todas las tareas de configuración de IPsec:

- **IPsec y zonas** – Para administrar la directiva IPsec y las claves para una zona no global IP compartida, cree el archivo de directiva IPsec en la zona global y ejecute los comandos de configuración de IPsec desde la zona global. Utilice la dirección de origen que corresponda a la zona no global que se esté configurando. También puede configurar la directiva IPsec y las claves en la zona global para la zona global. Para una zona de IP exclusiva, configure la directiva IPsec en la zona no global. A partir de la versión Solaris 10 7/07, puede utilizar IKE para administrar claves en una zona no global.
- **IPsec y RBAC** – Para utilizar los roles para administrar IPsec, consulte el [Capítulo 9, “Uso del control de acceso basado en roles \(tareas\)” de Guía de administración del sistema: servicios de seguridad](#). Si desea ver un ejemplo, consulte “Cómo configurar una función para la seguridad de la red” en la página 526.
- **IPsec y SCTP** – IPsec se puede utilizar para proteger las asociaciones SCTP (Streams Control Transmission Protocol), pero debe hacerse con precaución. Para obtener más información, consulte “IPsec y SCTP” en la página 504.

▼ Cómo proteger el tráfico entre dos sistemas con IPsec

Este procedimiento presupone la siguiente configuración:

- Los dos sistemas se denominan *enigma* y *partym*.
- Cada sistema tiene dos direcciones, una dirección IPv4 y otra IPv6.
- Cada sistema requiere cifrado ESP con el algoritmo AES, que, a su vez, requiere una clave de 128 bits y autenticación ESP con el resumen de mensajes de SHA1, que, a su vez, requiere una clave de 160 bits.
- Cada sistema utiliza asociaciones de seguridad compartidas.

Con las asociaciones de seguridad (SA) compartidas, sólo se necesita un par de SA para proteger los dos sistemas.

Antes de empezar

Debe estar en la zona global para configurar la directiva IPsec para el sistema o para una zona de IP compartida. Para una zona de IP exclusiva, configure la directiva IPsec en la zona no global.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

Nota – El registro remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para iniciar una sesión remota de forma segura. Si desea ver un ejemplo, consulte el [Ejemplo 20–1](#).

2 En cada sistema, agregue entradas de host.

En la versión actual, agregue las entradas de host al archivo `/etc/inet/hosts`.

En un sistema que se ejecute en una versión anterior a Solaris 10 7/07, agregue entradas IPv4 e IPv6 en el archivo `/etc/inet/ipnodes`. Las entradas de un sistema deben ser contiguas en el archivo. Para obtener información sobre los archivos de configuración del sistema, consulte [“Archivos de configuración TCP/IP” en la página 233](#) y el [Capítulo 11, “IPv6 en profundidad \(referencia\)”](#).

Si está conectando sistemas sólo con direcciones IPv4, debe modificar el archivo `/etc/inet/hosts`. En este ejemplo, los sistemas que se conectan ejecutan una versión anterior de Solaris y utilizan direcciones IPv6.

a. En un sistema denominado `enigma`, escriba lo siguiente en el archivo `hosts` o `ipnodes`:

```
# Secure communication with partym
192.168.13.213 partym
2001::eeee:3333:3333 partym
```

b. En un sistema denominado `partym`, escriba lo siguiente en el archivo `hosts` o `ipnodes`:

```
# Secure communication with enigma
192.168.116.16 enigma
2001::aaaa:6666:6666 enigma
```

El uso de los servicios de asignación de nombres simbólicos no es seguro.

3 En cada sistema, cree el archivo de directiva IPsec.

El nombre de archivo es `/etc/inet/ipsecinit.conf`. Para ver un ejemplo, consulte el archivo `/etc/inet/ipsecinit.sample`.

4 Agregue una entrada de directiva IPsec al archivo `ipsecinit.conf`.

a. En el sistema `enigma`, agregue la directiva siguiente:

```
{laddr enigma raddr partym} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. En el sistema `partym`, agregue una directiva idéntica:

```
{laddr partym raddr enigma} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Para ver la sintaxis de las entradas de la directiva IPsec, consulte la página del comando `man ipsecconf(1M)`.

5 En cada sistema, agregue un par de SA IPsec entre los dos sistemas.

Puede configurar el intercambio de claves de Internet (IKE) para crear las SA automáticamente. También puede agregar las SA de forma manual.

Nota – Debe utilizar IKE a menos que tenga una razón de peso para generar y mantener las claves manualmente. La administración de claves IKE es más segura que la administración manual.

- Configure IKE siguiendo uno de los métodos de configuración de [“Configuración de IKE \(mapa de tareas\)” en la página 583](#). Para ver la sintaxis del archivo de configuración de IKE, consulte la página del comando `man ike.config(4)`.
- Para agregar las SA manualmente, consulte [“Cómo crear manualmente asociaciones de seguridad IPsec” en la página 520](#).

6 Habilite la directiva IPsec.

- Si está ejecutando una versión anterior a Solaris 10 4/09 reinicie el sistema.

```
# init 6
```

A continuación, vaya a [“Cómo verificar que los paquetes estén protegidos con IPsec” en la página 525](#).

- A partir de la versión Solaris 10 4/09, actualice el servicio IPsec y habilite el servicio de administración de claves.

Complete del [Paso 7](#) al [Paso 10](#).

7 Compruebe la sintaxis del archivo de directiva IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

Subsane los posibles errores, compruebe la sintaxis del archivo y continúe.

8 Actualice la directiva IPsec.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

La directiva IPsec está habilitada de forma predeterminada, por lo que *puede actualizarla*. Si ha deshabilitado la directiva IPsec, habilítela.

```
# svcadm enable svc:/network/ipsec/policy:default
```

9 Active las claves para IPsec.

- Si ha configurado IKE en el [Paso 5](#), realice una de las acciones siguientes:

- Si el servicio `ike` no está habilitado, habilítelo.

```
# svcadm enable svc:/network/ipsec/ike:default
```

- Si el servicio `ike` está habilitado, reinícielo.

```
# svcadm restart svc:/network/ipsec/ike:default
```
 - Si ha configurado manualmente las claves en el [Paso 5](#), realice una de las acciones siguientes:
 - Si el servicio `manual-key` no está habilitado, habilítelo.

```
# svcadm enable svc:/network/ipsec/manual-key:default
```
 - Si el servicio `manual-key` está habilitado, actualícelo.

```
# svcadm refresh svc:/network/ipsec/manual-key:default
```
- 10 Compruebe que los paquetes se estén protegiendo.**
Para ver el procedimiento, consulte [“Cómo verificar que los paquetes estén protegidos con IPsec” en la página 525](#).

Ejemplo 20-1 Adición de directivas IPsec al utilizar una conexión `ssh`

En este ejemplo, el administrador configura como superusuario las claves y la directiva IPsec en dos sistemas mediante el comando `ssh` para llegar al segundo sistema. Para obtener más información, consulte la página de comando `man ssh(1)`.

- En primer lugar, el administrador realiza del [Paso 2](#) al [Paso 5](#) del procedimiento anterior para configurar el primer sistema.
- A continuación, en una ventana de terminal distinta, el administrador utiliza el comando `ssh` para iniciar la sesión en el segundo sistema.

```
local-system # ssh other-system  
other-system #
```
- En la ventana de terminal de la sesión `ssh`, el administrador configura la directiva IPsec y las claves del segundo sistema; para ello, realiza del [Paso 2](#) al [Paso 6](#).
- A continuación, el administrador termina la sesión `ssh`.

```
other-system # exit  
local-system #
```
- Por último, el administrador realiza el [Paso 6](#) para habilitar la directiva IPsec en el primer sistema.

La próxima ocasión que los dos sistemas se comunican, incluida la conexión `ssh`, la comunicación queda protegida por IPsec.

Ejemplo 20-2 Cómo proteger el tráfico con IPsec sin reiniciar

El siguiente ejemplo es útil cuando se está ejecutando una versión anterior a Solaris 10 4/09. Es decir, en su versión, IPsec no se gestiona como un servicio. El ejemplo describe cómo

implementar IPsec en un entorno de prueba. En un entorno de producción, es más seguro reiniciar que ejecutar el comando `ipsecconf`. Consulte las consideraciones de seguridad al final de este ejemplo.

En lugar de reiniciar en el [Paso 6](#), elija una de estas opciones:

- Si ha utilizado IKE para crear material de claves, detenga y reinicie el daemon `in.iked`.


```
# pkill in.iked
# /usr/lib/inet/in.iked
```
- Si ha agregado claves manualmente, utilice el comando `ipseckey` para agregar las SA a la base de datos.

```
# ipseckey -c -f /etc/inet/secret/ipseckey
```

A continuación, active la directiva IPsec con el comando `ipsecconf`.

```
# ipsecconf -a /etc/inet/ipsecinit.conf
```

Consideraciones de seguridad: lea la advertencia que aparece al ejecutar el comando `ipsecconf`. Un socket que ya está bloqueado, es decir, un socket que ya está en uso, constituye una puerta trasera no segura al sistema. Si desea más información al respecto, consulte [“Consideraciones de seguridad para `ipsecinit.conf` e `ipsecconf`” en la página 570](#).

▼ Cómo utilizar IPsec para proteger un servidor web del tráfico que no procede de Internet

Un servidor web seguro permite a los clientes web comunicarse con el servicio web. En un servidor web seguro, el tráfico que no sea de la red *debe* someterse a comprobaciones de seguridad. El siguiente procedimiento incluye las omisiones del tráfico de red. Además, este servidor web puede realizar solicitudes de clientes DNS no seguras. El resto del tráfico requiere ESP con los algoritmos AES y SHA-1.

Antes de empezar

Debe encontrarse en la zona global para poder configurar la directiva IPsec. Para una zona de IP exclusiva, configure la directiva IPsec en la zona no global. Ha completado [“Cómo proteger el tráfico entre dos sistemas con IPsec” en la página 511](#) para que se apliquen las condiciones siguientes:

- Que la comunicación entre los dos sistemas esté protegida por IPsec.
- Que se esté generando material de claves, ya sea de forma manual o mediante IKE.
- Que haya comprobado que los paquetes se estén protegiendo.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para iniciar una sesión remota de forma segura.

2 Determine qué servicios deben omitir las comprobaciones de directiva de seguridad.

En el caso de un servidor web, estos servicios incluyen los puertos TCP 80 (HTTP) y 443 (HTTP seguro). Si el servidor web proporciona consultas de nombres DNS, el servidor también podría incluir el puerto 53 tanto para TCP como para UDP.

3 Cree una directiva IPsec para el servidor web y habilítela.

- A partir de la versión Solaris 10 4/09, siga del [Paso 4](#) al [Paso 7](#).
- Si está ejecutando una versión anterior a Solaris 10 4/09, siga del [Paso 8](#) al [Paso 11](#).

El [Paso 12](#) es opcional en todas las versiones de Solaris.

4 Agregue la directiva de servidor web al archivo de directiva IPsec.

Agregue las líneas siguientes al archivo `/etc/inet/ipsecinit.conf`:

```
# Web traffic that web server should bypass.
{lport 80 ulp tcp dir both} bypass {}
{lport 443 ulp tcp dir both} bypass {}

# Outbound DNS lookups should also be bypassed.
{rport 53 dir both} bypass {}

# Require all other traffic to use ESP with AES and SHA-1.
# Use a unique SA for outbound traffic from the port
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Esta configuración sólo permite que el tráfico seguro acceda al sistema, con las excepciones de omisión que se describen en el [Paso 4](#).

5 Compruebe la sintaxis del archivo de directiva IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 Actualice la directiva IPsec.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

7 Actualice las claves para IPsec.

- Si ha configurado IKE en el [Paso 5](#) de “[Cómo proteger el tráfico entre dos sistemas con IPsec](#)” en la [página 511](#), reinicie el servicio `ike`.

```
# svcadm restart svc:/network/ipsec/ike
```

- Si ha configurado manualmente las claves en el [Paso 5](#) de “[Cómo proteger el tráfico entre dos sistemas con IPsec](#)” en la [página 511](#), actualice el servicio `manual-key`.

```
# svcadm refresh svc:/network/ipsec/manual-key:default
```

La configuración se ha completado. Si lo desea, puede llevar a cabo el [Paso 12](#).

8 Cree un archivo en el directorio `/etc/inet` para la directiva del servidor web.

Nota – Los siguientes pasos configuran un servidor web que está ejecutando una versión anterior a Solaris 10 4/09.

Asigne al archivo un nombre que indique su finalidad, por ejemplo `IPsecWebInitFile`. Escriba las siguientes líneas en el archivo:

```
# Web traffic that web server should bypass.
{lport 80 ulp tcp dir both} bypass {}
{lport 443 ulp tcp dir both} bypass {}

# Outbound DNS lookups should also be bypassed.
{rport 53 dir both} bypass {}

# Require all other traffic to use ESP with AES and SHA-1.
# Use a unique SA for outbound traffic from the port
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Esta configuración sólo permite que el tráfico seguro acceda al sistema, con las excepciones de omisión que se describen en el [Paso 4](#).

9 Copie el contenido del archivo que haya creado en el [Paso 8](#) en el archivo `/etc/inet/ipsecinit.conf`.**10 Proteja el archivo `IPsecWebInitFile` con permisos de sólo lectura.**

```
# chmod 400 IPsecWebInitFile
```

11 Proteja el servidor web sin reiniciar.

Elija una de las siguientes opciones:

- Si está utilizando IKE para la administración de claves, detenga el daemon `in.iked` y reinícielo.

```
# pkill in.iked
# /usr/lib/inet/in.iked
```

- Si está administrando las claves manualmente, utilice los comandos `ipseckey` e `ipseconf`. Utilice `IPsecWebInitFile` como argumento para el comando `ipseconf`. Si utiliza el archivo `ipseconf` como argumento, el comando `ipseconf` genera errores cuando las directivas del archivo ya están implementadas en el sistema.

```
# ipseckey -c -f /etc/inet/secret/ipseckey
# ipseconf -a /etc/inet/IPsecWebInitFile
```



Precaución – Lea la advertencia cuando ejecute el comando `ipseconf`. Un socket que ya está bloqueado, es decir, un socket que ya está en uso, constituye una puerta trasera no segura al sistema. Si desea más información al respecto, consulte [“Consideraciones de seguridad para ipsecinit.conf e ipseconf” en la página 570](#). La misma advertencia aparece al reiniciar el daemon `in.iked`.

También puede reiniciar. Al reiniciar se asegura de que la directiva IPsec esté aplicada en todas las conexiones TCP. Al reiniciar, las conexiones TCP utilizan la directiva del archivo de directiva IPsec.

12 (Opcional) Habilite un sistema remoto para comunicarse con el servidor web para tráfico que no sea de red.

Escriba la siguiente directiva en el archivo `ipseconf` de un sistema remoto:

```
# Communicate with web server about nonweb stuff
#
{laddr webserver} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Un sistema remoto puede comunicarse de forma segura con el servidor web para tráfico que no sea de web sólo cuando las directivas IPsec del sistema coinciden.

▼ Cómo visualizar las directivas de IPsec

Puede ver las directivas configuradas en el sistema ejecutando el comando `ipseconf` sin argumentos.

Antes de empezar

Debe ejecutar el comando `ipseconf` en la zona global. Para una zona de IP exclusiva, ejecute el comando `ipseconf` en la zona no global.

1 Asuma un rol que incluya el perfil de administración IPsec de la red o conviértase en superusuario.

Si está ejecutando una versión anterior a Solaris 10 4/09, el perfil de Network IPsec Management no está disponible. Utilice el perfil de la seguridad de la red.

Para crear un rol que incluya un perfil de seguridad de red y asignarlo a un usuario, consulte [“Cómo configurar una función para la seguridad de la red” en la página 526](#).

2 Visualice las directivas de IPsec.

- a. Visualice las entradas de la directiva IPsec global en el orden en que se agregaron las entradas.

```
$ ipsecconf
```

El comando muestra cada entrada con un *índice*, seguida de un número.

- b. Visualice las entradas de la directiva IPsec en el orden en que se produzca una coincidencia.

```
$ ipsecconf -l
```

- c. Visualice las entradas de la directiva IPsec, incluidas las entradas por túnel, en el orden en que se produzca una coincidencia.

```
$ ipsecconf -L
```

▼ Cómo generar números aleatorios en un sistema Solaris

Si está especificando claves manualmente, el material de claves debe ser aleatorio. El formato del material de claves de un sistema Solaris es hexadecimal. Otros sistemas operativos pueden requerir material de claves ASCII. Para generar material de claves para un sistema Solaris que se comunica con otro sistema operativo que requiera ASCII, consulte el [Ejemplo 23-1](#).

Si su sitio cuenta con un generador de números aleatorios, utilícelo. De lo contrario, puede utilizar el comando `od` con el dispositivo Solaris `/dev/random` como entrada. Para más información, consulte la página del comando `man od(1)`.

En la versión Solaris 10 4/09, también puede utilizar el comando `pktool`. La sintaxis de este comando es más sencilla que la del comando `od`. Para obtener más detalles, consulte “[Cómo generar una clave simétrica con el comando pktool](#)” de *Guía de administración del sistema: servicios de seguridad*.

1 Genere números aleatorios en formato hexadecimal.

```
% od -x|-X -A n file | head -n
```

-x Muestra el vaciado octal en formato hexadecimal. El formato hexadecimal resulta útil para el material de claves. Dicho formato se imprime en bloques de 4 caracteres.

-X Muestra el vaciado octal en formato hexadecimal. Dicho formato se imprime en bloques de 8 caracteres.

-A n Elimina la base de desfase de entrada de la pantalla.

archivo Actúa como origen para los números aleatorios.

head -n Limita el resultado de la pantalla a las primeras *n* líneas.

2 Combine el resultado para crear una clave con la longitud adecuada.

Elimine los espacios entre los números de una línea para crear una clave de 32 caracteres. Una clave de 32 caracteres tiene 128 bits. En el caso de un índice de parámetros de seguridad (SPI), debe utilizar una clave de 8 caracteres. La clave debe utilizar el prefijo 0x.

Ejemplo 20-3 Generación de material de claves para IPsec

El ejemplo siguiente muestra dos líneas de claves en grupos de ocho caracteres hexadecimales cada uno.

```
% od -x -A n /dev/random | head -2
d54d1536 4a3e0352 0faf93bd 24fd6cad
8ecc2670 f3447465 20db0b0c c83f5a4b
```

Al combinar los cuatro números de la primera línea, puede crear una clave de 32 caracteres. Un número de 8 caracteres precedido por 0x proporciona un valor de SPI adecuado, por ejemplo, 0xf3447465.

El ejemplo siguiente muestra dos líneas de claves en grupos de cuatro caracteres hexadecimales cada uno.

```
% od -x -A n /dev/random | head -2
34ce 56b2 8b1b 3677 9231 42e9 80b0 c673
2f74 2817 8026 df68 12f4 905a db3d ef27
```

Al combinar los ocho números en la primera línea, puede crear una clave de 32 caracteres.

▼ Cómo crear manualmente asociaciones de seguridad IPsec

El procedimiento siguiente proporciona el material de claves para el procedimiento [“Cómo proteger el tráfico entre dos sistemas con IPsec” en la página 511](#). Está generando claves para dos sistemas, partym y enigma. Se generan las claves en un sistema, y después se utilizan las claves del primer sistema en ambos sistemas.

Antes de empezar

Debe estar en la zona global para administrar manualmente material de claves para una zona IP compartida.

1 Genere el material de claves para la SA.

Necesita tres números aleatorios hexadecimales para el tráfico saliente y tres para el tráfico entrante.

Por tanto, un sistema necesita generar los siguientes números:

- Dos números aleatorios hexadecimales como valor para la palabra clave spi. Un número es para el tráfico saliente. Otro es para el tráfico entrante. Cada número puede tener hasta ocho caracteres de longitud.
- Dos números aleatorios hexadecimales para el algoritmo SHA-1 para la autenticación. Para una clave de 160 bits, cada número debe tener 40 caracteres de longitud. Un número es para dst enigma. Un número es para dst partym.
- Dos números aleatorios hexadecimales para el algoritmo DES para el cifrado de ESP. Para una clave de 256 bits, cada número debe tener 64 caracteres de longitud. Un número es para dst enigma. Un número es para dst partym.

Si dispone de un generador de números aleatorios en su sitio, utilícelo. También puede utilizar el comando `od`. Consulte [“Cómo generar números aleatorios en un sistema Solaris” en la página 519](#) para ver el procedimiento.

2 En la consola del sistema de uno de los sistemas, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para iniciar una sesión remota de forma segura.

3 Cree las SA.

- A partir de la versión Solaris 10 4/09, siga del [Paso 8](#) al [Paso 10](#).
- Si está ejecutando una versión anterior a Solaris 10 4/09, siga del [Paso 4](#) al [Paso 9](#).

4 Habilite el modo de comando `ipseckey`.

```
# ipseckey
```

```
>
```

El indicador de comandos `>` indica que está en el modo de comando `ipseckey`.

5 Si está sustituyendo las SA existentes, vacíelas.

```
> flush
```

```
>
```

Para evitar que un intruso interrumpa las SA, debe sustituir el material de claves.

Nota – Es necesario coordinar la sustitución de claves en los sistemas que se comunican. Al sustituir las SA en un sistema, también deben sustituirse las del sistema remoto.

6 Para crear SA, escriba el comando siguiente.

```
> add protocol spi random-hex-string \  
src addr dst addr2 \  
protocol-prefix alg protocol-algorithm \  
protocol-prefixkey random-hex-string-of-algorithm-specified-length
```

Esta sintaxis también se utiliza para sustituir las SA que acaba de vaciar.

protocol

Especifica esp o ah.

random-hex-string

Especifica un número aleatorio de hasta ocho caracteres en formato hexadecimal. Preceda los caracteres con 0x. Si especifica más números de los que acepta el índice de parámetros de seguridad (SPI), el sistema omitirá los números adicionales. Si especifica menos números de los que acepta el SPI, el sistema rellena la entrada.

addr

Especifica la dirección IP de un sistema.

addr2

Especifica la dirección IP del sistema equivalente a *addr*.

protocol-prefix

Especifica un prefijo encr o auth. El prefijo encr se utiliza con el protocolo esp. El prefijo auth se utiliza con el protocolo ah y para autenticar el protocolo esp.

protocol-algorithm

Especifica un algoritmo para ESP o AH. Cada algoritmo requiere una clave de una longitud específica.

Los algoritmos de autenticación incluyen MD5 y SHA-1. A partir de la versión Solaris 10 4/09, SHA256 y SHA512 son compatibles. Los algoritmos de cifrado incluyen DES, 3DES, AES y Blowfish.

random-hex-string-of-algorithm-specified-length

Especifica un número hexadecimal aleatorio de la longitud que requiere el algoritmo. Por ejemplo, el algoritmo MD5 requiere una cadena de 32 caracteres para su clave de 128 bits. El algoritmo 3DES requiere una cadena de 48 caracteres para su clave de 192 bits.

a. Por ejemplo, en el sistema **enigma**, proteja los paquetes salientes.

Utilice los números aleatorios que haya generado en el paso [Paso 1](#).

Para Solaris 10 1/06:

```
> add esp spi 0x8bcd1407 \  
src 192.168.116.16 dst 192.168.13.213 \  
encr_alg aes \  
auth_alg sha1 \  
encrkey c0c65b888c2ee301c84245c3da63127e92b2676105d5330e85327c1442f37d49 \  
authkey 6fab07fec4f289544500ed992ab48835b9286ff  
>
```

Nota – El sistema equivalente debe utilizar el mismo material de claves y el mismo SPI.

b. Continúe en modo de comando ipseckey en el sistema enigma y proteja los paquetes entrantes.

Escriba los siguientes comandos para proteger los paquetes:

```
> add esp spi 0x122a43e4 \  
src 192.168.13.213 dst 192.168.116.16 \  
encr_alg aes \  
auth_alg sha1 \  
encrkey a2ea934cd62ca7fa14907cb2ad189b68e4d18c976c14f22b30829e4b1ea4d2ae \  
authkey c80984bc4733cc0b7c228b9b74b988d2b7467745  
>
```

Nota – Las claves y el SPI pueden ser diferentes para cada SA. *Debe* asignar claves y SPI distintos para cada SA.

7 Para salir del modo de comando ipseckey, pulse Control-D o escriba quit.

8 Agregue, el material de claves al archivo /etc/inet/secret/ipseckeys.

En las versiones anteriores a Solaris 10 4/09 este paso garantiza que el material de claves está disponible para IPsec al reiniciar.

Las líneas del archivo /etc/inet/secret/ipseckeys son idénticas al lenguaje de la línea de comandos ipseckey.

a. Por ejemplo, el archivo /etc/inet/secret/ipseckeys del sistema enigma tendría un aspecto similar al siguiente:

```
# ipseckeys - This file takes the file format documented in  
# ipseckey(1m).  
# Note that naming services might not be available when this file  
# loads, just like ipsecinit.conf.  
#  
# for outbound packets on enigma  
add esp spi 0x8bcd1407 \  
src 192.168.116.16 dst 192.168.13.213 \  
encr_alg aes \  
auth_alg sha1 \  
encrkey c0c65b888c2ee301c84245c3da63127e92b2676105d5330e85327c1442f37d49 \  
authkey 6fab07fec4f289544500ed992ab48835b9286ff
```

```
#
# for inbound packets
add esp spi 0x122a43e4 \
  src 192.168.13.213 dst 192.168.116.16 \
  encr_alg aes \
  auth_alg sha1 \
  encrkey a2ea934cd62ca7fa14907cb2ad189b68e4d18c976c14f22b30829e4b1ea4d2ae \
  authkey c80984bc4733cc0b7c228b9b74b988d2b7467745
```

b. Proteja el archivo con permisos de sólo lectura.

```
# chmod 400 /etc/inet/secret/ipseckeys
```

9 Repita el procedimiento en el sistema partym.

Utilice el mismo material de claves que utilizó en *enigma*.

El material de claves de los dos sistemas *debe* ser idéntico. Tal como se muestra en el ejemplo siguiente, sólo los comentarios de `ipseckeys` son distintos. Los comentarios difieren porque `dst enigma` entra en el sistema *enigma* y sale del sistema *partym*.

```
# partym ipseckeys file
#
# for inbound packets
add esp spi 0x8bcd1407 \
  src 192.168.116.16 dst 192.168.13.213 \
  encr_alg aes \
  auth_alg sha1 \
  encrkey c0c65b888c2ee301c84245c3da63127e92b2676105d5330e85327c1442f37d49 \
  authkey 6fab07fec4f2895445500ed992ab48835b9286ff
#
# for outbound packets
add esp spi 0x122a43e4 \
  src 192.168.13.213 dst 192.168.116.16 \
  encr_alg aes \
  auth_alg sha1 \
  encrkey a2ea934cd62ca7fa14907cb2ad189b68e4d18c976c14f22b30829e4b1ea4d2ae \
  authkey c80984bc4733cc0b7c228b9b74b988d2b7467745
```

10 Habilite el servicio `manual-key`.

```
# svcadm enable svc:/network/ipsec/manual-key
```

Para sustituir las claves de la versión actual, consulte el [Ejemplo 20–4](#).

Ejemplo 20–4 Sustitución de SA de IPsec

En este ejemplo, el administrador está configurando un sistema que ejecuta la versión Solaris 10 actual. El administrador genera nuevas claves, cambia la información sobre claves en el archivo `ipseckeys` y reinicia el servicio.

- En primer lugar, el administrador completa “[Cómo generar números aleatorios en un sistema Solaris](#)” en la [página 519](#) para generar las claves.
- A continuación, el administrador utiliza las claves generadas en el archivo `/etc/inet/secret/ipseckeys`.

El administrador ha utilizado los mismos algoritmos. Por tanto, el administrador cambia los valores de SPI, encrkey y authkey únicamente:

```
add esp spi 0x8xzy1492 \
src 192.168.116.16 dst 192.168.13.213 \
encr_alg aes \
auth_alg sha1 \
encrkey 0a1f3886b06ebd7d39f6f89e4c29c93f2741c6fa598a38af969907a29ab1b42a \
authkey a7230aabf513f35785da73e33b064608be41f69a
#
# add esp spi 0x177xce34\
src 192.168.13.213 dst 192.168.116.16 \
encr_alg aes \
auth_alg sha1 \
encrkey 4ef5be40bf93498017b2151d788bb37e372f091add9b11149fba42435fefe328 \
authkey 0e1875d9ff8e42ab652766a5cad49f38c9152821
# svcadm restart manual-key
```

- Por último, el administrador reinicia el servicio manual-key. El comando de reinicio borra las claves anteriores antes de agregar las nuevas.

▼ Cómo verificar que los paquetes estén protegidos con IPsec

Para verificar que los paquetes estén protegidos, pruebe la conexión con el comando snoop. Los prefijos siguientes pueden aparecer en el resultado de snoop:

- AH: prefijo que indica que AH está protegiendo los encabezados. El prefijo AH: aparece si se utiliza auth_alg para proteger el tráfico.
- ESP: prefijo que indica que se están enviando los datos cifrados. ESP: aparece si se utiliza encr_auth_alg o encr_alg para proteger el tráfico.

Antes de empezar

Debe ser superusuario o asumir un rol equivalente para crear el resultado snoop. Para poder probar la conexión, es preciso tener acceso a ambos sistemas.

1 Conviértase en superusuario en un sistema, por ejemplo partym.

```
% su -
Password:      Type root password
#
```

2 En el sistema partym, prepárese para buscar paquetes desde un sistema remoto.

En una ventana de terminal en partym, busque los paquetes desde el sistema enigma.

```
# snoop -v enigma
Using device /dev/hme (promiscuous mode)
```

3 Envíe un paquete desde el sistema remoto.

En otra ventana de terminal, inicie sesión remotamente en el sistema enigma. Facilite su contraseña. A continuación, conviértase en superusuario y envíe un paquete del sistema enigma al sistema partym. El paquete debe capturarse mediante el comando snoop -v enigma.

```
% ssh enigma
Password:      Type your password
% su -
Password:      Type root password
# ping partym
```

4 Examine el resultado de snoop.

En el sistema partym, debería ver el resultado que incluye la información de AH y ESP tras la información de encabezado IP inicial. Aparecerá información de AH y ESP que muestra que se están protegiendo los paquetes:

```
IP:   Time to live = 64 seconds/hops
IP:   Protocol = 51 (AH)
IP:   Header checksum = 4e0e
IP:   Source address = 192.168.116.16, enigma
IP:   Destination address = 192.168.13.213, partym
IP:   No options
IP:
AH:   ----- Authentication Header -----
AH:
AH:   Next header = 50 (ESP)
AH:   AH length = 4 (24 bytes)
AH:   <Reserved field = 0x0>
AH:   SPI = 0xb3a8d714
AH:   Replay = 52
AH:   ICV = c653901433ef5a7d77c76eaa
AH:
ESP:   ----- Encapsulating Security Payload -----
ESP:
ESP:   SPI = 0xd4f40a61
ESP:   Replay = 52
ESP:   ....ENCRYPTED DATA....

ETHER:  ----- Ether Header -----
...
```

▼ Cómo configurar una función para la seguridad de la red

Si está utilizando RBAC (Role-Based Access Control) para administrar los sistemas, siga este procedimiento para proporcionar una función de administración de red o de seguridad de red.

1 Busque los perfiles de derechos de red en la base de datos `prof_attr` local.

En la versión actual, aparece una salida similar a la siguiente:

```
% cd /etc/security
% grep Network prof_attr
Network IPsec Management:::Manage IPsec and IKE...
Network Link Security:::Manage network link security...
Network Management:::Manage the host and network configuration...
Network Security:::Manage network and host security...
Network Wifi Management:::Manage wifi network configuration...
Network Wifi Security:::Manage wifi network security...
```

Si está ejecutando una versión anterior a Solaris 10 4/09, la salida presenta un aspecto parecido al siguiente:

```
% cd /etc/security
% grep Network prof_attr
Network Management:::Manage the host and network configuration
Network Security:::Manage network and host security
System Administrator::: Network Management
```

El perfil de administración de red es un perfil complementario del perfil de administrador de sistemas. Si ha incluido el perfil de derechos de administrador de sistemas en un rol, dicho rol podrá ejecutar los comandos del perfil de administración de red.

2 Determine qué comandos hay disponibles en el perfil de derechos de administración de red.

```
% grep "Network Management" /etc/security/exec_attr
Network Management:solaris:cmd:::/usr/sbin/ifconfig:privs=sys_net_config
...
Network Management:suser:cmd:::/usr/sbin/snoop:uid=0
```

Los comandos de directiva `solaris` se ejecutan con privilegio (`privs=sys_net_config`). Los comandos de directiva `suser` se ejecutan como superusuario (`uid=0`).

3 Decida el ámbito de las funciones de seguridad de la red en su sitio.

Utilice las definiciones de los perfiles de derechos en el [Paso 1](#) para guiar la decisión.

- Para crear una función que administre toda la seguridad de la red, utilice el perfil de derechos de la seguridad de la red.
- En la versión actual, para crear una función que administre sólo IPsec e IKE, utilice el perfil de derechos de gestión de red IPsec.

4 Cree un rol de seguridad de red que incluya el perfil de derechos de gestión de la red.

Una función con el perfil de derechos de gestión de red IPsec o de seguridad de la red, además del perfil de gestión de la red, puede ejecutar los comandos `ifconfig`, `snoop`, `ipseconf` e `ipseckey`, entre otros, con privilegios adecuados.

Para crear el rol, asígnelo a un usuario y registre los cambios con el servicio de nombres, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

Ejemplo 20-5 División de responsabilidades de seguridad de la red entre las funciones

En este ejemplo, el administrador divide las responsabilidades de seguridad de la red entre dos funciones. Una función administra wifi y seguridad de los vínculos; otra administra IPsec e IKE. Cada función está asignada a tres personas, una por turno.

El administrador crea las funciones como se indica a continuación:

- El administrador asigna el nombre de LinkWifi a la primera función.
 - El administrador asigna los perfiles de derechos wifi de red, seguridad de vínculos de red y gestión de red a la función.
 - A continuación, el administrador asigna la función LinkWifi a los usuarios pertinentes.
- El administrador asigna el nombre de IPsec Administrator a la segunda función.
 - El administrador asigna los perfiles de derechos de gestión de red IPsec y de gestión de red a la función.
 - A continuación, el administrador asigna la función de administrador de IPsec a los usuarios pertinentes.

▼ Cómo administrar servicios de IPsec e IKE

Los siguientes pasos ofrecen los usos más probables de los servicios SMF para IPsec, IKE y la gestión manual de claves. Por defecto, los servicios `policy` e `ipsecalgs` están habilitados. También por defecto, los servicios `ike` y `manual-key` están deshabilitados.

1 Para administrar la directiva IPsec, lleve a cabo una de las siguientes acciones:

- Después de agregar nuevas directivas al archivo `ipsecinit.conf`, actualice el servicio `policy`.

```
# svcadm refresh svc:/network/ipsec/policy
```
- Tras cambiar el valor de una propiedad de servicio, consulte el valor de la propiedad y, a continuación, actualice y reinicie el servicio `policy`.

```
# svccfg -s policy setprop config/config_file=/etc/inet/MyIpsecinit.conf
# svcprop -p config/config_file policy
/etc/inet/MyIpsecinit.conf
# svcadm refresh svc:/network/ipsec/policy
# svcadm restart svc:/network/ipsec/policy
```

2 Para administrar claves automáticamente, realice una de las siguientes acciones:

- Después de agregar entradas al archivo `/etc/inet/ike/config`, habilite el servicio `ike`.

```
# svcadm enable svc:/network/ipsec/ike
```


- Después de cambiar las entradas en el archivo `/etc/inet/ike/config`, actualice el servicio `ike`.

```
# svcadm refresh svc:/network/ipsec/ike
```

- Tras cambiar el valor de una propiedad de servicio, consulte el valor de la propiedad y, a continuación, actualice el servicio y reinícielo.

```
# svccfg -s ike setprop config/admin_privilege=modkeys
# svcprop -p config/admin_privilege ike
modkeys
# svcadm refresh svc:/network/ipsec/ike
# svcadm restart svc:/network/ipsec/ike
```

- Para detener el servicio `ike`, deshabilítelo.

```
# svcadm disable svc:/network/ipsec/ike
```

3 Para administrar claves manualmente, lleve a cabo una de las siguientes acciones:

- Después de agregar entradas al archivo `/etc/inet/secret/ipseckey`, habilite el servicio `manual-key`.

```
# svcadm enable svc:/network/ipsec/manual-key
```

- Después de cambiar el archivo `ipseckey`, actualice el servicio.

```
# svcadm refresh manual-key
```

- Tras cambiar el valor de una propiedad de servicio, consulte el valor de la propiedad y, a continuación, actualice el servicio y reinícielo.

```
# svccfg -s manual-key setprop config/config_file=/etc/inet/secret/MyIpseckeyfile
# svcprop -p config/config_file manual-key
/etc/inet/secret/MyIpseckeyfile
# svcadm refresh svc:/network/ipsec/manual-key
# svcadm restart svc:/network/ipsec/manual-key
```

- Para impedir la gestión manual de claves, deshabilite el servicio `manual-key`.

```
# svcadm disable svc:/network/ipsec/manual-key
```

4 Si modifica la tabla de algoritmos y los protocolos IPsec, actualice el servicio `ipsecalgs`.

```
# svcadm refresh svc:/network/ipsec/ipsecalgs
```

Errores más frecuentes

Utilice el comando `svcs service` para buscar el estado de un servicio. Si el servicio está en el modo `maintenance`, siga las sugerencias de depuración en la salida del comando `svcs -x servicio`.

Protección de una VPN con IPsec

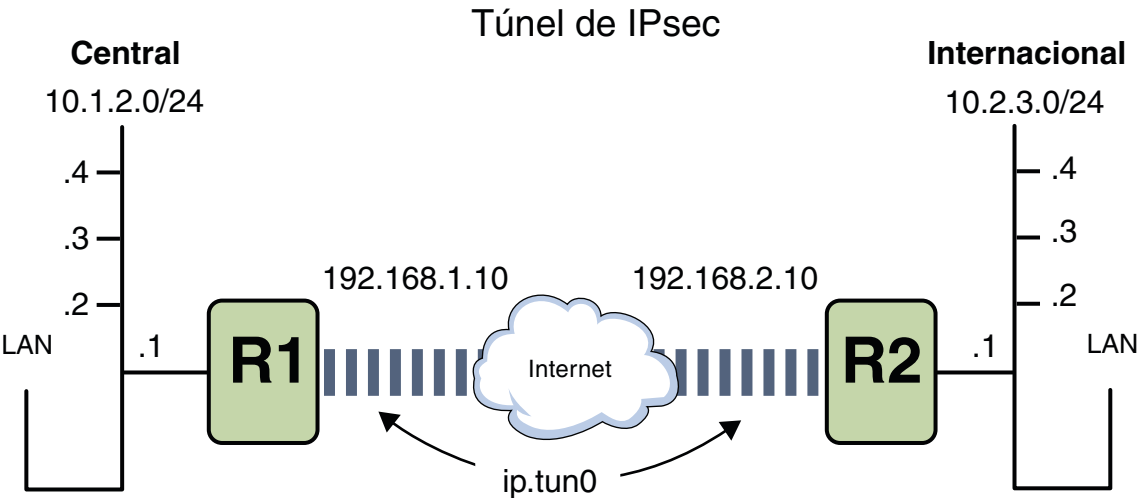
Los túneles de IPsec pueden proteger una VPN. En la versión Solaris 10 7/07, un túnel puede estar en modo de túnel o de transporte. El *modo de túnel* es interoperable con la implementación de IPsec por parte de otros proveedores. El *modo de transporte* es interoperable con las versiones anteriores de SO Solaris. Para ver una descripción de los modos de túnel, consulte [“Modos de transporte y túnel en IPsec” en la página 499](#).

Los túneles en modo túnel ofrecen un control más preciso del tráfico. En modo túnel, para ver una dirección IP interna, puede especificar la protección concreta que desee, hasta alcanzar un único puerto.

- Para ver ejemplos de las directivas de IPsec para los túneles en modo túnel, consulte [“Ejemplos de protección de una VPN con IPsec mediante el uso de túneles en modo túnel” en la página 530](#).
- Para ver los procedimientos que protegen las VPN, consulte [“Protección de una VPN con IPsec \(mapa de tareas\)” en la página 532](#).

Ejemplos de protección de una VPN con IPsec mediante el uso de túneles en modo túnel

FIGURA 20-1 Diagrama de túnel de IPsec



Los ejemplos siguientes presuponen que el túnel se ha configurado para todas las subredes de la LAN:

```
## Tunnel configuration ##
# Tunnel name is ip.tun0
# Intranet point for the source is 10.1.2.1
# Intranet point for the destination is 10.2.3.1
# Tunnel source is 192.168.1.10
# Tunnel destination is 192.168.2.10
```

EJEMPLO 20-6 Creación de un túnel que puedan utilizar todas las subredes

En este ejemplo, se puede crear un túnel de todo el tráfico de las redes LAN locales de la red LAN central de la [Figura 20-1](#) del enrutador 1 al 2 y, a continuación, transferirlo a todas las redes LAN locales de la red LAN internacional. El tráfico se cifra con AES.

```
## IPsec policy ##
{tunnel ip.tun0 negotiate tunnel}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

EJEMPLO 20-7 Creación de un túnel que sólo conecta dos subredes

En este ejemplo, sólo se crea un túnel y se cifra el tráfico entre la subred 10.1.2.0/24 de la LAN central y la subred 10.2.3.0/24 de la LAN internacional. En caso de no haber otras directivas IPsec para Central, si la LAN central intenta enrutar el tráfico para otras LAN por este túnel, el tráfico se transferirá al enrutador 1.

```
## IPsec policy ##
{tunnel ip.tun0 negotiate tunnel laddr 10.1.2.0/24 raddr 10.2.3.0/24}
  ipsec {encr_algs aes encr_auth_algs md5 sha1 shared}
```

EJEMPLO 20-8 Creación de un túnel sólo para el tráfico de correo electrónico entre dos subredes

En este ejemplo, se crea un túnel sólo para el tráfico de correo electrónico. El tráfico se transfiere de la subred 10.1.2.0/24 de la LAN central al servidor de correo electrónico de la subred 10.2.3.0/24 de la LAN internacional. El correo electrónico se cifra con Blowfish. Las directivas se aplican a los puertos de correo electrónico remoto y local. La directiva rport protege el correo electrónico que Central envía al puerto de correo electrónico remoto de Internacional. La directiva lport protege el correo electrónico que Central recibe de Internacional en el puerto local 25.

```
## IPsec policy for email from Central to Overseas ##
{tunnel ip.tun0 negotiate tunnel ulp tcp rport 25
  laddr 10.1.2.0/24 raddr 10.2.3.0/24}
  ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}

## IPsec policy for email from Overseas to Central ##
{tunnel ip.tun0 negotiate tunnel ulp tcp lport 25
  laddr 10.1.2.0/24 raddr 10.2.3.0/24}
  ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}
```

EJEMPLO 20-9 Creación de un túnel para el tráfico FTP para todas las subredes

En este ejemplo, la directiva IPsec protege los puertos FTP de la [Figura 20-1](#) con AES para todas las subredes de la red LAN central a todas las subredes de la red LAN internacional. Esta configuración funciona para el modo activo de FTP.

```
## IPsec policy for outbound FTP from Central to Overseas ##
{tunnel ip.tun0 negotiate tunnel ulp tcp rport 21}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
{tunnel ip.tun0 negotiate tunnel ulp tcp lport 20}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## IPsec policy for inbound FTP from Central to Overseas ##
{tunnel ip.tun0 negotiate tunnel ulp tcp lport 21}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
{tunnel ip.tun0 negotiate tunnel ulp tcp rport 20}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Protección de una VPN con IPsec (mapa de tareas)

El mapa de tareas siguiente indica procedimientos que configuran IPsec para la protección del tráfico por Internet. Estos procedimientos configuran una red privada virtual (VPN) entre dos sistemas separados por Internet. Un uso común de esta tecnología es proteger el tráfico entre los trabajadores remotos y su oficina corporativa.

Tarea	Descripción	Para obtener instrucciones
Proteger el tráfico de túnel en modo túnel por IPv4.	Protege el tráfico en modo túnel entre dos sistemas Solaris 10, dos sistemas Oracle Solaris o entre un sistema Solaris 10 y un sistema Oracle Solaris Express. El sistema Solaris 10 debe ejecutar como mínimo la versión Solaris 10 7/07. Asimismo, protege el tráfico en modo túnel entre un sistema Solaris 10 o un sistema Oracle Solaris Express y un sistema que se ejecuta en otra plataforma. El sistema Solaris 10 debe ejecutar como mínimo la versión Solaris 10 7/07.	“Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4” en la página 535
Proteger el tráfico de túnel en modo túnel por IPv6.	Protege el tráfico en modo túnel entre dos sistemas Oracle Solaris que utilizan el protocolo IPv6.	“Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv6” en la página 545

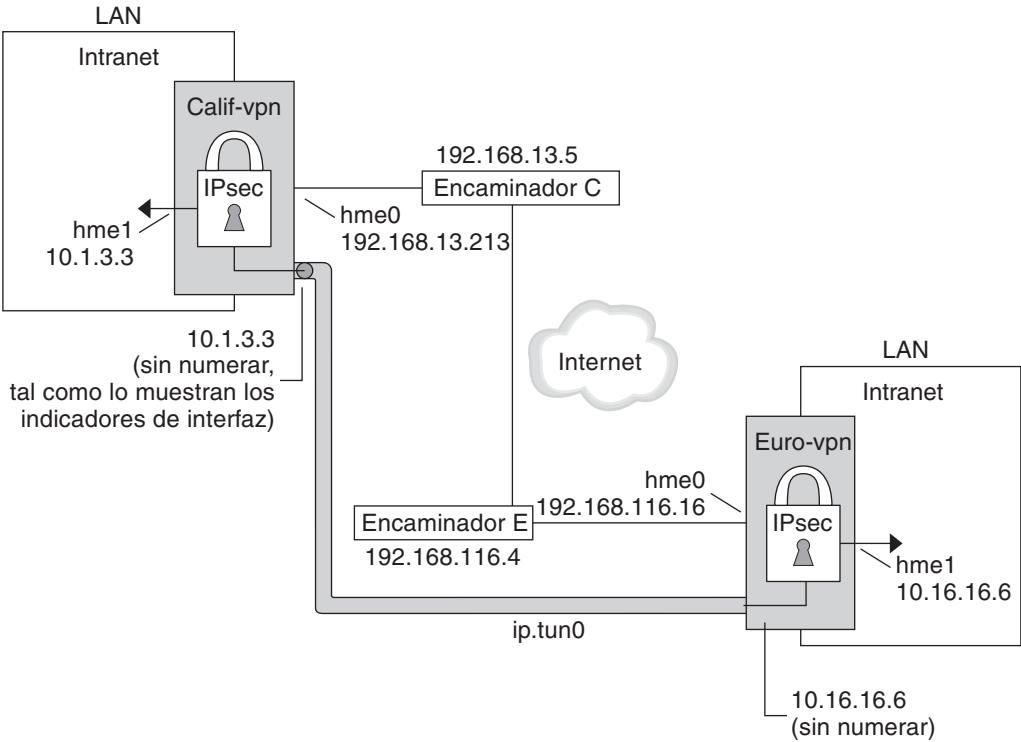
Tarea	Descripción	Para obtener instrucciones
Proteger el tráfico de túnel en modo de transporte por IPv4.	Protege el tráfico en modo transporte entre dos sistemas Solaris 10, dos sistemas Solaris o entre un sistema Solaris 10 y un sistema Oracle Solaris. El sistema Solaris 10 debe ejecutar como mínimo la versión Solaris 10 7/07.	“Cómo proteger una VPN con un túnel IPsec en modo transporte mediante IPv4” en la página 551
	Además, protege el tráfico en modo transporte entre un sistema que ejecuta una versión anterior de SO Solaris y Solaris 10 o un sistema Oracle Solaris. El sistema Solaris 10 debe ejecutar como mínimo la versión Solaris 10 7/07.	Ejemplo 20–11 Ejemplo 20–16
Proteger el tráfico de túnel en modo transporte por IPv6.	Protege el tráfico en modo transporte entre dos sistemas Oracle Solaris que utilizan el protocolo IPv6.	“Cómo proteger una VPN con un túnel IPsec en modo transporte mediante IPv6” en la página 557
Evitar la falsificación de la IP.	Crea un servicio SMF para evitar que el sistema reenvíe paquetes a través de una VPN sin descifrarlos.	“Cómo evitar la falsificación de la IP” en la página 563

Descripción de la topología de red para la protección de una VPN por parte de las tareas de IPsec

Los procedimientos que se describen a continuación presuponen la siguiente configuración. Para ver una representación de la red, consulte la [Figura 20–2](#).

- Cada sistema utiliza un espacio de dirección IPv4.
Para ver un ejemplo similar con direcciones IPv6, consulte [“Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv6” en la página 545](#).
- Cada sistema cuenta con dos interfaces. La interfaz hme0 se conecta a Internet. En este ejemplo, las direcciones IP de Internet empiezan por 192 . 168. La interfaz hme1 se conecta a la LAN de la compañía, es decir, a su intranet. En este ejemplo, las direcciones IP de la intranet empiezan por el número 10.
- Cada sistema requiere autenticación ESP con el algoritmo SHA-1. El algoritmo SHA-1 requiere una clave de 160 bits.
- Cada sistema requiere cifrado ESP con el algoritmo AES. El algoritmo AES utiliza una clave de 128 o 256 bits.
- Cada sistema puede conectarse a un enrutador que tenga acceso directo a Internet.
- Cada sistema utiliza asociaciones de seguridad compartidas.

FIGURA 20-2 VPN de ejemplo entre oficinas separadas por Internet



hme0 = Desactivar reenvío de IP

hme0 = Activar reenvío de IP

ip.tun0 = Activar reenvío de IP

Encaminador C - /etc/defaultrouter for Calif-vpn

Encaminador E - /etc/defaultrouter for Euro-vpn

Como muestra la ilustración anterior, los procedimientos para la red IPv4 utilizan los siguientes parámetros de configuración.

Parámetro	Europa	California
Nombre del sistema	enigma	partym
Interfaz de la intranet del sistema	hme1	hme1

Parámetro	Europa	California
La dirección de intranet del sistema, también la dirección <i>-punto</i> en el Paso 7	10.16.16.6	10.1.3.3
Interfaz de Internet del sistema	hme0	hme0
Dirección de Internet del sistema, también la dirección <i>tsrc</i> en el Paso 7	192.168.116.16	192.168.13.213
Nombre del enrutador de Internet	router-E	router-C
Dirección del enrutador de Internet	192.168.116.4	192.168.13.5
Nombre de túnel	ip.tun0	ip.tun0

Las siguientes direcciones IPv6 se utilizan en los procedimientos. Los nombres de túnel son los mismos.

Parámetro	Europa	California
Dirección de intranet del sistema	6000:6666::aaaa:1116	6000:3333::eeee:1113
Dirección de Internet del sistema	2001::aaaa:6666:6666	2001::eeee:3333:3333
Dirección del enrutador de Internet	2001::aaaa:0:4	2001::eeee:0:1

▼ Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4

En modo túnel, el paquete IP interior determina la directiva IPsec que protege su contenido.

Este procedimiento amplía el procedimiento de [“Cómo proteger el tráfico entre dos sistemas con IPsec” en la página 511](#). El procedimiento de configuración se describe en [“Descripción de la topología de red para la protección de una VPN por parte de las tareas de IPsec” en la página 533](#).

Nota – Lleve a cabo los pasos de este procedimiento en ambos sistemas.

Además de conectar dos sistemas, está conectando dos intranets que se conectan a estos dos sistemas. Los sistemas de este procedimiento actúan como portales.

Antes de empezar

Debe estar en la zona global para configurar la directiva IPsec para el sistema o para una zona de IP compartida. Para una zona de IP exclusiva, configure la directiva IPsec en la zona no global.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Controle el flujo de paquetes antes de configurar IPsec.

a. Asegúrese de que el reenvío de IP y el enrutamiento dinámico de IP estén deshabilitados.

```
# routeadm
Configuration      Current      Current
      Option      Configuration System State
-----
IPv4 forwarding    disabled          disabled
      IPv4 routing default (enabled)  enabled
...
```

Si el reenvío de IP y el encaminamiento dinámico de IP están activos, deshabilítelos.

```
# routeadm -d ipv4-routing -d ipv4-forwarding
# routeadm -u
```

La desactivación del reenvío de IP impide que los paquetes se envíen de una red a otra a través de este sistema. Para ver una descripción del comando `routeadm`, consulte la página del comando `man routeadm(1M)`.

b. Active los hosts múltiples de destino estricto de IP.

```
# ndd -set /dev/ip ip_strict_dst_multihoming 1
```

La activación de los hosts múltiples de destino estricto de IP garantiza que los paquetes de una de las direcciones de destino del sistema lleguen a la dirección de destino correcta.

Cuando está habilitada la función de hosts múltiples de destino estricto, los paquetes que alcanzan una determinada interfaz deben dirigirse a una de las direcciones IP locales de dicha interfaz. Todos los demás paquetes, incluidos los que se dirigen a otras direcciones locales del sistema, se eliminan.



Precaución – El valor de host múltiple vuelve al predeterminado cuando se inicia el sistema. Para hacer que el valor cambiado sea persistente, consulte [“Cómo evitar la falsificación de la IP” en la página 563](#).

c. Deshabilite la mayoría de los servicios de red, y posiblemente todos.

Nota – Si su sistema se instaló con el perfil SMF "limitado", puede omitir este paso. Los servicios de red se deshabilitan, a excepción de Solaris Secure Shell.

La desactivación de los servicios de red evita que los paquetes IP dañen el sistema. Por ejemplo, podrían aprovecharse un daemon SNMP, una conexión telnet o una conexión rlogin.

Elija una de las siguientes opciones:

- Si ejecuta Solaris 10 11/06 o una versión posterior, ejecute el perfil SMF "limitado".

```
# netservices limited
```

- De lo contrario, deshabilite los servicios de red de forma individual.

```
# svcadm disable network/ftp:default
# svcadm disable network/finger:default
# svcadm disable network/login:rlogin
# svcadm disable network/nfs/server:default
# svcadm disable network/rpc/rstat:default
# svcadm disable network/smtp:sendmail
# svcadm disable network/telnet:default
```

d. Compruebe que la mayoría de los servicios de red estén deshabilitados.

Compruebe que los montajes de realimentación y el servicio ssh se estén ejecutando.

```
# svcs | grep network
online      Aug_02   svc:/network/loopback:default
...
online      Aug_09   svc:/network/ssh:default
```

3 Agregue un par de SA entre los dos sistemas.

Elija una de las siguientes opciones:

- Configure IKE para administrar las claves para las SA. Utilice uno de los procedimientos de “[Configuración de IKE \(mapa de tareas\)](#)” en la página 583 para configurar IKE para la VPN.
- Si tiene motivos para administrar las claves manualmente, consulte “[Cómo crear manualmente asociaciones de seguridad IPsec](#)” en la página 520.

4 Agregue la directiva IPsec.

Edite el archivo `/etc/inet/ipsecinit.conf` para agregar la directiva IPsec para la VPN. Para reforzar la directiva, consulte el [Ejemplo 20–12](#). Para ver ejemplos adicionales, consulte “[Ejemplos de protección de una VPN con IPsec mediante el uso de túneles en modo túnel](#)” en la página 530.

En esta directiva, la protección IPsec no se necesita entre sistemas de la LAN local y la dirección IP del servidor de seguridad, de modo que se agrega una instrucción `bypass`.

a. En el sistema `enigma`, escriba la entrada siguiente en el archivo `ipsecinit.conf`:

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.16.16.6 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate tunnel}
ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. En el sistema `partym`, escriba la entrada siguiente en el archivo `ipsecinit.conf`:

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate tunnel}
ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

5 (Opcional) Compruebe la sintaxis del archivo de directiva IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 Para configurar el túnel y protegerlo con IPsec, siga los pasos en función de la versión de Solaris:

- A partir de la versión Solaris 10 4/09, siga los pasos del [Paso 7](#) al [Paso 13](#) y, a continuación, ejecute el protocolo de enrutamiento en el [Paso 22](#).
- Si está ejecutando una versión anterior a Solaris 10 4/09, siga las indicaciones del [Paso 14](#) al [Paso 22](#).

7 Configure el túnel, `ip.tun0` en el archivo `/etc/hostname.ip.tun0`.

La sintaxis del archivo es la siguiente:

```
system1-point system2-point tsrc system1-taddr tdst system2-taddr router up
```

a. En el sistema `enigma`, agregue la entrada siguiente al archivo `hostname.ip.tun0`:

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 tdst 192.168.13.213 router up
```

b. En el sistema `partym`, agregue la entrada siguiente al archivo `hostname.ip.tun0`:

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 tdst 192.168.116.16 router up
```

8 Proteja el túnel con la directiva IPsec que ha creado.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9 Para leer el contenido del archivo de configuración de túnel en el núcleo, reinicie los servicios de red.

```
# svcadm restart svc:/network/initial:default
```

10 Active el reenvío de IP para la interfaz hme1.

- a. En el sistema *enigma*, agregue la entrada del enrutador al archivo `/etc/hostname.hme1`.

```
192.168.116.16 router
```

- b. En el sistema *partym*, agregue la entrada del enrutador al archivo `/etc/hostname.hme1`.

```
192.168.13.213 router
```

El reenvío de IP significa que los paquetes que llegan desde cualquier parte se pueden reenviar. El reenvío de IP también significa que los paquetes que abandonan esta interfaz podrían haberse originado en cualquier otra parte. Para reenviar un paquete correctamente, tanto la interfaz receptora como la de transmisión deben tener activa la opción de reenvío de IP.

Dado que la interfaz *hme1* está *dentro* de la intranet, el reenvío de IP debe estar activo para *hme1*. Dado que *ip.tun0* conecta los dos sistemas a través de Internet, el reenvío de IP debe estar activo para *ip.tun0*.

La interfaz *hme0* tiene su propio reenvío de IP desactivado para evitar que un adversario *externo* inserte paquetes en la intranet protegida. El término *externo* hace referencia a Internet.

11 Asegúrese de que los protocolos de enrutamiento no publiquen la ruta predeterminada en la intranet.

- a. En el sistema *enigma*, agregue el indicador *private* al archivo `/etc/hostname.hme0`.

```
10.16.16.6 private
```

- b. En el sistema *partym*, agregue el indicador *private* al archivo `/etc/hostname.hme0`.

```
10.1.3.3 private
```

Aunque *hme0* tenga el reenvío de IP desactivado, la implementación de un protocolo de enrutamiento podría seguir publicando la interfaz. Por ejemplo, el protocolo *in.routed* podría seguir anunciando que *hme0* está disponible para reenviar paquetes a sus equivalentes dentro de la intranet. Al configurar el indicador *private* de la interfaz, se evita la publicación de estos datos.

12 Agregue manualmente una ruta predeterminada a través de la interfaz hme0.

La ruta predeterminada debe ser un enrutador con acceso directo a Internet.

- a. En el sistema *enigma*, agregue la ruta siguiente:

```
# route add default 192.168.116.4
```

- b. En el sistema *partym* agregue la siguiente ruta:

```
# route add default 192.168.13.5
```

Aunque la interfaz *hme0* no forme parte de la intranet, *hme0* necesita alcanzar su sistema equivalente a través de Internet. Para encontrar su equivalente, *hme0* necesita información sobre el enrutamiento de Internet. El sistema VPN aparece como host, en lugar de aparecer

como enrutador, para el resto de Internet. Por tanto, puede utilizar un enrutador predeterminado o ejecutar el protocolo de descubrimiento de enrutador para encontrar un sistema equivalente. Para más información, consulte las páginas del comando `man route(1M)` e `in.routed(1M)`.

13 Para completar el procedimiento, vaya al Paso 22 para ejecutar un protocolo de enrutamiento.

14 Configure el túnel `ip.tun0`.

Nota – Los siguientes pasos configuran un túnel en un sistema que esté ejecutando una versión anterior a Solaris 10 4/09.

Utilice los comandos `ifconfig` para crear la interfaz de punto a punto:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 system1-point system2-point \
tsrc system1-taddr tdst system2-taddr
```

a. En el sistema `enigma`, escriba los comandos siguientes:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213
```

b. En el sistema `partym`, escriba los comandos siguientes:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.1.3.3 10.16.16.6 \
tsrc 192.168.13.213 tdst 192.168.116.16
```

15 Proteja el túnel con la directiva IPsec que ha creado.

```
# ipsecconf
```

16 Muestre el enrutador para el túnel.

```
# ifconfig ip.tun0 router up
```

17 Active el reenvío de IP para la interfaz `hme1`.

```
# ifconfig hme1 router
```

El reenvío de IP significa que los paquetes que llegan desde cualquier parte se pueden reenviar. El reenvío de IP también significa que los paquetes que abandonan esta interfaz podrían haberse originado en cualquier otra parte. Para reenviar un paquete correctamente, tanto la interfaz receptora como la de transmisión deben tener activa la opción de reenvío de IP.

Puesto que la interfaz `hme1` está *dentro* de la intranet, el reenvío de IP debe estar activo para `hme1`. Dado que `ip.tun0` conecta los dos sistemas a través de Internet, el reenvío de IP debe estar activo para `ip.tun0`.

La interfaz `hme0` tiene su propio reenvío de IP desactivado para evitar que un adversario *externo* inserte paquetes en la intranet protegida. El término *externo* hace referencia a Internet.

18 Asegúrese de que los protocolos de enrutamiento no publiquen la ruta predeterminada en la intranet.

```
# ifconfig hme0 private
```

Aunque `hme0` tenga el reenvío de IP desactivado, la implementación de un protocolo de enrutamiento podría seguir publicando la interfaz. Por ejemplo, el protocolo `in.routed` podría seguir publicando que `hme0` está disponible para reenviar paquetes a sus equivalentes dentro de la intranet. Al configurar el indicador *private* de la interfaz, se evita la publicación de estos datos.

19 Agregue manualmente una ruta predeterminada a través de `hme0`.

La ruta predeterminada debe ser un enrutador con acceso directo a Internet.

a. En el sistema `enigma`, agregue la ruta siguiente:

```
# route add default 192.168.116.4
```

b. En el sistema `partym`, agregue la ruta siguiente.

```
# route add default 192.168.13.5
```

Aunque la interfaz `hme0` no forme parte de la intranet, `hme0` necesita alcanzar su sistema equivalente a través de Internet. Para encontrar su equivalente, `hme0` necesita información sobre el enrutamiento de Internet. El sistema VPN aparece como host, en lugar de aparecer como enrutador, para el resto de Internet. Por tanto, puede utilizar un enrutador predeterminado o ejecutar el protocolo de descubrimiento de enrutador para encontrar un sistema equivalente. Para más información, consulte las páginas del comando `man route(1M)` e `in.routed(1M)`.

20 Asegúrese de que la VPN se inicie tras un reinicio mediante la adición de una entrada al archivo `/etc/hostname.ip.tun0`.

```
system1-point system2-point tsrc system1-taddr tdst system2-taddr router up
```

a. En el sistema `enigma`, agregue la entrada siguiente al archivo `hostname.ip.tun0`:

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 tdst 192.168.13.213 router up
```

b. En el sistema `partym`, agregue la entrada siguiente al archivo `hostname.ip.tun0`:

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 tdst 192.168.116.16 router up
```

21 Configure los archivos de interfaz para transferir los parámetros correctos al daemon de enrutamiento.

a. En el sistema *enigma*, modifique los archivos */etc/hostname.interfaz*.

```
# cat /etc/hostname.hme0
## enigma
10.16.16.6 private

# cat /etc/hostname.hme1
## enigma
192.168.116.16 router
```

b. En el sistema *partym*, modifique los archivos */etc/hostname.interfaz*.

```
# cat /etc/hostname.hme0
## partym
10.1.3.3 private

# cat /etc/hostname.hme1
## partym
192.168.13.213 router
```

22 Ejecute un protocolo de enrutamiento.

```
# routeadm -e ipv4-routing
# routeadm -u
```

Podría ser que antes de ejecutar el protocolo de enrutamiento fuese necesario configurarlo. Para obtener más información, consulte [“Protocolos de enrutamiento en Oracle Solaris” en la página 253](#). Para conocer el procedimiento, consulte [“Configuración de un enrutador IPv4” en la página 121](#).

Ejemplo 20–10 Creación de túneles temporales durante la prueba

En este ejemplo, el administrador prueba la creación del túnel en un sistema Solaris 10 4/09. Más tarde, el administrador utilizará el procedimiento [“Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4” en la página 535](#) para que los túneles sean permanentes. Durante la prueba, el administrador realiza las siguientes series de pasos en los sistemas *system1* y *system2*:

- En ambos sistemas, el administrador completa los cinco primeros pasos de [“Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4” en la página 535](#).
- El administrador utiliza el comando `ifconfig` para conectar y configurar un túnel temporal.

```
system1 # ifconfig ip.tun0 plumb
system1 # ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
        tsrc 192.168.116.16 tdst 192.168.13.213

# ssh system2
Password: admin-password-on-system2
```

```
system2 # ifconfig ip.tun0 plumb
system2 # ifconfig ip.tun0 10.1.3.3 10.16.16.6 \
        tsrc 192.168.13.213 tdst 192.168.116.16
```

- El administrador habilita la directiva IPsec en el túnel. La directiva se creó en el [Paso 4](#) de “[Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4](#)” en la página 535.

```
system1 # svcadm refresh svc:/network/ipsec/policy:default
system2 # svcadm refresh svc:/network/ipsec/policy:default
```

- El administrador realiza la interfaz de Internet y evita que los protocolos de enrutamiento pasen a través de la interfaz de la intranet.

```
system1 # ifconfig hme1 router ; ifconfig hme0 private
```

```
system2 # ifconfig hme1 router ; ifconfig hme0 private
```

- El administrador agrega manualmente enrutamiento y ejecuta el protocolo de enrutamiento mediante el [Paso 12](#) y el [Paso 22](#) de “[Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4](#)” en la página 535 en ambos sistemas.

Ejemplo 20–11 Creación de un túnel en una versión anterior de un sistema Solaris mediante la línea de comandos

En la versión Solaris 10 7/07, la sintaxis del comando `ifconfig` se ha simplificado. En este ejemplo, el administrador prueba la creación del túnel en un sistema que está ejecutando una versión de Solaris anterior a Solaris 10 7/07. Mediante la sintaxis original del comando `ifconfig`, el administrador puede utilizar comandos idénticos en los dos sistemas comunicantes. Más tarde, el administrador utilizará “[Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4](#)” en la página 535 para hacer que los túneles sean permanentes.

Durante la prueba, el administrador realiza los pasos siguientes en los sistemas `system1` y `system2`:

- En ambos sistemas, el administrador completa los cinco primeros pasos de “[Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4](#)” en la página 535.
- El administrador conecta y configura el túnel.

```
system1 # ifconfig ip.tun0 plumb
system1 # ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
        tsrc 192.168.116.16 tdst 192.168.13.213 \
        encr_algs aes encr_auth_algs sha1
system1 # ifconfig ip.tun0 router up

# ssh system2
Password:      admin-password-on-system2
system2 # ifconfig ip.tun0 plumb
system2 # ifconfig ip.tun0 10.1.3.3 10.16.16.6 \
        tsrc 192.168.13.213 tdst 192.168.116.16 \
```

```

encr_algs aes encr_auth_algs sha1
system2 # ifconfig ip.tun0 router up

```

- El administrador habilita la directiva IPsec en el túnel. La directiva se creó en el [Paso 4](#) de “Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4” en la página 535.

```

system1 # svcadm refresh svc:/network/ipsec/policy:default
system2 # svcadm refresh svc:/network/ipsec/policy:default

```

- El administrador realiza la interfaz de Internet y evita que los protocolos de enrutamiento pasen a través de la interfaz de la intranet.

```

system1 # ifconfig hme1 router ; ifconfig hme0 private
system2 # ifconfig hme1 router ; ifconfig hme0 private

```

- El administrador agrega enrutamiento mediante la realización del [Paso 12](#) y el [Paso 22](#) de “Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4” en la página 535 en ambos sistemas.

Ejemplo 20-12 Requisito de directiva IPsec en todos los sistemas de una LAN

En este ejemplo, el administrador comenta la directiva `bypass` que se ha configurado en el [Paso 4](#), con lo cual se refuerza la seguridad. Con esta configuración de directiva, cada sistema de la LAN debe activar IPsec para comunicarse con el enrutador.

```

# LAN traffic must implement IPsec.
# {laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate tunnel} ipsec {encr_algs aes encr_auth_algs sha1}

```

Ejemplo 20-13 Uso de IPsec para proteger el tráfico Telnet de un modo distinto del tráfico SMTP

En este ejemplo, la primera regla protege al tráfico `telnet` del puerto 23 con Blowfish y SHA-1. La segunda regla protege al tráfico SMTP del puerto 25 con AES y MD5.

```

{laddr 10.1.3.3 ulp tcp dport 23 dir both}
  ipsec {encr_algs blowfish encr_auth_algs sha1 sa unique}
{laddr 10.1.3.3 ulp tcp dport 25 dir both}
  ipsec {encr_algs aes encr_auth_algs md5 sa unique}

```

Ejemplo 20-14 Uso de un túnel IPsec en modo túnel para proteger una subred de un modo distinto del resto del tráfico de red

La siguiente configuración de túnel protege todo el tráfico de la subred `10.1.3.0/24` a través del túnel:

```

{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

```


Las siguientes configuraciones de túnel protegen el tráfico de la subred 10.1.3.0/24 a distintas subredes a través del túnel. Las subredes que empiezan por 10.2.x.x atraviesan el túnel.

```
{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24 raddr 10.2.1.0/24}
 ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}

{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24 raddr 10.2.2.0/24}
 ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}

{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24 raddr 10.2.3.0/24}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

▼ Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv6

Para configurar una VPN en una red IPv6, debe seguir los mismos pasos que para configurar una red IPv4. No obstante, la sintaxis de los comandos es ligeramente distinta. Para ver una descripción completa de los motivos para ejecutar comandos específicos, consulte los pasos correspondientes en [“Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4” en la página 535](#).

Nota – Lleve a cabo los pasos de este procedimiento en ambos sistemas.

Este procedimiento utiliza los siguientes parámetros.

Parámetro	Europa	California
Nombre del sistema	enigma	partym
Interfaz de la intranet del sistema	hme1	hme1
Interfaz de Internet del sistema	hme0	hme0
Dirección de intranet del sistema	6000:6666::aaaa:1116	6000:3333::eeee:1113
Dirección de Internet del sistema	2001::aaaa:6666:6666	2001::eeee:3333:3333
Nombre del enrutador de Internet	router-E	router-C
Dirección del enrutador de Internet	2001::aaaa:0:4	2001::eeee:0:1
Nombre de túnel	ip6.tun0	ip6.tun0

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Controle el flujo de paquetes antes de configurar IPsec.

Para ver los efectos de estos comandos, consulte el [Paso 2 de “Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4” en la página 535](#).

a. Asegúrese de que el reenvío de IP y el enrutamiento dinámico de IP estén deshabilitados.

# routeadm		
Configuration	Current	Current
Option	Configuration	System State

...		
IPv6 forwarding	disabled	disabled
IPv6 routing	disabled	disabled

Si el reenvío de IP y el enrutamiento dinámico de IP están habilitados, puede deshabilitarlos escribiendo:

```
# routeadm -d ipv6-forwarding -d ipv6-routing
# routeadm -u
```

b. Active los hosts múltiples de destino estricto de IP.

```
# ndd -set /dev/ip ip6_strict_dst_multihoming 1
```



Precaución – El valor de `ip6_strict_dst_multihoming` vuelve al predeterminado cuando se inicia el sistema. Para hacer que el valor cambiado sea persistente, consulte [“Cómo evitar la falsificación de la IP” en la página 563](#).

c. Deshabilite la mayoría de los servicios de red, y posiblemente todos.

Nota – Si su sistema se instaló con el perfil SMF "limitado", puede omitir este paso. Los servicios de red se deshabilitan, a excepción de Solaris Secure Shell.

La desactivación de los servicios de red evita que los paquetes IP dañen el sistema. Por ejemplo, podrían aprovecharse un daemon SNMP, una conexión `telnet` o una conexión `rlogin`.

Elija una de las siguientes opciones:

- Si ejecuta Solaris 10 11/06 o una versión posterior, ejecute el perfil SMF "limitado".

```
# netservices limited
```

- De lo contrario, deshabilite los servicios de red de forma individual.

```
# svcadm disable network/ftp:default
# svcadm disable network/finger:default
# svcadm disable network/login:rlogin
# svcadm disable network/nfs/server:default
# svcadm disable network/rpc/rstat:default
# svcadm disable network/smtp:sendmail
# svcadm disable network/telnet:default
```

d. Compruebe que la mayoría de los servicios de red estén deshabilitados.

Compruebe que los montajes de realimentación y el servicio ssh se estén ejecutando.

```
# svcs | grep network
online      Aug_02   svc:/network/loopback:default
...
online      Aug_09   svc:/network/ssh:default
```

3 Agregue un par de SA entre los dos sistemas.

Elija una de las siguientes opciones:

- Configure IKE para administrar las claves para las SA. Utilice uno de los procedimientos de [“Configuración de IKE \(mapa de tareas\)” en la página 583](#) para configurar IKE para la VPN.
- Si tiene motivos para administrar las claves manualmente, consulte [“Cómo crear manualmente asociaciones de seguridad IPsec” en la página 520](#).

4 Agregue una directiva IPsec para la VPN.

Edita el archivo `/etc/inet/ipsecinit.conf` para agregar la directiva IPsec para la VPN.

a. En el sistema enigma, escriba la entrada siguiente en el archivo `ipsecinit.conf`:

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic to and from this host can bypass IPsec.
{laddr 6000:6666::aaaa:1116 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate tunnel}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. En el sistema partym, escriba la entrada siguiente en el archivo `ipsecinit.conf`:

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic to and from this host can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}
```

```
# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate tunnel}
ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

5 (Opcional) Compruebe la sintaxis del archivo de directiva IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 Para configurar el túnel y protegerlo con IPsec, siga los pasos en función de la versión de Solaris:

- A partir de la versión Solaris 10 4/09, siga los pasos del [Paso 7](#) al [Paso 13](#) y, a continuación, ejecute el protocolo de enrutamiento en el [Paso 22](#).
- Si está ejecutando una versión anterior a Solaris 10 4/09, siga las indicaciones del [Paso 14](#) al [Paso 22](#).

7 Configure el túnel, ip6.tun0 en el archivo /etc/hostname.ip6.tun0.

a. En el sistema enigma agregue la siguiente entrada al archivo hostname.ip6.tun0:

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 tsrsc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 router up
```

b. En el sistema partym, agregue la entrada siguiente al archivo hostname.ip6.tun0:

```
6000:3333::eeee:1113 6000:6666::aaaa:1116 tsrsc 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666 router up
```

8 Proteja el túnel con la directiva IPsec que ha creado.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9 Para leer el contenido del archivo de configuración de túnel en el núcleo, reinicie los servicios de red.

```
# svcadm restart svc:/network/initial:default
```

10 Active el reenvío de IP para la interfaz hme1.

a. En el sistema enigma, agregue la entrada del enrutador al archivo /etc/hostname6.hme1.

```
2001::aaaa:6666:6666 inet6 router
```

b. En el sistema partym, agregue la entrada del enrutador al archivo /etc/hostname6.hme1.

```
2001::eeee:3333:3333 inet6 router
```

11 Asegúrese de que los protocolos de enrutamiento no publiquen la ruta predeterminada en la intranet.

a. En el sistema enigma, agregue el indicador private al archivo /etc/hostname6.hme0.

```
6000:6666::aaaa:1116 inet6 private
```

- b. En el sistema `partym`, agregue el indicador `private` al archivo `/etc/hostname6.hme0`.

```
6000:3333::eeee:1113 inet6 private
```

- 12 Agregue manualmente una ruta predeterminada a través de `hme0`.

- a. En el sistema `enigma`, agregue la ruta siguiente:

```
# route add -inet6 default 2001::aaaa:0:4
```

- b. En el sistema `partym`, agregue la ruta siguiente:

```
# route add -inet6 default 2001::eeee:0:1
```

- 13 Para completar el procedimiento, vaya al [Paso 22](#) para ejecutar un protocolo de enrutamiento.

- 14 Configure un túnel seguro, `ip6.tun0`.

Nota – Los siguientes pasos configuran un túnel en un sistema que esté ejecutando una versión anterior a Solaris 10 4/09.

- a. En el sistema `enigma`, escriba los comandos siguientes:

```
# ifconfig ip6.tun0 inet6 plumb
```

```
# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333
```

- b. En el sistema `partym`, escriba los comandos siguientes:

```
# ifconfig ip6.tun0 inet6 plumb
```

```
# ifconfig ip6.tun0 inet6 6000:3333::eeee:1113 6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666
```

- 15 Proteja el túnel con la directiva IPsec que ha creado.

```
# ipsecconf
```

- 16 Muestre el enrutador para el túnel.

```
# ifconfig ip6.tun0 router up
```

- 17 En cada sistema, active el reenvío de IP para la interfaz `hme1`.

```
# ifconfig hme1 router
```

- 18 Asegúrese de que los protocolos de enrutamiento no publiquen la ruta predeterminada en la intranet.

```
# ifconfig hme0 private
```

19 Agregue manualmente una ruta predeterminada a través de hme0.

La ruta predeterminada debe ser un enrutador con acceso directo a Internet.

a. En el sistema enigma, agregue la ruta siguiente:

```
# route add -inet6 default 2001::aaaa:0:4
```

b. En el sistema partym, agregue la ruta siguiente:

```
# route add -inet6 default 2001::eeee:0:1
```

20 Asegúrese de que la VPN se inicie tras un reinicio, mediante la adición de una entrada al archivo /etc/hostname6.ip6.tun0.

La entrada replica los parámetros que se hayan transferido al comando ifconfig en el [Paso 14](#).

a. En el sistema enigma, agregue la entrada siguiente al archivo hostname6.ip6.tun0:

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 router up
```

b. En el sistema partym, agregue la entrada siguiente al archivo hostname6.ip6.tun0:

```
6000:3333::eeee:1113 6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666 router up
```

21 En cada sistema, configure los archivos de interfaz para transferir los parámetros correctos al daemon de enrutamiento.**a. En el sistema enigma, modifique los archivos /etc/hostname6.interfaz.**

```
# cat /etc/hostname6.hme0
## enigma
6000:6666::aaaa:1116 inet6 private

# cat /etc/hostname6.hme1
## enigma
2001::aaaa:6666:6666 inet6 router
```

b. En el sistema partym, modifique los archivos /etc/hostname6.interfaz.

```
# cat /etc/hostname6.hme0
## partym
6000:3333::eeee:1113 inet6 private

# cat /etc/hostname6.hme1
## partym
2001::eeee:3333:3333 inet6 router
```

22 Ejecute un protocolo de enrutamiento.

```
# routeadm -e ipv6-routing
# routeadm -u
```

Podría ser que antes de ejecutar el protocolo de enrutamiento fuese necesario configurarlo. Para obtener más información, consulte [“Protocolos de enrutamiento en Oracle Solaris” en la página 253](#). Para obtener un procedimiento, consulte [“Configuración de un enrutador IPv6” en la página 177](#).

▼ Cómo proteger una VPN con un túnel IPsec en modo transporte mediante IPv4

En modo transporte, el encabezado exterior determina la directiva IPsec que protege el paquete IP interior.

Este procedimiento amplía el procedimiento de [“Cómo proteger el tráfico entre dos sistemas con IPsec” en la página 511](#). Además de conectar dos sistemas, está conectando dos intranets que se conectan a estos dos sistemas. Los sistemas de este procedimiento actúan como portales.

En este procedimiento se utiliza la configuración descrita en [“Descripción de la topología de red para la protección de una VPN por parte de las tareas de IPsec” en la página 533](#). Para ver una descripción completa de los motivos para ejecutar comandos específicos, consulte los pasos correspondientes en [“Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4” en la página 535](#).

Nota – Lleve a cabo los pasos de este procedimiento en ambos sistemas.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Controle el flujo de paquetes antes de configurar IPsec.

a. Asegúrese de que el reenvío de IP y el enrutamiento dinámico de IP estén deshabilitados.

```
# routeadm
Configuration      Current      Current
      Option      Configuration System State
-----
IPv4 forwarding    disabled      disabled
      IPv4 routing default (enabled) enabled
...
```

Si el reenvío de IP y el enrutamiento dinámico de IP están habilitados, puede deshabilitarlos escribiendo:

```
# routeadm -d ipv4-routing -d ipv4-forwarding
# routeadm -u
```

b. Active los hosts múltiples de destino estricto de IP.

```
# ndd -set /dev/ip ip_strict_dst_multihoming 1
```



Precaución – El valor de `ip_strict_dst_multihoming` vuelve al predeterminado cuando se inicia el sistema. Para hacer que el valor cambiado sea persistente, consulte [“Cómo evitar la falsificación de la IP” en la página 563](#).

c. Deshabilite la mayoría de los servicios de red, y posiblemente todos.

Nota – Si su sistema se instaló con el perfil SMF "limitado", puede omitir este paso. Los servicios de red se deshabilitan, a excepción de Solaris Secure Shell.

La desactivación de los servicios de red evita que los paquetes IP dañen el sistema. Por ejemplo, podrían aprovecharse un daemon SNMP, una conexión telnet o una conexión rlogin.

Elija una de las siguientes opciones:

- Si ejecuta Solaris 10 11/06 o una versión posterior, ejecute el perfil SMF "limitado".

```
# netservices limited
```

- De lo contrario, deshabilite los servicios de red de forma individual.

```
# svcadm disable network/ftp:default
# svcadm disable network/finger:default
# svcadm disable network/login:rlogin
# svcadm disable network/nfs/server:default
# svcadm disable network/rpc/rstat:default
# svcadm disable network/smtp:sendmail
# svcadm disable network/telnet:default
```

d. Compruebe que la mayoría de los servicios de red estén deshabilitados.

Compruebe que los montajes de realimentación y el servicio ssh se estén ejecutando.

```
# svcs | grep network
online      Aug_02   svc:/network/loopback:default
...
online      Aug_09   svc:/network/ssh:default
```

3 Agregue un par de SA entre los dos sistemas.

Elija una de las siguientes opciones:

- Configure IKE para administrar las claves para las SA. Utilice uno de los procedimientos de “[Configuración de IKE \(mapa de tareas\)](#)” en la [página 583](#) para configurar IKE para la VPN.
- Si tiene motivos para administrar las claves manualmente, consulte “[Cómo crear manualmente asociaciones de seguridad IPsec](#)” en la [página 520](#).

4 Agregue la directiva IPsec.

Edita el archivo `/etc/inet/ipsecinit.conf` para agregar la directiva IPsec para la VPN. Para reforzar la directiva, consulte el [Ejemplo 20–15](#).

a. En el sistema `enigma` escriba la entrada siguiente en el archivo `ipsecinit.conf`:

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.16.16.6 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate transport}
ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. En el sistema `partym`, escriba la entrada siguiente en el archivo `ipsecinit.conf`:

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate transport}
ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

5 (Opcional) Compruebe la sintaxis del archivo de directiva IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 Para configurar el túnel y protegerlo con IPsec, siga los pasos en función de la versión de Solaris:

- A partir de la versión Solaris 10 4/09, siga los pasos del [Paso 7](#) al [Paso 13](#) y, a continuación, ejecute el protocolo de enrutamiento en el [Paso 22](#).
- Si está ejecutando una versión anterior a Solaris 10 4/09, siga las indicaciones del [Paso 14](#) al [Paso 22](#).

7 Configure el túnel `ip.tun0` en el archivo `/etc/hostname.ip.tun0`.

a. En el sistema `enigma`, agregue la entrada siguiente al archivo `hostname.ip.tun0`:

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 tdst 192.168.13.213 router up
```

b. En el sistema `partym`, agregue la entrada siguiente al archivo `hostname.ip.tun0`:

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 tdst 192.168.116.16 router up
```

- 8 Proteja el túnel con la directiva IPsec que ha creado.
`# svcadm refresh svc:/network/ipsec/policy:default`
- 9 Para leer el contenido del archivo `hostname.ip.tun0` en el núcleo, reinicie los servicios de red.
`# svcadm restart svc:/network/initial:default`
- 10 Active el reenvío de IP para la interfaz `hme1`.
 - a. En el sistema `enigma`, agregue la entrada del enrutador al archivo `/etc/hostname.hme1`.
`192.168.116.16 router`
 - b. En el sistema `partym`, agregue la entrada del enrutador al archivo `/etc/hostname.hme1`.
`192.168.13.213 router`
- 11 Asegúrese de que los protocolos de enrutamiento no publiquen la ruta predeterminada en la intranet.
 - a. En el sistema `enigma`, agregue el indicador `private` al archivo `/etc/hostname.hme1`.
`10.16.16.6 private`
 - b. En el sistema `partym`, agregue el indicador `private` al archivo `/etc/hostname.hme1`.
`10.1.3.3 private`
- 12 Agregue manualmente una ruta predeterminada a través de `hme0`.
 - a. En el sistema `enigma`, agregue la ruta siguiente:
`# route add default 192.168.116.4`
 - b. En el sistema `partym`, agregue la ruta siguiente:
`# route add default 192.168.13.5`
- 13 Para completar el procedimiento, vaya al [Paso 22](#) para ejecutar un protocolo de enrutamiento.
- 14 Configure el túnel, `ip.tun0`.

Nota – Los siguientes pasos configuran un túnel en un sistema que esté ejecutando una versión anterior a Solaris 10 4/09.

Utilice los comandos `ifconfig` para crear la interfaz de punto a punto:

```
# ifconfig ip.tun0 plumb
```

```
# ifconfig ip.tun0 system1-point system2-point \
tsrc system1-taddr tdst system2-taddr
```

a. En el sistema **enigma**, escriba los comandos siguientes:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213
```

b. En el sistema **partym**, escriba los comandos siguientes:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.1.3.3 10.16.16.6 \
tsrc 192.168.13.213 tdst 192.168.116.16
```

15 Proteja el túnel con la directiva IPsec que ha creado.

```
# ipsecconf
```

16 Muestre el enrutador para el túnel.

```
# ifconfig ip.tun0 router up
```

17 Active el reenvío de IP para la interfaz **hme1**.

```
# ifconfig hme1 router
```

18 Asegúrese de que los protocolos de enrutamiento no publiquen la ruta predeterminada en la intranet.

```
# ifconfig hme0 private
```

19 Agregue manualmente una ruta predeterminada a través de **hme0**.

La ruta predeterminada debe ser un enrutador con acceso directo a Internet.

```
# route add default router-on-hme0-subnet
```

a. En el sistema **enigma**, agregue la ruta siguiente:

```
# route add default 192.168.116.4
```

b. En el sistema **partym**, agregue la ruta siguiente:

```
# route add default 192.168.13.5
```

20 Asegúrese de que la VPN se inicie tras un reinicio mediante la adición de una entrada al archivo **/etc/hostname.ip.tun0**.

```
system1-point system2-point tsrc system1-taddr \
tdst system2-taddr encr_algs aes encr_auth_algs sha1 router up
```

a. En el sistema **enigma**, agregue la entrada siguiente al archivo **hostname.ip.tun0**:

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 \
tdst 192.168.13.213 router up
```

b. En el sistema partym, agregue la entrada siguiente al archivo `hostname.ip.tun0`:

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 \
tdst 192.168.116.16 router up
```

21 Configure los archivos de interfaz para transferir los parámetros correctos al daemon de enrutamiento.**a. En el sistema enigma, modifique los archivos `/etc/hostname.interfaz`.**

```
# cat /etc/hostname.hme0
## enigma
10.16.16.6 private
```

```
# cat /etc/hostname.hme1
## enigma
192.168.116.16 router
```

b. En el sistema partym, modifique los archivos `/etc/hostname.interfaz`.

```
# cat /etc/hostname.hme0
## partym
10.1.3.3 private
```

```
# cat /etc/hostname.hme1
## partym
192.168.13.213 router
```

22 Ejecute un protocolo de enrutamiento.

```
# routeadm -e ipv4-routing
# routeadm -u
```

Ejemplo 20–15 Requisito de directiva IPsec en todos los sistemas en modo transporte

En este ejemplo, el administrador comenta la directiva `bypass` configurada en el [Paso 4](#), con lo cual se refuerza la seguridad. Con esta configuración de directiva, cada sistema de la LAN debe activar IPsec para comunicarse con el enrutador.

```
# LAN traffic must implement IPsec.
# {laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate transport} ipsec {encr_algs aes encr_auth_algs sha1}
```

Ejemplo 20–16 Uso de sintaxis no admitida para configurar un túnel IPsec en modo transporte

En este ejemplo, el administrador conecta un sistema Solaris 10 7/07 con un sistema con la versión Solaris 10. Por tanto, el administrador utiliza la sintaxis de Solaris 10 en el archivo de configuración e incluye los algoritmos IPsec en el comando `ifconfig`.

El administrador sigue el procedimiento “[Cómo proteger una VPN con un túnel IPsec en modo transporte mediante IPv4](#)” en la página 551 con los siguientes cambios en la sintaxis.

- Para el [Paso 4](#), la sintaxis del archivo `ipsecinit.conf` es la siguiente:

```
# LAN traffic to and from this address can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{} ipsec {encr_algs aes encr_auth_algs sha1}
```

- Para el proceso del [Paso 14](#) al [Paso 16](#), la sintaxis para configurar un túnel seguro es la siguiente:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213 \
encr_algs aes encr_auth_algs sha1

# ifconfig ip.tun0 router up

# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213 \
encr_algs aes encr_auth_algs sha1
```

La directiva IPsec que se transfiere a los comandos `ifconfig` debe ser la misma que la directiva IPsec del archivo `ipsecinit.conf`. Al reiniciar, cada sistema lee el archivo `ipsecinit.conf` para su directiva.

- Para el [Paso 20](#), la sintaxis del archivo `hostname.ip.tun0` es la siguiente:

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 \
tdst 192.168.13.213 encr_algs aes encr_auth_algs sha1 router up
```

▼ Cómo proteger una VPN con un túnel IPsec en modo transporte mediante IPv6

Para configurar una VPN en una red IPv6, debe seguir los mismos pasos que para configurar una red IPv4. No obstante, la sintaxis de los comandos es ligeramente distinta. Para ver una descripción completa de los motivos para ejecutar comandos específicos, consulte los pasos correspondientes en “[Cómo proteger una VPN con un túnel IPsec en modo túnel mediante IPv4](#)” en la página 535.

Nota – Lleve a cabo los pasos de este procedimiento en ambos sistemas.

Este procedimiento utiliza los siguientes parámetros.

Parámetro	Europa	California
Nombre del sistema	enigma	partym
Interfaz de la intranet del sistema	hme1	hme1
Interfaz de Internet del sistema	hme0	hme0
Dirección de intranet del sistema	6000:6666::aaaa:1116	6000:3333::eeee:1113
Dirección de Internet del sistema	2001::aaaa:6666:6666	2001::eeee:3333:3333
Nombre del enrutador de Internet	router-E	router-C
Dirección del enrutador de Internet	2001::aaaa:0:4	2001::eeee:0:1
Nombre de túnel	ip6.tun0	ip6.tun0

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Controle el flujo de paquetes antes de configurar IPsec.

a. Asegúrese de que el reenvío de IP y el enrutamiento dinámico de IP estén deshabilitados.

```
# routeadm
Configuration      Current      Current
      Option      Configuration  System State
-----
...
IPv6 forwarding    disabled      disabled
  IPv6 routing      disabled      disabled
```

Si el reenvío de IP y el enrutamiento dinámico de IP están habilitados, puede deshabilitarlos escribiendo:

```
# routeadm -d ipv6-forwarding -d ipv6-routing
# routeadm -u
```

b. Active los hosts múltiples de destino estricto de IP.

```
# ndd -set /dev/ip ip6_strict_dst_multihoming 1
```



Precaución – El valor de `ip6_strict_dst_multihoming` vuelve al predeterminado cuando se inicia el sistema. Para hacer que el valor cambiado sea persistente, consulte [“Cómo evitar la falsificación de la IP” en la página 563](#).

c. Compruebe que la mayoría de los servicios de red estén deshabilitados.

Compruebe que los montajes de realimentación y el servicio ssh se estén ejecutando.

```
# svcs | grep network
online      Aug_02   svc:/network/loopback:default
...
online      Aug_09   svc:/network/ssh:default
```

3 Agregue un par de SA entre los dos sistemas.

Elija una de las siguientes opciones:

- Configure IKE para administrar las claves para las SA. Utilice uno de los procedimientos de [“Configuración de IKE \(mapa de tareas\)” en la página 583](#) para configurar IKE para la VPN.
- Si tiene motivos para administrar las claves manualmente, consulte [“Cómo crear manualmente asociaciones de seguridad IPsec” en la página 520](#).

4 Agregue la directiva IPsec.

Edita el archivo `/etc/inet/ipsecinit.conf` para agregar la directiva IPsec para la VPN.

a. En el sistema enigma, escriba la entrada siguiente en el archivo `ipsecinit.conf`:

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:6666::aaaa:1116 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate transport}
ipsec {encr_algs aes encr_auth_algs sha1}
```

b. En el sistema partym, escriba la entrada siguiente en el archivo `ipsecinit.conf`:

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate transport}
ipsec {encr_algs aes encr_auth_algs sha1}
```

5 (Opcional) Compruebe la sintaxis del archivo de directiva IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 Para configurar el túnel y protegerlo con IPsec, siga los pasos en función de la versión de Solaris:

- A partir de la versión Solaris 10 4/09, siga los pasos del [Paso 7](#) al [Paso 13](#) y, a continuación, ejecute el protocolo de enrutamiento en el [Paso 22](#).
- Si está ejecutando una versión anterior a Solaris 10 4/09, siga las indicaciones del [Paso 14](#) al [Paso 22](#).

7 Configure el túnel `ip6.tun0` en el archivo `/etc/hostname.ip6.tun0`.**a. En el sistema `enigma`, agregue la entrada siguiente al archivo `hostname.ip6.tun0`:**

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 tsr 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 router up
```

b. En el sistema `partym`, agregue la entrada siguiente al archivo `hostname.ip6.tun0`:

```
6000:3333::eeee:1113 6000:6666::aaaa:1116 tsr 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666 router up
```

8 Proteja el túnel con la directiva IPsec que ha creado.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9 Para leer el contenido del archivo `hostname.ip6.tun0` en el núcleo, reinicie los servicios de red.

```
# svcadm restart svc:/network/initial:default
```

10 Active el reenvío de IP para la interfaz `hme1`.**a. En el sistema `enigma`, agregue la entrada del enrutador al archivo `/etc/hostname6.hme1`.**

```
2001::aaaa:6666:6666 inet6 router
```

b. En el sistema `partym`, agregue la entrada del enrutador al archivo `/etc/hostname6.hme1`.

```
2001::eeee:3333:3333 inet6 router
```

11 Asegúrese de que los protocolos de enrutamiento no publiquen la ruta predeterminada en la intranet.**a. En el sistema `enigma`, agregue el indicador `private` al archivo `/etc/hostname6.hme0`.**

```
6000:6666::aaaa:1116 inet6 private
```

b. En el sistema `partym`, agregue el indicador `private` al archivo `/etc/hostname6.hme0`.

```
6000:3333::eeee:1113 inet6 private
```

12 Agregue manualmente una ruta predeterminada a través de `hme0`.**a. En el sistema `enigma`, agregue la ruta siguiente:**

```
# route add -inet6 default 2001::aaaa:0:4
```


b. En el sistema `partym`, agregue la ruta siguiente:

```
# route add -inet6 default 2001::eeee:0:1
```

13 Para completar el procedimiento, vaya al [Paso 22](#) para ejecutar un protocolo de enrutamiento.

14 Configure un túnel seguro, `ip6.tun0`.

Nota – Los siguientes pasos configuran un túnel en un sistema que esté ejecutando una versión anterior a Solaris 10 4/09.

a. En el sistema `enigma`, escriba los comandos siguientes:

```
# ifconfig ip6.tun0 inet6 plumb
```

```
# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
  tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333
```

b. En el sistema `partym`, escriba los comandos siguientes:

```
# ifconfig ip6.tun0 inet6 plumb
```

```
# ifconfig ip6.tun0 inet6 6000:3333::eeee:1113 6000:6666::aaaa:1116 \
  tsrc 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666
```

15 Proteja el túnel con la directiva IPsec que ha creado.

```
# ipsecconf
```

16 Muestre el enrutador para el túnel.

```
# ifconfig ip6.tun0 router up
```

17 Active el reenvío de IP para la interfaz `hme1`.

```
# ifconfig hme1 router
```

18 Asegúrese de que los protocolos de enrutamiento no publiquen la ruta predeterminada en la intranet.

```
# ifconfig hme0 private
```

19 En cada sistema, agregue manualmente una ruta predeterminada mediante `hme0`.

La ruta predeterminada debe ser un enrutador con acceso directo a Internet.

a. En el sistema `enigma`, agregue la ruta siguiente:

```
# route add -inet6 default 2001::aaaa:0:4
```

b. En el sistema `partym`, agregue la ruta siguiente:

```
# route add -inet6 default 2001::eeee:0:1
```

20 En cada sistema, asegúrese de que la VPN se inicie tras un reinicio agregando una entrada al archivo `/etc/hostname6.ip6.tun0`.

La entrada replica los parámetros que se hayan transferido al comando `ifconfig` en el [Paso 14](#).

a. En el sistema `enigma`, agregue la entrada siguiente al archivo `hostname6.ip6.tun0`:

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 router up
```

b. En el sistema `partym`, agregue la entrada siguiente al archivo `hostname6.ip6.tun0`:

```
6000:3333::eeee:1113 6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666 router up
```

21 Configure los archivos de interfaz para transferir los parámetros correctos al daemon de enrutamiento.**a. En el sistema `enigma`, modifique los archivos `/etc/hostname6.interfaz`.**

```
# cat /etc/hostname6.hme0
## enigma
6000:6666::aaaa:1116 inet6 private
```

```
# cat /etc/hostname6.hme1
## enigma
2001::aaaa:6666:6666 inet6 router
```

b. En el sistema `partym`, modifique los archivos `/etc/hostname6.interfaz`.

```
# cat /etc/hostname6.hme0
## partym
6000:3333::eeee:1113 inet6 private
```

```
# cat /etc/hostname6.hme1
##
partym2001::eeee:3333:3333 inet6 router
```

22 Ejecute un protocolo de enrutamiento.

```
# routeadm -e ipv6-routing
# routeadm -u
```

Ejemplo 20–17 Uso de sintaxis descartada para configurar IPsec en modo de transporte mediante IPv6

En este ejemplo, el administrador conecta un sistema Solaris 10 7/07 con un sistema con la versión Solaris 10. Por tanto, el administrador utiliza la sintaxis de Solaris 10 en el archivo de configuración e incluye los algoritmos IPsec en el comando `ifconfig`.

El administrador sigue el procedimiento “[Cómo proteger una VPN con un túnel IPsec en modo transporte mediante IPv6](#)” en la [página 557](#) con los siguientes cambios en la sintaxis.

- Para el [Paso 4](#), la sintaxis del archivo `ipseccinit.conf` es la siguiente:

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}
```

```
# LAN traffic can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}
```

```
# WAN traffic uses ESP with AES and SHA-1.
{} ipsec {encr_algs aes encr_auth_algs sha1}
```

- Para el proceso del [Paso 14](#) al [Paso 17](#), la sintaxis para configurar un túnel seguro es la siguiente:

```
# ifconfig ip6.tun0 inet6 plumb
```

```
# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 \
encr_algs aes encr_auth_algs sha1
```

```
# ifconfig ip6.tun0 inet6 router up
```

La directiva IPsec que se transfiere a los comandos `ifconfig` debe ser la misma que la directiva IPsec del archivo `ipsecinit.conf`. Al reiniciar, cada sistema lee el archivo `ipsecinit.conf` para su directiva.

- Para el [Paso 20](#), la sintaxis del archivo `hostname6.ip6.tun0` es la siguiente:

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 \
encr_algs aes encr_auth_algs sha1 router up
```

▼ Cómo evitar la falsificación de la IP

Para evitar que el sistema reenvíe paquetes a otra interfaz sin intentar descifrarlos, el sistema debe comprobar que no haya falsificación de IP. Un método de prevención es definir el parámetro de inicio múltiple de destino estricto de IP mediante el uso del comando `ndd`. Cuando este parámetro se define en un manifiesto SMF, el parámetro se establece cuando el sistema se reinicia.

Nota – Lleve a cabo los pasos de este procedimiento en ambos sistemas.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Cree el manifiesto SMF específico para el sitio con el fin de comprobar que no haya falsificación de IP.

Use el siguiente ejemplo de secuencia de comandos:

/var/svc/manifest/site/spoof_check.xml.

```
<?xml version="1.0"?>
<!DOCTYPE service_bundle SYSTEM "/usr/share/lib/xml/dtd/service_bundle.dtd.1">

<service_bundle type='manifest' name='Custom:ip_spoof_checking'>

<!-- This is a custom smf(5) manifest for this system. Place this
      file in /var/svc/manifest/site, the directory for local
      system customizations. The exec method uses an unstable
      interface to provide a degree of protection against IP
      spoofing attacks when this system is acting as a router.

      IP spoof protection can also be achieved by using ipfilter(5).
      If ipfilter is configured, this service can be disabled.

      Note: Unstable interfaces might be removed in later
      releases. See attributes(5).
-->

<service
  name='site/ip_spoofcheck'
  type='service'
  version='1'>

  <create_default_instance enabled='false' />
  <single_instance />

  <!-- Don't enable spoof protection until the
        network is up.
  -->
  <dependency
    name='basic_network'
    grouping='require_all'
    restart_on='none'
    type='service'>
    <service_fmri value='svc:/milestone/network' />
  </dependency>

  <exec_method
    type='method'
    name='start'
    exec='/usr/sbin/ndd -set /dev/ip ip_strict_dst_multihoming 1'
  <!-- For an IPv6 network, use the IPv6 version of this command, as in:
        exec='/usr/sbin/ndd -set /dev/ip ip6_strict_dst_multihoming 1
  -->
    timeout_seconds='60'
  />

  <exec_method
    type='method'
    name='stop'
    exec=':true'
    timeout_seconds='3'
```

```

    />

    <property_group name='startd' type='framework'>
        <propval
            name='duration'
            type='astring'
            value='transient'
        />
    </property_group>

    <stability value='Unstable' />

</service>
</service_bundle>

```

3 Importe este manifiesto al depósito SMF.

```
# svccfg import /var/svc/manifest/site/spoof_check.xml
```

4 Habilite el servicio ip_spoofcheck.

Utilice el nombre que se ha definido en el manifiesto, /site/ip_spoofcheck.

```
# svcadm enable /site/ip_spoofcheck
```

5 Compruebe que el servicio ip_spoofcheck esté en línea.

```
# svcs /site/ip_spoofcheck
```


Arquitectura de seguridad IP (referencia)

Este capítulo contiene la siguiente información de referencia:

- “Utilidad de gestión de servicios de IPsec” en la página 567
- “Comando `ipsecconf`” en la página 568
- “Archivo `ipsecinit.conf`” en la página 569
- “Comando `ipsecalgs`” en la página 570
- “Base de datos de asociaciones de seguridad para IPsec” en la página 571
- “Utilidades para la generación de claves en IPsec” en la página 571
- “Extensiones IPsec para otras utilidades” en la página 573

Para obtener instrucciones sobre cómo implementar IPsec en la red, consulte el [Capítulo 20](#), “Configuración de IPsec (tareas)”. Para ver una descripción general de IPsec, consulte el [Capítulo 19](#), “Arquitectura de seguridad IP (descripción general)”.

Utilidad de gestión de servicios de IPsec

La utilidad de gestión de servicios (SMF) proporciona los siguientes servicios para IPsec:

- `svc:/network/ipsec/policy` **servicio** – administra la directiva IPsec. Por defecto, este servicio está habilitado. El valor de la propiedad `config_file` determina la ubicación del archivo `ipsecinit.conf`. El valor inicial es `/etc/inet/ipsecinit.conf`.
- `svc:/network/ipsec/ipsecalgs` **servicio** – Administra los algoritmos que están disponibles para IPsec. Por defecto, este servicio está habilitado.
- `svc:/network/ipsec/manual-key` **servicio** – Activa la gestión manual de claves. Por defecto, este servicio está inhabilitado. El valor de la propiedad `config_file` determina la ubicación del archivo de configuración `ipseckeys`. El valor inicial es `/etc/inet/secret/ipseckeys`.
- `svc:/network/ipsec/ike` **servicio** – Administra IKE. Por defecto, este servicio está inhabilitado. Si desea conocer las propiedades configurables, consulte “[Utilidad de gestión de servicios de IKE](#)” en la página 629.

Para obtener más información sobre SMF, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)”](#) de *Guía de administración del sistema: administración básica*. Consulte también las páginas de comando `man smf(5)`, `svcadm(1M)` y `svccfg(1M)`.

Comando ipsecconf

El comando `ipsecconf` permite configurar la directiva IPsec para un host. Al ejecutar el comando para configurar la directiva, el sistema crea las entradas de la directiva IPsec en el núcleo. El sistema utiliza estas entradas para comprobar la directiva en todos los datagramas IP entrantes y salientes. Los datagramas reenviados no están sujetos a las comprobaciones de directivas que se agregan utilizando este comando. El comando `ipsecconf` también configura la base de datos de directivas de seguridad (SPD).

- Para obtener información sobre cómo proteger los paquetes reenviados, consulte las páginas del comando `man ifconfig(1M)` y `tun(7M)`.
- Para conocer las opciones de directiva IPsec, consulte la página del comando `man ipsecconf(1M)`.
- Para obtener instrucciones sobre cómo utilizar el comando `ipsecconf` para proteger el tráfico entre los sistemas, consulte [“Configuración de IKE \(mapa de tareas\)” en la página 583](#).

Debe convertirse en superusuario o asumir un rol equivalente para invocar el comando `ipsecconf`. El comando acepta entradas que protegen el tráfico en ambas direcciones. El comando también acepta entradas que protegen el tráfico sólo en una dirección.

Las entradas de directiva con un formato de dirección local y dirección remota pueden proteger el tráfico en ambas direcciones con una sola entrada de directiva. Por ejemplo, las entradas que contienen los patrones `laddr host1` y `raddr host2` protegen el tráfico en ambas direcciones, si no se especifica ninguna dirección para el host con nombre. De este modo, sólo necesita una entrada de directiva para cada host.

Las entradas de directiva con un formato de dirección de origen a dirección de destino sólo protegen el tráfico en una dirección. Por ejemplo, una entrada de directiva del patrón `saddr host1 daddr host2` protege el tráfico entrante o el saliente, no el tráfico en ambas direcciones. Por tanto, para proteger el tráfico en ambas direcciones, es necesario transferir al comando `ipsecconf` otra entrada, como en `saddr host2 daddr host1`.

Para asegurarse de que la directiva IPsec esté activa cuando se inicie el equipo, puede crear un archivo de directiva IPsec, `/etc/inet/ipsecinit.conf`. Este archivo se lee cuando se inician los servicios de red. Para obtener instrucciones sobre cómo crear un archivo de directiva IPsec, consulte [“Protección del tráfico con IPsec \(mapa de tareas\)” en la página 509](#).

A partir de la versión &#s10u7, con la opción `-c`, el comando `ipsecconf` comprueba la sintaxis del archivo de directiva IPsec que proporciona como argumento.

Las entradas de directivas agregadas por el comando `ipseconf` no persisten tras un reinicio del sistema. Para asegurarse de que la directiva IPsec está activa cuando el sistema se inicia, agregue las entradas de directivas al archivo `/etc/inet/ipsecinit.conf`. En la versión actual, actualice o habilite el servicio `directiva`. En una versión anterior a Solaris 10 4/09 reinicie o utilice el comando `ipseconf`. Si desea conocer ejemplos, consulte [“Protección del tráfico con IPsec \(mapa de tareas\)” en la página 509](#).

Archivo ipsecinit.conf

Para invocar las directivas de seguridad IPsec al iniciar Sistema operativo Solaris (sistema operativo Solaris), se crea un archivo de configuración para iniciar IPsec con las entradas de directiva IPsec específicas. El nombre predeterminado para este archivo es `/etc/inet/ipsecinit.conf`. Consulte la página del comando `man ipseconf(1M)` para obtener más información acerca de las entradas de directiva y su formato. Una vez configuradas las directivas, puede utilizar el comando `ipseconf` para ver o modificar la configuración existente. A partir de Solaris 10 4/09, debe actualizar el servicio `policy` para modificar la configuración existente.

Archivo ipsecinit.conf de ejemplo

El software Solaris incluye un archivo de directiva IPsec de ejemplo, `ipsecinit.sample`. Puede utilizar dicho archivo como plantilla para crear su propio archivo `ipsecinit.conf`. El archivo `ipsecinit.sample` contiene los ejemplos siguientes:

```
#
# For example,
#
#     {rport 23} ipsec {encr_algs des encr_auth_algs md5}
#
# will protect the telnet traffic originating from the host with ESP using
# DES and MD5. Also:
#
#     {raddr 10.5.5.0/24} ipsec {auth_algs any}
#
# will protect traffic to or from the 10.5.5.0 subnet with AH
# using any available algorithm.
#
#
# To do basic filtering, a drop rule may be used. For example:
#
#     {lport 23 dir in} drop {}
#     {lport 23 dir out} drop {}
# will disallow any remote system from telnetting in.
#
# If you are using IPv6, it may be useful to bypass neighbor discovery
# to allow in.iked to work properly with on-link neighbors. To do that,
# add the following lines:
#
```

```
#          {ulp ipv6-icmp type 133-137 dir both } pass { }  
#  
# This will allow neighbor discovery to work normally.
```

Consideraciones de seguridad para ipsecinit.conf e ipsecconf

Tenga especial precaución al transmitir una copia del archivo `ipsecinit.conf` por una red. Un adversario puede leer un archivo montado en red mientras se lee el archivo. Si, por ejemplo, se accede al archivo `/etc/inet/ipsecinit.conf` o se copia desde un sistema de archivos montado en NFS, un adversario puede cambiar la directiva que contiene el archivo.

Asegúrese de configurar las directivas IPsec antes de iniciar cualquier comunicación, ya que las conexiones existentes podrían verse afectadas por la adición de nuevas entradas de directiva. Asimismo, no cambie las directivas durante una comunicación.

Específicamente, la directiva IPsec no puede cambiarse para los sockets SCTP, TCP o UDP en los que se ha emitido una llamada de función `connect()` o `accept()`. Un socket cuya directiva no se puede modificar se denomina *socket bloqueado*. Las nuevas entradas de directiva no protegen los sockets que ya están bloqueados. Para más información, consulte las páginas del comando `man connect(3SOCKET)` y `accept(3SOCKET)`.

Proteja su sistema de nombres. Si se cumplen las dos condiciones siguientes, los nombres de host dejarán de ser de confianza:

- La dirección de origen es un host que se puede buscar en la red.
- El sistema de nombres está en peligro.

Los fallos de seguridad a menudo se deben a la mala aplicación de las herramientas, no a las herramientas en sí. Utilice el comando `ipsecconf` con precaución. Utilice una consola u otro TTY conectado físicamente para obtener el funcionamiento mas seguro.

Comando ipsecalgs

La estructura criptográfica de Solaris proporciona autenticación y algoritmos de cifrado para IPsec. El comando `ipsecalgs` puede enumerar los algoritmos que cada protocolo de IPsec admite. La configuración `ipsecalgs` se almacena en el archivo `/etc/inet/ipsecalgs`. Normalmente, este archivo no necesita modificarse. Sin embargo, si el archivo debe modificarse, utilice el comando `ipsecalgs`. El archivo nunca debe editarse directamente. En la versión actual, los algoritmos admitidos se sincronizan con el núcleo en el inicio del sistema mediante el servicio `svc:/network/ipsec/ipsecalgs:default`.

ISAKMP [dominio de interpretación](#), que se trata en la norma RFC 1407, describe los algoritmos y protocolos IPsec válidos. De manera general, el dominio de interpretación define los formatos

de los datos, los tipos de intercambio de tráfico de red y las convenciones de denominación de información relacionada con la seguridad. Ejemplos de información relacionada con la seguridad son los algoritmos y modos criptográficos, y las directrices de seguridad.

En concreto, el DOI ISAKMP define las convenciones de denominación y numeración para los algoritmos IPsec válidos y sus protocolos. `PROTO_IPSEC_AH` y `PROTO_IPSEC_ESP`. Cada algoritmo se asocia exactamente con un protocolo. Estas definiciones DOI ISAKMP se encuentran en el archivo `/etc/inet/ipsecalg`s. Los números de protocolo y algoritmos los define la Autoridad de números asignados de Internet (IANA). El comando `ipseca`lgs permite ampliar la lista de algoritmos para IPsec.

Para obtener más información acerca de los algoritmos, consulte la página del comando `man ipseca`lgs(1M). Para más información sobre la estructura criptográfica de Solaris, consulte el [Capítulo 13, “Estructura criptográfica de Oracle Solaris \(descripción general\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

Base de datos de asociaciones de seguridad para IPsec

La información sobre el material de claves para los servicios de seguridad IPsec se guarda en una base de datos de asociaciones de seguridad (SADB). Las asociaciones de seguridad (SA) protegen los paquetes entrantes y salientes. Las SADB se controlan mediante un proceso de usuario, o posiblemente varios procesos a la vez, que envían mensajes a través de un tipo de socket especial. Este modo de controlar las SADB es análogo al método que se describe en la página del comando `man route`(7P). Sólo el superusuario o un usuario que haya asumido un rol equivalente pueden acceder a la base de datos.

El daemon `in.iked` y el comando `ipseckey` utilizan la interfaz de socket `PF_KEY` para mantener las SADB. Para más información sobre cómo administrar las solicitudes y mensajes de SADB, consulte la página del comando `man pf_key`(7P).

Utilidades para la generación de claves en IPsec

El protocolo IKE permite administrar automáticamente las claves para las direcciones IPv4 e IPv6. Consulte el [Capítulo 23, “Configuración de IKE \(tarear\)”](#) para obtener instrucciones sobre cómo configurar IKE. La utilidad de claves manuales es el comando `ipseckey`, que se describe en la página del comando `man ipseckey`(1M).

Puede usar el comando `ipseckey` para rellenar manualmente la base de datos de asociaciones de seguridad (SADB). Normalmente, la generación manual de SA se utiliza cuando IKE no está disponible por algún motivo. Sin embargo, si los valores SPI son exclusivos, la generación manual de SA e IKE se pueden utilizar al mismo tiempo.

El comando `ipseckey` puede utilizarse para ver todas las SA conocidas por el sistema, independientemente de si las claves se han agregado manualmente o mediante IKE. A partir de

la versión Solaris 10 4/09, con la opción -c, el comando ipseckey comprueba la sintaxis del archivo de claves que proporciona como argumento.

Las IPsec SA que añade el comando ipseckey no persisten tras el reinicio del sistema. En la versión actual, para habilitar manualmente las SA agregadas en el inicio del sistema, agregue entradas al archivo `/etc/inet/secret/ipseckey` y, a continuación, habilite el servicio `svc:/network/ipsec/manual-key:default`. Si desea conocer el procedimiento, consulte [“Cómo crear manualmente asociaciones de seguridad IPsec” en la página 520](#).

Aunque el comando ipseckey tiene un número limitado de opciones generales, admite un lenguaje de comandos amplio. Puede especificar que las solicitudes se envíen mediante una interfaz de programación específica para las claves manuales. Para obtener información adicional, consulte la página del comando `man pf_key(7P)`.

Consideraciones de seguridad para ipseckey

El comando ipseckey permite al superusuario o a una función con el perfil de seguridad de red o de derechos de administración de redes IPsec especificar información criptográfica confidencial de claves. Si un adversario obtiene acceso a esta información, puede poner en peligro la seguridad del tráfico IPsec.

Cuando administre material de claves y utilice el comando ipseckey, debe tener en cuenta los aspectos siguientes:

- ¿Ha actualizado el material de claves? La actualización periódica de las claves es fundamental para garantizar la seguridad. La actualización de las claves protege contra posibles ataques de los algoritmos y las claves, y limita los daños a los que se expone una clave.
- ¿El TTY se transfiere por una red? ¿El comando ipseckey está en modo interactivo?
 - En modo interactivo, la seguridad del material de claves es la seguridad de la ruta de red para el tráfico de este TTY. Debe evitar el uso del comando ipseckey en una sesión rlogin o telnet de texto simple.
 - Incluso las ventanas locales podrían ser vulnerables a ataques de un programa oculto que lee los eventos de ventanas.
- ¿Ha utilizado la opción -f? ¿Se está accediendo al archivo a través de la red? ¿Todo el mundo puede leer el archivo?
 - Un adversario puede leer un archivo montado en red mientras se lee el archivo. Debe evitar el uso de un archivo con material de claves que pueda leer todo el mundo.
 - Proteja su sistema de nombres. Si se cumplen las dos condiciones siguientes, los nombres de host dejarán de ser de confianza:
 - La dirección de origen es un host que se puede buscar en la red.
 - El sistema de nombres está en peligro.

Los fallos de seguridad a menudo se deben a la mala aplicación de las herramientas, no a las herramientas en sí. Utilice el comando `ipseckey` con precaución. Utilice una consola u otro TTY conectado físicamente para obtener el funcionamiento mas seguro.

Extensiones IPsec para otras utilidades

El comando `ifconfig` tiene opciones para administrar la directiva IPsec en una interfaz de túnel. El comando `snoop` puede analizar los encabezados AH y ESP.

Comando `ifconfig` e IPsec

En Solaris 10, Solaris 10 7/05, Solaris 10 1/06 y Solaris 10 11/06: Para admitir IPsec, con el comando `ifconfig` hay disponibles las siguientes opciones de seguridad. Estas opciones de seguridad se administran mediante el comando `ipseccnf` de Solaris 10 7/07.

- `auth_algs`
- `encr_auth_algs`
- `encr_algs`

Debe especificar todas las opciones de seguridad de IPsec para un túnel de una invocación. Por ejemplo, si utiliza solamente ESP para proteger el tráfico, debe configurar el túnel (`ip.tun0`) una vez con ambas opciones de seguridad, como en el ejemplo siguiente:

```
# ifconfig ip.tun0 encr_algs aes encr_auth_algs md5
```

De un modo similar, una entrada de `ipsecinit.conf` configuraría el túnel una vez con ambas opciones de seguridad, como en el caso siguiente:

```
# WAN traffic uses ESP with AES and MD5.
{} ipsec {encr_algs aes encr_auth_algs md5}
```

Opción de seguridad `auth_algs`

Esta opción habilita AH IPsec para un túnel con un algoritmo de autenticación especificado. La opción `auth_algs` tiene el formato siguiente:

```
auth_algs authentication-algorithm
```

Para el algoritmo, puede especificar un número o un nombre de algoritmo, incluido el parámetro *any*, para no expresar ninguna preferencia de algoritmo específica. Para desactivar la seguridad del túnel, especifique la opción siguiente:

```
auth_algs none
```

Para ver una lista de los algoritmos de autenticación disponibles, ejecute el comando `ipsecalgs`.

Nota – La opción `auth_algs` no puede funcionar con NAT-Traversal. Para más información, consulte [“Paso a través de IPsec y NAT” en la página 503](#).

Opción de seguridad `encr_auth_algs`

Esta opción habilita ESP IPsec para un túnel con un algoritmo de autenticación especificado. La opción `encr_auth_algs` tiene el formato siguiente:

```
encr_auth_algs authentication-algorithm
```

Para el algoritmo, puede especificar un número o un nombre de algoritmo, incluido el parámetro *any*, para no expresar ninguna preferencia de algoritmo específica. Si especifica un algoritmo de cifrado ESP pero no especifica el algoritmo de autenticación, el valor predeterminado del algoritmo de autenticación ESP es el parámetro *any*.

Para ver una lista de los algoritmos de autenticación disponibles, ejecute el comando `ipsecalgs`.

Opción de seguridad `encr_algs`

Esta opción habilita ESP IPsec para un túnel con un algoritmo de cifrado especificado. La opción `encr_algs` tiene el formato siguiente:

```
encr_algs encryption-algorithm
```

Para el algoritmo, puede especificar un número o un nombre de algoritmo. Para desactivar la seguridad del túnel, especifique la opción siguiente:

```
encr_algs none
```

Si especifica un algoritmo de autenticación ESP pero no un algoritmo de cifrado, el valor de cifrado predeterminado de ESP será el parámetro *null*.

Para ver una lista de los algoritmos de cifrado disponibles, ejecute el comando `ipsecalgs`.

Comando `snoop` e IPsec

El comando `snoop` puede analizar encabezados AH y ESP. Dado que ESP cifra sus datos, el comando `snoop` no puede ver los encabezados cifrados protegidos por ESP. AH no cifra los datos. En consecuencia, el tráfico que protege AH se puede examinar con el comando `snoop`. La opción `-V` para el comando muestra cuándo se está utilizando AH en un paquete. Para obtener más información, consulte la página del comando `man snoop(1M)`.

Para ver un ejemplo de resultado `snoop` detallado en un paquete protegido, consulte [“Cómo verificar que los paquetes estén protegidos con IPsec” en la página 525](#).

Intercambio de claves de Internet (descripción general)

El Protocolo de intercambio de claves de Internet (Internet Key Exchange, IKE) automatiza la gestión de claves de IPsec. Este capítulo contiene la información siguiente sobre IKE:

- “Novedades de IKE” en la página 575
- “Administración de claves con IKE” en la página 576
- “Negociación de claves IKE” en la página 576
- “Opciones de configuración de IKE” en la página 578
- “IKE y aceleración de hardware” en la página 580
- “IKE y almacenamiento de hardware” en la página 580
- “Archivos y utilidades IKE” en la página 580
- “Cambios de IKE en Solaris 10” en la página 582

Para obtener instrucciones sobre cómo implementar IKE, consulte el [Capítulo 23, “Configuración de IKE \(tareas\)”](#). Para obtener información de referencia, consulte el [Capítulo 24, “Intercambio de claves de Internet \(referencia\)”](#). Para obtener información sobre IPsec, consulte el [Capítulo 19, “Arquitectura de seguridad IP \(descripción general\)”](#).

Novedades de IKE

Solaris 10 4/09: A partir de esta versión, la utilidad de gestión de servicios (SMF) administra IKE como servicio. Por defecto, el servicio `red/svc:/ipsec/ike:predeterminado` está deshabilitado. También en esta versión, el perfil de derechos Network IPsec Management se proporciona para administrar IPsec e IKE.

Solaris 10 7/07: A partir de esta versión, IKE puede utilizar el algoritmo AES y configurarse en la zona global para utilizar en zonas no globales.

- La opción de socket `SO_ALLZONES` permite a IKE controlar el tráfico de las zonas no globales.
- Para ver una lista completa de las nuevas funciones de Solaris 10 y una descripción de las versiones de Solaris, consulte [Novedades de Oracle Solaris 10 8/11](#).

Administración de claves con IKE

La administración del material de claves de las asociaciones de seguridad de IPsec se denomina *administración de claves*. La administración de claves automática requiere un canal de comunicación seguro para la creación, autenticación e intercambio de claves. Sistema operativo Solaris utiliza el intercambio de claves de Internet (IKE) para automatizar la administración de claves. IKE se escala fácilmente para proporcionar un canal seguro para un volumen de tráfico importante. Las asociaciones de seguridad de IPsec en paquetes IPv4 e IPv6 pueden aprovechar IKE.

Cuando se utiliza IKE en un sistema con una placa de Sun Crypto Accelerator 1000, Sun Crypto Accelerator 4000 o Sun Crypto Accelerator 6000, las operaciones de claves públicas se pueden descargar en el acelerador. Los recursos del sistema operativo no se utilizan para las operaciones de claves públicas. Cuando se utiliza IKE en un sistema con una placa de Sun Crypto Accelerator 6000 o Sun Crypto Accelerator 4000, los certificados, claves públicas y claves privadas se pueden almacenar en la placa. El almacenamiento de claves fuera del sistema proporciona una capa de protección adicional.

Negociación de claves IKE

El daemon IKE, `in.iked`, negocia y autentica el material de claves para las asociaciones de seguridad de forma protegida. El daemon utiliza números generadores aleatorios a partir de funciones internas que proporciona Sistema operativo Solaris. IKE proporciona confidencialidad directa perfecta (PFS). En PFS, las claves que protegen la transmisión de datos no se utilizan para derivar claves adicionales. Asimismo, los números generadores que se utilizan para crear claves de transmisión de datos no se vuelven a utilizar. Consulte la página del comando `man in.iked(1M)`.

Cuando el daemon IKE descubre una clave de cifrado pública del sistema remoto, el sistema puede utilizar dicha clave. El sistema cifra los mensajes utilizando la clave pública del sistema remoto. Sólo el sistema remoto puede leer los mensajes. El daemon IKE lleva a cabo su trabajo en dos fases. Las fases se denominan *intercambios*.

Terminología de claves IKE

La tabla siguiente enumera los términos que se utilizan en el ámbito de la negociación de claves, incluye sus acrónimos habituales y aporta una definición e información del uso de cada término.

TABLA 22-1 Términos de negociación de claves, acrónimos y usos

Término de negociación de claves	Acrónimo	Definición y uso
Intercambio de claves		El proceso de generación de claves para los algoritmos criptográficos asimétricos. Los dos métodos principales son los protocolos RSA y el protocolo Diffie-Hellman.
Protocolo Diffie-Hellman	DH	Protocolo de intercambio de claves que implica la generación y la autenticación de claves. A menudo se denomina <i>intercambio de claves autenticadas</i> .
Protocolo RSA	RSA	Protocolo de intercambio de claves que implica la generación y el transporte de claves. El protocolo recibe el nombre de sus tres creadores, Rivest, Shamir y Adleman.
Confidencialidad directa perfecta	PFS	Sólo se aplica en el intercambio de claves autenticadas. PFS garantiza que el material secreto a largo plazo para las claves no ponga en peligro la confidencialidad de las claves intercambiadas de comunicaciones anteriores. En PFS, la clave que se emplea para proteger la transmisión de datos no se aplica en la derivación de claves adicionales. La fuente de la clave que se usa para proteger la transmisión de datos tampoco se emplea en la derivación de claves adicionales.
Método Oakley		Método para establecer claves para la fase 2 de un modo seguro. Este protocolo es análogo al método Diffie-Hellman de intercambio de claves. De un modo similar a Diffie-Hellman, el intercambio de claves de grupo Oakley implica la generación de claves y la autenticación de claves. El método Oakley se utiliza para negociar PFS.

Intercambio de IKE de fase 1

El intercambio de fase 1 se conoce como *modo principal*. En el intercambio de fase 1, IKE utiliza métodos de cifrado de claves públicas para autenticarse con entidades IKE equivalentes. El resultado es una asociación de seguridad de Internet y una asociación de seguridad del protocolo de administración de claves (ISAKMP). Una asociación de seguridad ISAKMP es un canal seguro para que IKE negocie el material de claves para los datagramas IP. A diferencia de las asociaciones de seguridad de IPsec, las asociaciones de seguridad de ISAKMP son bidireccionales, de modo que sólo se necesita una asociación de seguridad.

El modo en que IKE negocia el material de claves en el intercambio de la fase 1 es configurable. IKE lee la información de configuración del archivo `/etc/inet/ike/config`. La información de configuración incluye:

- Parámetros globales, como los nombres de los certificados de claves públicas
- Si se utiliza confidencialidad directa perfecta (PFS)
- Las interfaces implicadas

- Los protocolos de seguridad y sus algoritmos
- El método de autenticación

Los dos métodos de autenticación son las claves previamente compartidas y los certificados de claves públicas. Los certificados de claves públicas pueden ser autofirmados. Los certificados también los puede emitir una [autoridad de certificación](#) desde una organización de infraestructuras de clave pública (PKI). Las organizaciones incluyen beTrusted, Entrust, GeoTrust, RSA Security y Verisign.

Intercambio de IKE de fase 2

El intercambio de fase 2 se conoce como *modo rápido (Quick)*. En el intercambio de fase 2, IKE crea y administra las asociaciones de seguridad de IPsec entre los sistemas que ejecutan el daemon de IKE. IKE utiliza el canal seguro creado en el intercambio de fase 1 para proteger la transmisión del material de claves. El daemon IKE crea las claves a partir de un generador de números aleatorio utilizando el dispositivo `/dev/random`. La velocidad a la que el daemon actualiza las claves se puede configurar. El material de claves está disponible para los algoritmos especificados en el archivo de configuración para la directiva IPsec, `ipsecinit.conf`.

Opciones de configuración de IKE

El archivo de configuración `/etc/inet/ike/config` contiene entradas de directiva IKE. Para que dos daemons IKE se autenticuen entre sí, las entradas deben ser válidas. Además, el material de claves debe estar disponible. Las entradas del archivo de configuración determinan el método para utilizar el material de claves para autenticar el intercambio de fase 1. Las opciones son las claves previamente compartidas o los certificados de claves públicas.

La entrada `auth_method preshared` indica que se utilizan claves previamente compartidas. Los valores de `auth_method` que no sean `preshared` indican que se deben utilizar certificados de claves públicas. Los certificados de claves públicas pueden ser autofirmados o instalarse desde una organización de PKI. Para más información, consulte la página del comando `man ike.config(4)`.

IKE con claves previamente compartidas

Las claves previamente compartidas las crea un administrador de un sistema. A continuación, se comparten las claves fuera de la banda con administradores de sistemas remotos. Debe procurar crear claves aleatorias largas y proteger el archivo y la transmisión fuera de banda. Las claves se colocan en el archivo `/etc/inet/secret/ike.preshared` de cada sistema. El archivo `ike.preshared` para IKE hace las funciones del archivo `ipseckey` para IPsec. Cualquier peligro para las claves del archivo `ike.preshared` pondrá en peligro todas las claves que se deriven de las claves del archivo.

La clave precompartida de un sistema debe ser idéntica a la clave de su sistema remoto. Las claves están vinculadas a una dirección IP específica. Las claves son más seguras cuando un administrador controla los sistemas que se comunican. Para obtener más información, consulte la página del comando `man ike.preshared(4)`.

IKE con certificados de claves públicas

Los certificados de claves públicas acaban con la necesidad de que los sistemas que se comunican compartan el material de claves secreto fuera de banda. Las claves públicas utilizan el [protocolo de Diffie-Hellman](#) (DH) para autenticar y negociar claves. Existen dos tipos de certificados de claves públicas. Los certificados pueden ser autofirmados o certificados por una [autoridad de certificación](#).

Los certificados de claves públicas autofirmados los crea el administrador. El comando `ikecert cert local -ks` crea la parte privada del par de claves pública-privada para el sistema. A continuación se obtiene el resultado del certificado autofirmado en formato X.509 del sistema remoto. El certificado del sistema remoto se incluye en el comando `ikecert certdb` para la parte pública del par de claves. Los certificados autofirmados se encuentran en el directorio `/etc/inet/ike/publickeys` de los sistemas que se comunican. Cuando se utiliza la opción `-T`, los certificados residen en el hardware conectado.

Los certificados autofirmados son un punto intermedio entre las claves previamente compartidas y las autoridades de certificación. A diferencia de las claves previamente compartidas, un certificado autofirmado se puede utilizar en un equipo portátil o en un sistema cuya numeración podría cambiar. Para autofirmar un certificado para un sistema sin un número fijo, utilice un nombre alternativo DNS (`www.example.org`) o `email (root@domain.org)`.

Las claves públicas se pueden entregar mediante PKI o una organización de autoridad de certificación. Las claves públicas y sus autoridades de certificación pertinentes se instalan en el directorio `/etc/inet/ike/publickeys`. Cuando se utiliza la opción `-T`, los certificados residen en el hardware conectado. Los proveedores también emiten listas de revocación de certificados (CRL). Junto con la instalación de las claves y las autoridades de certificación, debe instalar la CRL en el directorio `/etc/inet/ike/crls`.

Las autoridades de certificación tienen la ventaja de estar certificadas por una organización exterior, en lugar del administrador del sitio. En cierto modo, las autoridades de certificación son certificados autorizados. Al igual que ocurre con los certificados autofirmados, las autoridades de certificación se pueden utilizar en un equipo portátil o en un sistema cuya numeración podría cambiar. A diferencia de los certificados autofirmados, las autoridades de certificación se pueden escalar muy fácilmente para proteger una gran cantidad de sistemas que se comunican.

IKE y aceleración de hardware

Los algoritmos IKE requieren cálculos complejos, especialmente en el intercambio de fase 1. Los sistemas que controlan una gran cantidad de intercambios pueden utilizar una placa de Sun Crypto Accelerator 1000 para administrar las operaciones de claves públicas. Las placas de Sun Crypto Accelerator 4000 y Crypto Accelerator 6000 de Sun también se pueden utilizar para manejar cálculos de Fase 1 costosos.

Para obtener información sobre cómo configurar IKE para descargar sus cálculos en la placa del acelerador, consulte [“Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 1000” en la página 622](#). Para obtener información sobre cómo almacenar claves, consulte [“Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 4000” en la página 623](#) y la página del comando `man cryptoadm(1M)`.

IKE y almacenamiento de hardware

Los certificados de claves públicas, las claves privadas y las claves públicas se pueden almacenar en una placa Sun Crypto Accelerator 4000 o Crypto Accelerator 6000 de Sun. Para el cifrado [RSA](#), la placa Sun Crypto Accelerator 4000 admite claves de hasta 2.048 bits. Para el cifrado [DSA](#), la placa admite claves de hasta 1.024 bits. La placa Crypto Accelerator 6000 de Sun es compatible con los algoritmos SHA-512 y ECC.

Para obtener información sobre cómo configurar IKE para acceder a la placa, consulte [“Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 1000” en la página 622](#). Para obtener información sobre cómo agregar certificados y claves públicas a la placa, consulte [“Cómo generar y almacenar certificados de clave pública en el hardware” en la página 608](#).

Archivos y utilidades IKE

La siguiente tabla resume los archivos de configuración para la directiva IKE, las ubicaciones de almacenamiento para las claves IKE y los distintos comandos y servicios que implementan IKE. Para obtener más información sobre los servicios, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)” de Guía de administración del sistema: administración básica](#).

TABLA 22–2 Archivos de configuración de IKE, ubicaciones de almacenamiento de claves, comandos y servicios

Archivo, ubicación, comando o servicio	Descripción	Para obtener más información
<code>svc: /network/ipsec/ike</code>	En la versión actual, el servicio SMF que gestiona IKE.	smf(5)
<code>Daemon /usr/lib/inet/in.iked</code>	Daemon de intercambio de claves de Internet (IKE). Activa la administración de claves automática. En la versión actual, el servicio <code>ike</code> habilita este daemon. En las versiones anteriores, se utiliza el comando <code>in.iked</code> .	in.iked(1M)

TABLA 22-2 Archivos de configuración de IKE, ubicaciones de almacenamiento de claves, comandos y servicios
(Continuación)

Archivo, ubicación, comando o servicio	Descripción	Para obtener más información
Comando <code>/usr/sbin/ikeadm</code>	Comando de administración de IKE para ver y modificar la directiva IKE.	ikeadm(1M)
Comando <code>/usr/sbin/ikecert</code>	Comando de administración de bases de datos de certificados para administrar bases de datos locales que contienen certificados de claves públicas. Estas bases de datos también se puede almacenar en una placa de Sun Crypto Accelerator 4000 conectada.	ikecert(1M)
Archivo <code>/etc/inet/ike/config</code>	<p>Archivo de configuración predeterminada para la directiva IKE en el directorio <code>/etc/inet</code>. Contiene las reglas del sitio para hacer coincidir las solicitudes IKE entrantes y preparar las solicitudes IKE salientes.</p> <p>En la versión actual, si este archivo existe, el daemon en <code>iked</code> se inicia cuando el servicio <code>ike</code> está habilitado. El comando <code>svccfg</code> puede modificar la ubicación de este archivo.</p>	ike.config(4)
Archivo <code>ike.preshared</code>	Archivo de claves previamente compartidas del directorio <code>/etc/inet/secret</code> . Contiene material de claves secretas para autenticación en el intercambio de fase 1. Se utiliza al configurar IKE con claves previamente compartidas.	ike.preshared(4)
Directorio <code>ike.privatekeys</code>	Directorio de claves privadas del directorio <code>/etc/inet/secret</code> . Contiene las claves privadas que forman parte de un par de claves pública-privada.	ikecert(1M)
Directorio <code>publickeys</code>	Directorio del directorio <code>/etc/inet/ike</code> que contiene archivos de certificados y claves públicas. Contiene la parte de clave pública de un par de claves pública-privada.	ikecert(1M)
Directorio <code>cr1s</code>	Directorio del directorio <code>/etc/inet/ike</code> que incluye listas de revocación para archivos de certificados y claves públicas.	ikecert(1M)
Placa de Sun Crypto Accelerator 1000	Hardware que acelera las operaciones de claves públicas al descargar las operaciones del sistema operativo.	ikecert(1M)
Placa de Sun Crypto Accelerator 4000	Hardware que acelera las operaciones de claves públicas al descargar las operaciones del sistema operativo. La placa también almacena claves públicas, claves privadas y certificados de claves públicas.	ikecert(1M)

Cambios de IKE en Solaris 10

A partir de Solaris 9, IKE incluye las funciones siguientes:

- IKE se puede utilizar para automatizar el intercambio de claves para IPsec en redes IPv6. Para más información, consulte [“Administración de claves con IKE” en la página 576](#).

Nota – IKE no se puede utilizar para administrar claves para IPsec en una zona no global.

- Las operaciones de claves públicas de IKE se pueden acelerar mediante una placa de Sun Crypto Accelerator 1000 o una placa de Sun Crypto Accelerator 4000. Las operaciones se descargan en la placa. La descarga acelera el cifrado y reduce las exigencias con respecto al sistema operativo. Para mas información, consulte [“IKE y aceleración de hardware” en la página 580](#). Para conocer los procedimientos, consulte [“Configuración de IKE para buscar el hardware conectado \(mapa de tareas\)” en la página 622](#).
- Los certificados de claves públicas, las claves privadas y las claves públicas se pueden guardar en una placa de Sun Crypto Accelerator 4000. Para obtener más información sobre el almacenamiento de claves, consulte [“IKE y almacenamiento de hardware” en la página 580](#).
- IKE se puede utilizar para automatizar el intercambio de claves para IPsec desde un enrutador NAT. Sin embargo, las claves ESP IPsec a través de NAT no pueden acelerarse con hardware. Para más información, consulte [“Paso a través de IPsec y NAT” en la página 503](#). Para ver los procedimientos, consulte [“Configuración de IKE para sistemas portátiles \(mapa de tareas\)” en la página 614](#).
- Al archivo `/etc/inet/ike/config` se le han agregado parámetros de retransmisión y parámetros de tiempo de espera agotado de paquetes. Estos parámetros ajustan la negociación de IKE de fase 1 (modo principal) para administrar la interferencia de redes, el tráfico de red elevado y la interoperación con plataformas que tienen diferentes implementaciones del protocolo IKE. Para obtener más información sobre los parámetros, consulte la página del comando `man ike.config(4)` Para ver los procedimientos, consulte [“Cambio de los parámetros de transmisión de IKE \(mapa de tareas\)” en la página 625](#).

Configuración de IKE (tareas)

En este capítulo se describe cómo configurar Internet Key Exchange (IKE) para sus sistemas. Una vez configurado IKE, se genera automáticamente material de claves para IPsec en la red. Este capítulo contiene la información siguiente:

- “Configuración de IKE (mapa de tareas)” en la página 583
- “Configuración de IKE con claves previamente compartidas (mapa de tareas)” en la página 584
- “Configuración de IKE con certificados de clave pública (mapa de tareas)” en la página 595
- “Configuración de IKE para sistemas portátiles (mapa de tareas)” en la página 614
- “Configuración de IKE para buscar el hardware conectado (mapa de tareas)” en la página 622
- “Cambio de los parámetros de transmisión de IKE (mapa de tareas)” en la página 625

Para obtener una descripción general sobre IKE, consulte el [Capítulo 22, “Intercambio de claves de Internet \(descripción general\)”](#). Para obtener información de referencia sobre IKE, consulte el [Capítulo 24, “Intercambio de claves de Internet \(referencia\)”](#). Para ver más procedimientos, consulte las secciones de ejemplos de las páginas del comando `man ikeadm(1M)`, `ikecert(1M)` y `ike.config(4)`.

Configuración de IKE (mapa de tareas)

Para autenticar IKE puede utilizar claves previamente compartidas, certificados autofirmados y certificados de una autoridad de certificación. Una regla vincula el método de autenticación de IKE específico con los puntos finales que se están protegiendo. Por tanto, puede utilizar uno o todos los métodos de autenticación de IKE de un sistema. Un puntero a una biblioteca PKCS #11 permite a los certificados utilizar un acelerador de hardware conectado.

Una vez configurado IKE, complete la tarea de IPsec que utilice la configuración de IKE. La tabla siguiente hace referencia a los mapas de tareas que se centran en una configuración de IKE específica.

Tarea	Descripción	Para obtener instrucciones
Configurar IKE con claves previamente compartidas	Protege la comunicación entre dos sistemas al hacer que dos sistemas compartan una clave secreta.	“Configuración de IKE con claves previamente compartidas (mapa de tareas)” en la página 584
Configurar IKE con certificados de clave pública	Protege las comunicaciones con certificados de clave pública. Los certificados pueden ser autofirmados o comprobados por una organización de PKI.	“Configuración de IKE con certificados de clave pública (mapa de tareas)” en la página 595
Cruzar un límite de NAT	Configura IPsec e IKE para comunicarse con un sistema portátil.	“Configuración de IKE para sistemas portátiles (mapa de tareas)” en la página 614
Configurar IKE para generar y guardar certificados de clave pública en el hardware conectado	Permite a una placa Sun Crypto Accelerator 1000 o Sun Crypto Accelerator 4000 acelerar las operaciones de IKE. También permite a las placas Sun Crypto Accelerator 4000 guardar certificados de clave pública.	“Configuración de IKE para buscar el hardware conectado (mapa de tareas)” en la página 622
Ajustar parámetros de negociación de clave de fase 1	Cambia el tiempo de las negociaciones de claves IKE.	“Cambio de los parámetros de transmisión de IKE (mapa de tareas)” en la página 625

Configuración de IKE con claves previamente compartidas (mapa de tareas)

En la tabla siguiente se incluyen los procedimientos para configurar y mantener IKE con claves previamente compartidas.

Tarea	Descripción	Para obtener instrucciones
Configurar IKE con claves previamente compartidas	Crea un archivo de directiva IKE y una clave para compartir.	“Cómo configurar IKE con claves previamente compartidas” en la página 585
Actualizar claves previamente compartidas en un sistema IKE en ejecución	Agrega nuevo material de claves para IKE en los sistemas que se comunican.	“Cómo actualizar las claves IKE previamente compartidas” en la página 588
Agregar claves previamente compartidas a un sistema IKE en ejecución	Agrega una nueva entrada de directiva IKE y nuevo material de claves en un sistema que está aplicando la directiva IKE.	“Cómo agregar una clave IKE previamente compartida para una nueva entrada de directiva en ipsecinit.conf” en la página 591
Comprobar que las claves previamente compartidas sean idénticas	Muestra las claves previamente compartidas en ambos sistemas para comprobar que las claves sean idénticas.	“Verificación de que las claves IKE previamente compartidas sean idénticas” en la página 594

Configuración de IKE con claves previamente compartidas

Las claves previamente compartidas constituyen el método de autenticación más sencillo para IKE. Si esta configurando dos sistemas para que utilicen IKE y es el administrador de ambos sistemas, se recomienda utilizar claves previamente compartidas. Sin embargo, a diferencia de los certificados de clave pública, las claves previamente compartidas están vinculadas a direcciones IP específicas. Las claves previamente compartidas no se pueden utilizar con sistemas portátiles o sistemas cuya numeración podría variar. Además, al utilizar claves previamente compartidas, no es posible descargar los cálculos de IKE en el hardware conectado.

▼ Cómo configurar IKE con claves previamente compartidas

La implementación de IKE ofrece algoritmos con claves cuya longitud varía. La longitud de claves que elija dependerá de la seguridad del sitio. En general, las claves largas son más seguras que las cortas.

Estos procedimientos utilizan los nombres de sistema `enigma` y `partym`. Sustituya los nombres de los sistemas con los nombres `enigma` y `partym`.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 En cada sistema, copie el archivo `/etc/inet/ike/config.sample` al archivo `/etc/inet/ike/config`.

3 Especifique las reglas y los parámetros generales en el archivo `ike/config` de cada sistema.

Las reglas y los parámetros generales de este archivo deberían permitir la correcta aplicación de la directiva IPsec en el archivo `ipsecinit.conf` del sistema. Los siguientes ejemplos de `ike/config` funcionan con los ejemplos de `ipsecinit.conf` de [“Cómo proteger el tráfico entre dos sistemas con IPsec”](#) en la página 511.

a. Por ejemplo, modifique el archivo `/etc/inet/ike/config` del sistema `enigma`:

```
### ike/config file on enigma, 192.168.116.16

## Global parameters
```

```
#
## Phase 1 transform defaults
p1_lifetime_secs 14400
p1_nonce_len 40
#
## Defaults that individual rules can override.
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 2
#
## The rule to communicate with partym
# Label must be unique
{ label "enigma-partym"
  local_addr 192.168.116.16
  remote_addr 192.168.13.213
  p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
  p2_pfs 5
}
```

Nota – Todos los argumentos del parámetro `auth_method` deben encontrarse en la misma línea.

b. Modifique el archivo `/etc/inet/ike/config` del sistema `partym`:

```
### ike/config file on partym, 192.168.13.213
## Global Parameters
#
p1_lifetime_secs 14400
p1_nonce_len 40
#
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 2

## The rule to communicate with enigma
# Label must be unique
{ label "partym-enigma"
  local_addr 192.168.13.213
  remote_addr 192.168.116.16
  p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
  p2_pfs 5
}
```

4 En cada sistema, compruebe la sintaxis del archivo.

```
# /usr/lib/inet/in.iked -c -f /etc/inet/ike/config
```

5 Genere números aleatorios para utilizar como material de claves.

Si su sitio cuenta con un generador de números aleatorios, utilícelo. En un sistema Solaris, puede utilizar el comando `od`. Por ejemplo, el siguiente comando imprime dos líneas de números hexadecimales:

```
% od -X -A n /dev/random | head -2
f47cb0f4 32e14480 951095f8 2b735ba8
```

```
0a9467d0 8f92c880 68b6a40e 0efe067d
```

Para ver una explicación del comando `od`, consulte [“Cómo generar números aleatorios en un sistema Solaris” en la página 519](#) y la página del comando `man od(1)`.

Nota – Otros sistemas operativos pueden requerir material de claves ASCII. Para generar una clave idéntica en los formatos hexadecimal y ASCII, consulte el [Ejemplo 23-1](#).

6 Cree una clave a partir del resultado obtenido en el Paso 5.

```
f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
```

El algoritmo de autenticación de este procedimiento es SHA-1, tal como se muestra en el [Paso 3](#). El tamaño del hash, es decir, el tamaño del resultado del algoritmo de autenticación, determina el tamaño mínimo recomendado de una clave previamente compartida. El resultado del algoritmo SHA-1 es 160 bits o 40 caracteres. La clave de ejemplo tiene una longitud de 56 caracteres, que proporciona material de claves adicional para usar en IKE.

7 Cree el archivo `/etc/inet/secret/ike.preshared` en cada sistema.

Coloque la clave previamente compartida en cada archivo.

a. Por ejemplo, en el sistema `enigma`, el archivo `ike.preshared` tendría el siguiente aspecto:

```
# ike.preshared on enigma, 192.168.116.16
#...
{ localidtype IP
  localid 192.168.116.16
  remoteidtype IP
  remoteid 192.168.13.213
  # enigma and partym's shared key in hex (192 bits)
  key f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
}
```

b. En el sistema `partym`, el archivo `ike.preshared` tendría el siguiente aspecto:

```
# ike.preshared on partym, 192.168.13.213
#...
{ localidtype IP
  localid 192.168.13.213
  remoteidtype IP
  remoteid 192.168.116.16
  # partym and enigma's shared key in hex (192 bits)
  key f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
}
```

Nota – Las claves previamente compartidas de cada sistema deben ser idénticas.

Ejemplo 23-1 Generación de material de claves idéntico para dos sistemas con diferentes sistemas operativos

Solaris IPsec interopera con otros sistemas operativos. Si su sistema se comunica con un sistema que requiere claves previamente compartidas ASCII, debe generar una clave en dos formatos, hexadecimal y ASCII.

En este ejemplo, el administrador del sistema Solaris desea material de claves de 56 caracteres. El administrador utiliza el comando siguiente para generar una clave hexadecimal a partir de una contraseña ASCII. La opción `-tx1` imprime los bytes uno a uno en todos los sistemas Solaris.

```
# /bin/echo "papiermache with cashews and\c" | od -tx1 | cut -c 8-55 | \
tr -d '\n' | tr -d ' ' | awk '{print}'
7061706965726d616368652077697468206361736865777320616e64
```

Al eliminar los desfases y concatenar el resultado hexadecimal, la clave hexadecimal del sistema Solaris es `7061706965726d616368652077697468206361736865777320616e64`. El administrador coloca este valor en el archivo `ike.preshared` del sistema Solaris.

```
# Shared key in hex (192 bits)
key 7061706965726d616368652077697468206361736865777320616e64
```

En el sistema que requiere claves previamente compartidas ASCII, la contraseña es la clave previamente compartida. El administrador del sistema Solaris comunica por teléfono la contraseña (`papiermache with cashews and`) al otro administrador.

▼ Cómo actualizar las claves IKE previamente compartidas

Este procedimiento presupone que desea reemplazar una clave previamente compartida a intervalos regulares.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Genere números aleatorios y cree una clave con la longitud adecuada.

Para obtener más información, consulte [“Cómo generar números aleatorios en un sistema Solaris” en la página 519](#). Si va a generar una clave previamente compartida para un sistema Solaris que se comunica con un sistema operativo que requiere ASCII, consulte el [Ejemplo 23-1](#).

3 Sustituya la clave actual por una nueva.

Por ejemplo, en los hosts `enigma` y `partym`, debe reemplazar el valor de `key` en el archivo `/etc/inet/secret/ike.preshared` con un nuevo número que tenga la misma longitud.

4 Lea la nueva clave en el núcleo.

- A partir de la versión Solaris 10 4/09, actualice el servicio `ike`.

```
# svcadm refresh ike
```

- Si está ejecutando una versión anterior a la Solaris 10 4/09, finalícela y reinicie el daemon `in.iked`.

a. Compruebe el nivel de privilegio del daemon `in.iked`.

```
# /usr/sbin/ikeadm get priv
Current privilege level is 0x0, base privileges enabled
```

Puede cambiar el material de claves si el comando devuelve un nivel de privilegio de `0x1` o `0x2`. El nivel `0x0` no permite a las operaciones modificar ni ver el material de claves. De modo predeterminado, el daemon `in.iked` se ejecuta en el nivel de privilegio `0x0`.

b. Si el nivel de privilegio es `0x0`, finalice el daemon y reinicielo.

Al reiniciar el daemon, lee la nueva versión del archivo `ike.preshared`.

```
# pkill in.iked
# /usr/lib/inet/in.iked
```

c. Si el nivel de privilegio es `0x1` o `0x2`, lea la nueva versión del archivo `ike.preshared`.

```
# ikedadm read preshared
```

▼ Cómo ver las claves IKE previamente compartidas

Por defecto, el comando `ikedadm` impide que vea las teclas reales en un volcado de una fase 1 SA. La visualización de las claves es útil durante la depuración.

Para ver las teclas reales, debe aumentar el nivel de privilegios del daemon. Para obtener una descripción de los niveles de privilegios, consulte [“Comando de administración de IKE” en la página 631](#).

Nota – Para llevar a cabo este procedimiento en una versión anterior a Solaris 10 4/09 consulte [Ejemplo 23–2](#).

Antes de empezar

IKE se configura y el servicio `ike` se ejecuta.

1 Consulte las teclas previamente compartidas de IKE.

```
# ikeadm
ikeadm> dump preshared
```

2 Si aparece un mensaje de error, aumente el nivel de privilegios del daemon `in.iked`.

a. Aumente el nivel de privilegios del daemon `in.iked` en el repositorio SMF.

```
# svcprop -p config/admin_privilege ike
base
# svccfg -s ike setprop config/admin_privilege=keymat
```

b. Aumente el nivel de privilegios del daemon `in.iked` en ejecución.

```
# svcadm refresh ike ; svcadm restart ike
```

c. (Opcional) Confirme que el nivel de privilegios es `keymat`.

```
# svcprop -p config/admin_privilege ike
keymat
```

d. Ejecute de nuevo el [Paso 1](#) para ver las teclas.

3 Devuelva al daemon IKE el nivel de privilegios base.

a. Después de ver las claves, devuelva al nivel de privilegios el valor predeterminado.

```
# svccfg -s ike setprop config/admin_privilege=base
```

b. Actualice y, a continuación, reinicie IKE.

```
# svcadm refresh ike ; svcadm restart ike
```

Ejemplo 23–2 Verificación de las claves IKE compartidas previamente en una versión anterior a Solaris 10 4/09

En el siguiente ejemplo, el administrador está consultando claves en un sistema Solaris que no ejecuta la versión actual de Solaris. El administrador desea comprobar que las claves de este sistema son idénticas a las del sistema de comunicación. Después de comprobar que las claves de los dos sistemas son idénticos, el administrador restablece el nivel de privilegios a 0.

- En primer lugar, el administrador determina el nivel de privilegios del daemon `in.iked`.

```
adm1 # /usr/sbin/ikeadm get priv
Current privilege level is 0x0, base privileges enabled
```

- Debido a que el nivel de privilegios no es 0x1 o 0x2, el administrador detiene el daemon `in.iked` y, a continuación, aumenta el nivel de privilegios a 2.

```
adm1 # pkill in.iked
adm1 # /usr/lib/inet/in.iked -p 2
Setting privilege level to 2
```

- El administrador muestra las claves.

```
adm1 # ikeadm dump preshared
PSKEY: Preshared key (24 bytes): f47cb.../192
LOCIP: AF_INET: port 0, 192.168.116.16 (adm1).
REMIP: AF_INET: port 0, 192.168.13.213 (com1).
```

- El administrador inicia sesión remota en el sistema de comunicación y determina que las claves sean idénticas.
- A continuación, el administrador restablece el nivel básico de privilegios.

```
# ikeadm set priv base
```

▼ Cómo agregar una clave IKE previamente compartida para una nueva entrada de directiva en `ipsecinit.conf`

Si agrega entradas de la directiva IPsec, mientras se ejecutan IPsec e IKE, deberá leer la nueva directiva y las reglas IKE en el núcleo. A partir de la versión Solaris 10 4/09, reinicie el servicio de directivas y actualice el servicio `ike` después de agregar las nuevas claves.

Nota – Para llevar a cabo este procedimiento en una versión anterior a Solaris 10 4/09, consulte el [Ejemplo 23–3](#).

Antes de empezar

Este procedimiento presupone lo siguiente:

- El sistema `enigma` está configurado de acuerdo con lo descrito en “[Cómo configurar IKE con claves previamente compartidas](#)” en la página 585.
- El sistema `enigma` va a proteger su tráfico con un nuevo sistema, `ada`.
- El daemon `in.iked` se ejecuta en ambos sistemas.
- Las interfaces de los sistemas se incluyen como entradas en el archivo `/etc/hosts` de ambos sistemas. La entrada siguiente es un ejemplo.

```
192.168.15.7 ada
192.168.116.16 enigma
```

Este procedimiento también funciona con una dirección IPv6 en el archivo `/etc/inet/ipnodes`. A partir de la versión Solaris 10 6/07 las entradas IPv6 se colocan en el archivo `/etc/hosts`.

- Ha agregado una nueva entrada de directiva en el archivo `/etc/inet/ipsecinit.conf` en ambos sistemas. Las entradas tienen el siguiente aspecto:

```
# ipsecinit.conf file for enigma
{laddr enigma raddr ada} ipsec {auth_algs any encr_algs any sa shared}

# ipsecinit.conf file for ada
{laddr ada raddr enigma} ipsec {auth_algs any encr_algs any sa shared}
```

- En la versión actual, ha comprobado la sintaxis del archivo `/etc/inet/ipsecinit.conf` en ambos sistemas mediante lo siguiente:

```
# ipseconf -c -f /etc/inet/ipsecinit.conf
```

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 En este sistema, genere números aleatorios y cree una clave de entre 64 y 448 bits.

Para obtener más información, consulte “[Cómo generar números aleatorios en un sistema Solaris](#)” en la [página 519](#). Si va a generar una clave previamente compartida para un sistema Solaris que se comunica con un sistema operativo que requiere ASCII, consulte el [Ejemplo 23–1](#).

3 Envíe la clave al administrador del sistema remoto.

Ambos deben agregar la misma clave previamente compartida y de forma simultánea. La seguridad de su clave depende de la seguridad de su mecanismo de transmisión. Se recomienda un mecanismo fuera de banda, como un correo registrado o un fax protegido. También puede utilizar una sesión `ssh` para administrar ambos sistemas.

4 Cree una regla para que IKE administre las claves para enigma y ada.

a. En el sistema enigma, agregue la regla siguiente al archivo `/etc/inet/ike/config`:

```
### ike/config file on enigma, 192.168.116.16

## The rule to communicate with ada

{label "enigma-to-ada"
 local_addr 192.168.116.16
 remote_addr 192.168.15.7
 pl_xform
 {auth_method preshared oakley_group 5 auth_alg sha1 encr_alg blowfish}}
```



```
p2_pfs 5
}
```

b. En el sistema ada, agregue la siguiente regla:

```
### ike/config file on ada, 192.168.15.7

## The rule to communicate with enigma

{label "ada-to-enigma"
 local_addr 192.168.15.7
 remote_addr 192.168.116.16
 p1_xform
 {auth_method preshared oakley_group 5 auth_alg sha1 encr_alg blowfish}
 p2_pfs 5
}
```

5 Asegúrese de que haya claves IKE previamente compartidas al iniciar.

a. En el sistema enigma, agregue la siguiente información al archivo `/etc/inet/secret/ike.preshared`:

```
# ike.preshared on enigma for the ada interface
#
{ localidtype IP
  localid 192.168.116.16
  remoteidtype IP
  remoteid 192.168.15.7
  # enigma and ada's shared key in hex (32 - 448 bits required)
  key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d
}
```

b. En el sistema ada, agregue la información siguiente al archivo `ike.preshared`:

```
# ike.preshared on ada for the enigma interface
#
{ localidtype IP
  localid 192.168.15.7
  remoteidtype IP
  remoteid 192.168.116.16
  # ada and enigma's shared key in hex (32 - 448 bits required)
  key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d
}
```

6 En cada sistema, reinicie el servicio de directivas de IPsec para asegurar la interfaz agregada.

```
# svcadm restart policy
```

7 En cada sistema, actualice el servicio ike.

```
# svcadm refresh ike
```

8 Compruebe que los sistemas se puedan comunicar.

Consulte [“Verificación de que las claves IKE previamente compartidas sean idénticas” en la página 594.](#)

Ejemplo 23–3 Adición de una clave IKE compartida previamente para una nueva entrada de directiva IPsec

En el siguiente ejemplo, el administrador agrega una clave compartida previamente a un sistema Solaris que no ejecuta la versión actual de Solaris. El administrador sigue el procedimiento anterior para modificar los archivos `ike/config` e `ike.`, así como generar las claves y establecer contacto con el sistema remoto. El administrador utiliza comandos diferentes para leer la nueva directiva IPsec y las reglas IKE en el núcleo.

- Antes de generar la nueva tecla, el administrador define el nivel de privilegios del daemon `in.iked` en 2.

```
# pkill in.iked
# /usr/lib/inet/in.iked -p 2
Setting privilege level to 2
```

- Después de enviar la tecla para el otro sistema y agregar la nueva tecla al sistema, el administrador reduce el nivel de privilegios.

```
# ikeadm set priv base
```

- A continuación, el administrador lee la nueva directiva IPsec en el núcleo.

```
# ipseconf -a /etc/inet/ipsecinit.conf
```

- Por último, el administrador lee las nuevas reglas IKE en el núcleo.

```
# ikeadm read rules
```

▼ Verificación de que las claves IKE previamente compartidas sean idénticas

Si las claves previamente compartidas de los sistemas que se comunican no son idénticas, los sistemas no se podrán autenticar.

Antes de empezar IPsec se ha configurado y se ha habilitado entre los dos sistemas que se están probando. Se está ejecutando la versión Solaris 10 actual.

Nota – Para llevar a cabo este procedimiento en una versión anterior a Solaris 10 4/09 consulte [Ejemplo 23–2](#).

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 En cada sistema, compruebe el nivel de privilegios del daemon `in.iked`.

```
# svcprop -p config/admin_privilege ike
base
```

- Si el nivel de privilegios es `keymat`, continúe con el [Paso 3](#).
- Si el nivel de privilegios es `base` o `modkeys`, aumente su nivel.

A continuación, actualice el servicio `ike` y reinícielo.

```
# svccfg -s ike setprop config/admin_privilege=keymat
# svcadm refresh ike ; svcadm restart ike
# svcprop -p config/admin_privilege ike
keymat
```

3 En cada sistema, visualice la información de claves previamente compartidas.

```
# ikeadm dump preshared
PSKEY: Preshared key (24 bytes): f47cb.../192
LOCIP: AF_INET: port 0, 192.168.116.16 (enigma).
REMIP: AF_INET: port 0, 192.168.13.213 (partym).
```

4 Compare los dos vaciados.

Si las claves previamente compartidas no son idénticas, sustituya una de ellas con la otra en el archivo `/etc/inet/secret/ike.preshared`.

5 Cuando se haya completado la verificación, devuelva al nivel de privilegios el valor predeterminado de cada sistema.

```
# svccfg -s ike setprop config/admin_privilege=base
# svcadm restart ike
```

Configuración de IKE con certificados de clave pública (mapa de tareas)

La tabla siguiente incluye los procedimientos para crear certificados de clave pública para IKE. Entre estos procedimientos se incluye cómo acelerar y guardar los certificados en el hardware conectado.

Tarea	Descripción	Para obtener instrucciones
Configurar IKE con certificados de clave pública autofirmados	Crea y coloca dos certificados en cada sistema: <ul style="list-style-type: none">■ Un certificado autofirmado■ El certificado de clave pública del sistema remoto	“Cómo configurar IKE con certificados de clave pública autofirmados” en la página 596
Configurar IKE con una autoridad de certificación de PKI	Crea una solicitud de certificado y coloca tres certificados en cada sistema: <ul style="list-style-type: none">■ El certificado que crea la autoridad de certificación a partir de su solicitud■ El certificado de clave pública de la autoridad de certificación■ La lista CRL de la autoridad de certificación	“Cómo configurar IKE con certificados firmados por una autoridad de certificación” en la página 602
Configurar certificados de clave pública en el hardware local	Implica una de estas acciones: <ul style="list-style-type: none">■ Generar un certificado autofirmado en el hardware local y luego agregar la clave pública de un sistema remoto al hardware■ Generar una solicitud de certificado en el hardware local y luego agregar los certificados de clave pública de la autoridad de certificación al hardware	“Cómo generar y almacenar certificados de clave pública en el hardware” en la página 608
Actualizar la lista de revocación de certificados (CRL) desde PKI	Accede a la CRL desde un punto de distribución central.	“Cómo administrar una lista de revocación de certificados” en la página 612

Configuración de IKE con certificados de clave pública

Los certificados de clave pública acaban con la necesidad de que los sistemas que se comunican compartan material de claves secreto fuera de banda. A diferencia de las claves previamente compartidas, un certificado de clave pública se puede utilizar en un equipo portátil o en un sistema cuya numeración podría cambiar.

Los certificados de clave pública también podrían guardarse en el hardware conectado. Para conocer el procedimiento, consulte [“Configuración de IKE para buscar el hardware conectado \(mapa de tareas\)” en la página 622](#).

▼ Cómo configurar IKE con certificados de clave pública autofirmados

Los certificados autofirmados requieren menos carga que los certificados públicos de una autoridad de certificación, pero no se escalan fácilmente.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Agregue un certificado autofirmado a la base de datos `ike.privatekeys`.

```
# ikecert certlocal -ks|-kc -m keysize -t keytype \
-D dname -A altname \
[-S validity-start-time] [-F validity-end-time] [-T token-ID]
```

-ks	Crea un certificado autofirmado.
-kc	Crea una solicitud de certificado. Para conocer el procedimiento, consulte “Cómo configurar IKE con certificados firmados por una autoridad de certificación” en la página 602.
-m tamaño_clave	Es el tamaño de la clave. <i>Tamaño_clave</i> puede ser 512, 1024, 2048, 3072 o 4096.
-t tipo_clave	Especifica el tipo de algoritmo que utilizar. <i>Tipo_algoritmo</i> puede ser <code>rsa-sha1</code> , <code>rsa-md5</code> o <code>dsa-sha1</code> .
-D nombre_d	Es el nombre X.509 distinguido para el tema del certificado. <i>Nombre_d</i> suele tener el formato siguiente: <code>C=country</code> (país), <code>O=organization</code> (organización=, <code>OU=organizational unit</code> (unidad organizativa), <code>CN=common name</code> (nombre común). Las etiquetas válidas son C, O, OU y CN.
-A nombre_alt	Nombre alternativo del certificado. <i>Nombre_alt</i> tiene el formato <code>tag=value</code> . Las etiquetas válidas son IP, DNS, email y DN.
-S tiempo_inicio_validez	Proporciona un tiempo de inicio de validez absoluto o relativo para el certificado.
-F tiempo_fin_validez	Proporciona un tiempo de fin de validez absoluto o relativo para el certificado.
-T ID_token	Permite al token de hardware PKCS #11 generar las claves. Los certificados se guardan en el hardware.

a. Por ejemplo, el comando del sistema `partym` sería como el siguiente:

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
```

```

-A IP=192.168.13.213
Creating software private keys.
Writing private key to file /etc/inet/secret/ike.privatekeys/0.
Enabling external key providers - done.
Acquiring private keys for signing - done.
Certificate:
Proceeding with the signing operation.
Certificate generated successfully (.../publickeys/0)
Finished successfully.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIICLTCCAzagAwIBAgIBATANBgkqhkiG9w0BAQQFADBQMwswCQYDVQQGEwJVUzEX
...
6sKTxpg4GP3GkQGcd0r1rhW/3yaWBkDwOdFCqEUyffzU
-----END X509 CERTIFICATE-----

```

b. El comando del sistema enigma sería como el siguiente:

```

# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax" \
-A IP=192.168.116.16
Creating software private keys.
...
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIICKDCCAzagAwIBAgIBATANBgkqhkiG9w0BAQQFADBQMwswCQYDVQQGEwJVUzEV
...
jpxfLM98xyFVyLCbkr3dZ3Tvxxvi732BXePKF2A==
-----END X509 CERTIFICATE-----

```

3 Guarde el certificado y envíelo al sistema remoto.

El certificado se puede pegar en un mensaje de correo electrónico.

a. Por ejemplo, enviaría el siguiente certificado de partym al administrador de enigma:

```

To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIICLTCCAzagAwIBAgIBATANBgkqhkiG9w0BAQQFADBQMwswCQYDVQQGEwJVUzEX
...
6sKTxpg4GP3GkQGcd0r1rhW/3yaWBkDwOdFCqEUyffzU
-----END X509 CERTIFICATE-----

```

b. El administrador de enigma enviaría el siguiente certificado de enigma:

```

To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIICKDCCAzagAwIBAgIBATANBgkqhkiG9w0BAQQFADBQMwswCQYDVQQGEwJVUzEV
...
jpxfLM98xyFVyLCbkr3dZ3Tvxxvi732BXePKF2A==
-----END X509 CERTIFICATE-----

```

4 En cada sistema, agregue el certificado que reciba.

a. Copie la clave pública del correo electrónico del administrador.

b. Escriba el comando `ikecert certdb -a` y pulse la tecla Intro.

Al pulsar Intro no aparecerá ningún mensaje.

```
# ikecert certdb -a      Press the Return key
```

c. Pegue la clave pública. A continuación, pulse la tecla Intro. Para finalizar la entrada, pulse Control+D.

```
-----BEGIN X509 CERTIFICATE-----
MIIC...
...
-----END X509 CERTIFICATE-----      Press the Return key
<Control>-D
```

5 Verifique con el otro administrador que el certificado proceda de dicho administrador.

Por ejemplo, puede llamar por teléfono al otro administrador para comparar los valores de hash de clave pública. El hash de clave pública del certificado compartido debe ser idéntico en los dos sistemas.

a. Enumere el certificado guardado en su sistema.

Por ejemplo, en el sistema partym, el certificado público se encuentra en la ranura 1 y el certificado privado se encuentra en la ranura 0.

```
partym # ikecert certdb -l
Certificate Slot Name: 0   Type: rsa-md5      Private Key
  Subject Name: <C=US, O=PartyCompany, OU=US-Partym, CN=Partym>
  Key Size: 1024
  Public key hash: B2BD13FCE95FD27ECE6D2DCD0DE760E2

Certificate Slot Name: 1   Type: rsa-md5      Public Certificate
  (Private key in certlocal slot 0)      Points to certificate's private key
  Subject Name: <C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax>
  Key Size: 1024
  Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

b. Compare este valor con el hash de clave pública del sistema enigma.

El hash de clave pública se puede comunicar por teléfono.

```
enigma # ikecert certdb -l
Certificate Slot Name: 4   Type: rsa-md5      Private Key
  Subject Name: <C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax>
  Key Size: 1024
  Public key hash: DF3F108F6AC669C88C6BD026B0FCE3A0
```

```
Certificate Slot Name: 5    Type: rsa-md5    Public Certificate
(Private key in certlocal slot 4)
Subject Name: <C=US, O=PartyCompany, OU=US-Partym, CN=Partym>
Key Size: 1024
Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

6 En cada sistema, confíe en ambos certificados.

Edita el archivo `/etc/inet/ike/config` para reconocer los certificados.

El administrador del sistema remoto proporciona los valores para los parámetros `cert_trust`, `remote_addr` y `remote_id`.

a. Por ejemplo, en el sistema `partym`, el archivo `ike/config` tendría el siguiente aspecto:

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

# Verified remote address and remote ID
# Verified public key hash per telephone call from administrator
cert_trust "192.168.13.213"    Local system's certificate Subject Alt Name
cert_trust "192.168.116.16"   Remote system's certificate Subject Alt Name

## Parameters that may also show up in rules.

p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 5

{
  label "US-partym to JA-enigmax"
  local_id_type dn
  local_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
  remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

  local_addr 192.168.13.213
  remote_addr 192.168.116.16

  p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

b. En el sistema `enigma`, agregue los valores de `enigma` para los parámetros locales en el archivo `ike/config`.

Para los parámetros remotos, utilice los valores de `partym`. Asegúrese de que el valor de la palabra clave `label` sea único. Este valor debe ser diferente del valor `label` del sistema remoto.

```
...
{
```



```

label "JA-enigmax to US-party"
local_id_type dn
local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

local_addr 192.168.116.16
remote_addr 192.168.13.213
...

```

Ejemplo 23-4 Verificación de la validez de un certificado procedente de otro administrador

En este ejemplo, los administradores recurren al nombre del asunto para verificar que los certificados sean idénticos.

El primer administrador guarda la salida de la generación y hace constar el certificado en un archivo. Debido a que la salida del comando `ikecert` imprime un error estándar, el administrador redirige el error estándar al archivo.

```

sys1# cd /
sys1# ikecert certlocal -ks -m1024 -t rsa-md5 \
-D"C=US, O=TestCo, CN=Co2Sys" 2>/tmp/for_co2sys
Certificate added to database.
sys1# ikecert certdb -l "C=US, O=TestCo, CN=Co2Sys" 2>>/tmp/for_co2sys

```

El administrador verifica el contenido del archivo.

```

sys1# cat /tmp/for_co2sys
Creating private key.
-----BEGIN X509 CERTIFICATE-----
MIIB7TCCAVarAwIBAgIEZkHfOTANBgkqhkiG9w0BAQQFADAMQwwCgYDVQQGEwNV
U0ExEDAOBgNVBAoMB3Rlc3RfY28xDzANBgNVBAMTBkVuaWdtYTAeFw0wODAxMTUx
OTI1MjBaFw0xMjAxMTUxOTI1MjBaMDExDDAKBgNVBAYTA1VTQTEQMA4GA1UECgwH
dGVzdF9jb2EPMA0GA1UEAxMGRW5pZ2Z1hMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQCPCxGv0rUzHMnFtkx9uwYuPiWbftmWfa9iDt6ELOEuW3zlb0y2qtuRUZoh
FIbCxAJevdCY6a+pktyYy3/2nJL0WATOb05T0FKn3F0bphajinLYbyCrYhEzD9E2
gkiT2D9/ttbSiMvi9usphprEDcLAFaWgCJiHnKPBEkjC0vhA3wIDAQABoxIwEDA0
BgNVHQ8BAf8EBAMCBAAwDQYJKoZIhvcNAQEEBQADgYEAL/q6xgweylGQylqLCwzN
5PIpjfzsNPf3saTyh3VplwEOW6WTHwRQT17IO/10c6Jnz9Mr0ZrbHWDXq+1sX180
F8+DMWlQv1UR/LGMq3ufDG3qedmSN6txDF8qLLPCUML0YL8m4oGdewqGb+78aPYE
Y/cJRsk1hWbYyseqcIkjj5k=
-----END X509 CERTIFICATE-----
Certificate Slot Name: 2    Key Type: rsa
(Private key in certlocal slot 2)
Subject Name: <C=US, O=TestCo, CN=Co2Sys>
Key Size: 1024
Public key hash: C46DE77EF09084CE2B7D9C70479D77FF

```

A continuación, el administrador envía el archivo al segundo administrador por correo electrónico.

El segundo administrador coloca el archivo en un directorio seguro e importa el certificado del archivo.

```
sys2# cd /
sys2# ikecert certdb -a < /sec/co2sys
```

El comando `ikecert` importa únicamente el texto que hay entre las líneas `-----BEGIN` y `-----END`. El administrador verifica que el certificado local tenga el mismo valor hash de clave pública que el valor hash de clave pública que haya en el archivo `co2sys`.

```
sys2# ikecert certdb -l
Certificate Slot Name: 1   Key Type: rsa
    (Private key in certlocal slot 1)
    Subject Name: <C=US, O=TestCo, CN=Co2Sys>
    Key Size: 1024
    Public key hash: C46DE77EF09084CE2B7D9C70479D77FF
```

Para asegurarse de que el primer administrador envíe este correo electrónico, el segundo administrador telefonea al primero para verificar el nombre del asunto del certificado.

Ejemplo 23-5 Especificación de un tiempo de inicio y un tiempo de fin para un certificado

En este ejemplo, el administrador del sistema `partym` establece las fechas durante las cuales el certificado es válido. El certificado será anterior en dos días y medio, y será válido para 4 años y 6 meses a partir de la fecha de creación.

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
-A IP=192.168.13.213 \
-S -2d12h -F +4y6m
```

El administrador del sistema `enigma` establece las fechas para la validez del certificado. El certificado será anterior en dos días y será válido hasta las 12 de la noche del 31 de diciembre de 2010.

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax" \
-A IP=192.168.116.16 \
-S -2d -F "12/31/2010 12:00 AM"
```

▼ Cómo configurar IKE con certificados firmados por una autoridad de certificación

Los certificados públicos de una autoridad de certificación requieren negociar con una organización externa. Los certificados se pueden escalar con gran facilidad para proteger un mayor número de sistemas que se comunican.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tarefas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Utilice el comando `ikecert certlocal -kc` para crear una solicitud de certificado.

Para ver una descripción de los argumentos del comando, consulte el [Paso 2](#) en “[Cómo configurar IKE con certificados de clave pública autofirmados](#)” en la [página 596](#).

```
# ikecert certlocal -kc -m keysize -t keytype \
-D dname -A altname
```

a. Por ejemplo, el comando siguiente crea una solicitud de certificado en el sistema `partym`:

```
# ikecert certlocal -kc -m 1024 -t rsa-md5 \
> -D "C=US, O=PartyCompany\, Inc., OU=US-Partym, CN=Partym" \
> -A "DN=C=US, O=PartyCompany\, Inc., OU=US-Partym"
Creating software private keys.
Writing private key to file /etc/inet/secret/ike.privatekeys/2.
Enabling external key providers - done.
Certificate Request:
Proceeding with the signing operation.
Certificate request generated successfully (.../publickeys/0)
Finished successfully.
-----BEGIN CERTIFICATE REQUEST-----
MIIBYjCCATMCAQAwUzELMAkGA1UEBhMCVVMxHTAbBgNVBAoTTFEV4YW1wbGVDb21w
...
lcM+tw0ThRrfuJX9t/Qa1R/KxRlMA3zck080m09X
-----END CERTIFICATE REQUEST-----
```

b. El comando siguiente crea una solicitud de certificado en el sistema `enigma`:

```
# ikecert certlocal -kc -m 1024 -t rsa-md5 \
> -D "C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax, CN=Enigmax" \
> -A "DN=C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax"
Creating software private keys.
...
Finished successfully.
-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu
...
8qlqджаStLGfhD00
-----END CERTIFICATE REQUEST-----
```

3 Envíe la solicitud de certificado a una organización de PKI.

La organización de PKI puede indicar cómo enviar la solicitud de certificado. La mayoría de las organizaciones cuenta con un sitio web con un formulario de envío. El formulario requiere una prueba de que el envío es legítimo. Normalmente, la solicitud de certificado se pega en el formulario. Cuando la organización ha comprobado la solicitud, emite los dos objetos de certificado siguientes y una lista de los certificados revocados:

- El certificado de clave pública: este certificado se basa en la solicitud que ha enviado a la organización. La solicitud que envía forma parte del certificado de clave pública. El certificado le identifica de forma exclusiva.
- Una autoridad de certificación: la firma de la organización. La autoridad de certificación verifica que el certificado de clave pública sea legítimo.
- Una lista de revocación de certificados (CRL): La lista de certificados más reciente que ha revocado la organización. La CRL no se envía por separado como objeto de certificado si el acceso a la CRL está integrado en el certificado de clave pública.

Cuando un URI para la CRL está integrado en el certificado de clave pública, IKE puede recuperar automáticamente la CRL. De modo similar, cuando una entrada DN (nombre de directorio en servidor LDAP) se integra en el certificado de clave pública, IKE puede recuperar la CRL y almacenarla en caché desde un servidor LDAP que se especifique.

Consulte [“Cómo administrar una lista de revocación de certificados” en la página 612](#) para ver un ejemplo de URI integrado y una entrada DN integrada en un certificado de clave pública.

4 Agregue cada certificado al sistema.

La opción `-a` de `ikecert certdb -a` agrega el objeto pegado a la base de datos de certificados pertinente del sistema. Para más información, consulte [“IKE con certificados de claves públicas” en la página 579](#).

a. En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

b. Agregue el certificado de clave pública que ha recibido de la organización de PKI.

```
# ikecert certdb -a
Press the Return key
Paste the certificate:
-----BEGIN X509 CERTIFICATE-----
...
-----END X509 CERTIFICATE-----
Press the Return key
<Control>-D
```

c. Agregue la autoridad de certificación de la organización de PKI.

```
# ikecert certdb -a
Press the Return key
```

```

    Paste the CA:
    -----BEGIN X509 CERTIFICATE-----
    ...
    -----END X509 CERTIFICATE-----
    Press the Return key
    <Control>-D

```

- d. Si la organización de PKI ha enviado una lista de certificados revocados, agregue la CRL a la base de datos `certrl.db`:

```

# ikecert certrl.db -a
    Press the Return key
    Paste the CRL:
    -----BEGIN CRL-----
    ...
    -----END CRL-----
    Press the Return key
    <Control>-D

```

- 5 Utilice la palabra clave `cert_root` para identificar la organización de PKI en el archivo `/etc/inet/ike/config`.

Utilice el nombre que proporciona la organización de PKI.

- a. Por ejemplo, el archivo `ike/config` del sistema `partym` podría ser similar a:

```

# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

## Parameters that may also show up in rules.

p1_xform
{ auth_method rsa_sig oakley_group 1 auth_alg sha1 encr_alg des }
p2_pfs 2

{
    label "US-partym to JA-enigmax - Example PKI"
    local_id_type dn
    local_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
    remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

    local_addr 192.168.13.213
    remote_addr 192.168.116.16

    p1_xform
    {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}

```

Nota – Todos los argumentos del parámetro `auth_method` deben encontrarse en la misma línea.

b. En el sistema enigma, cree un archivo similar.

En concreto, el archivo `enigma ike/config` llevará a cabo las siguientes acciones:

- Incluirá el mismo valor de `cert_root`.
- Utilizará los valores de `enigma` para los parámetros locales.
- Utilice los valores de `partym` para los parámetros remotos.
- Cree un valor único para la palabra clave `label`. Este valor debe ser diferente del valor `label` del sistema remoto.

```
...
cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"
...
{
  label "JA-enigma to US-party - Example PKI"
  local_id_type dn
  local_id "C=JA, O=EnigmaCo, OU=JA-Enigma, CN=Enigma"
  remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

  local_addr 192.168.116.16
  remote_addr 192.168.13.213
...

```

6 Indique a IKE cómo administrar las CRL.

Elija la opción adecuada:

■ **Ninguna CRL disponible**

Si la organización de PKI no proporciona ninguna CRL, agregue la palabra clave `ignore_crls` al archivo `ike/config`.

```
# Trusted root cert
...
cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example,..."
ignore_crls
...

```

La palabra clave `ignore_crls` indica a IKE que no debe buscar ninguna CRL.

■ **CRL disponible**

Si la organización de PKI proporciona un punto de distribución central para las CRL, puede modificar el archivo `ike/config` para que haga referencia a esa ubicación.

Consulte [“Cómo administrar una lista de revocación de certificados” en la página 612](#) para ver algunos ejemplos.

Ejemplo 23-6 Uso de `rsa_encrypt` durante la configuración de IKE

Cuando utiliza `auth_method rsa_encrypt` en el archivo `ike/config`, debe agregar el certificado equivalente a la base de datos `publickeys`.

1. Envíe el certificado al administrador del sistema remoto.

El certificado se puede pegar en un mensaje de correo electrónico.

Por ejemplo, el administrador de `partym` enviaría el siguiente mensaje de correo electrónico:

```
To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MII...
-----END X509 CERTIFICATE-----
```

El administrador de `enigma` enviaría el siguiente mensaje de correo electrónico:

```
To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MII
...
-----END X509 CERTIFICATE-----
```

2. En cada sistema, agregue el certificado enviado por correo electrónico a la base de datos `publickeys` local.

```
# ikercert certdb -a
Press the Return key
-----BEGIN X509 CERTIFICATE-----
MII...
-----END X509 CERTIFICATE-----
Press the Return key
<Control>-D
```

El método de autenticación para el cifrado de RSA oculta las identidades de IKE de los intrusos. Dado que el método `rsa_encrypt` oculta la identidad del equivalente, IKE no puede recuperar su certificado. Como consecuencia de ello, el método `rsa_encrypt` requiere que los equivalentes de IKE conozcan las claves públicas el uno del otro.

Por tanto, si utiliza un `auth_method` de `rsa_encrypt` en el archivo `/etc/inet/ike/config`, debe agregar el certificado del equivalente a la base de datos `publickeys`. La base de datos `publickeys` incluye tres certificados para cada par de sistemas que se comunican:

- Su certificado de clave pública
- El certificado de la administración de certificación
- El certificado de clave pública del equivalente

Resolución de problemas: La carga útil de IKE, que incluye los tres certificados, puede ser demasiado grande para que la cifre `rsa_encrypt`. Errores como un fallo de autenticación o

una carga útil mal formada pueden indicar que el método `rsa_encrypt` no puede cifrar la carga útil total. Reduzca el tamaño de la carga útil utilizando un método que requiera únicamente dos certificados, por ejemplo `rsa_sig`.

▼ Cómo generar y almacenar certificados de clave pública en el hardware

La generación y el almacenamiento de certificados de clave pública en hardware es similar a la generación y el almacenamiento de certificados de clave pública en el sistema. En el hardware, los comandos `ikecert certlocal` e `ikecert certdb` deben identificar el hardware. La opción `-T` con el ID de símbolo identifica el hardware para los comandos.

Antes de empezar

- El hardware debe estar configurado.
- El hardware utiliza la biblioteca `/usr/lib/libpkcs11.so`, a menos que la palabra clave `pkcs11_path` del archivo `/etc/inet/ike/config` haga referencia a una biblioteca distinta. La biblioteca debe implementarse de acuerdo con el estándar siguiente: RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki), es decir, una biblioteca PKCS #11.

Consulte “[Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 4000](#)” en la [página 623](#) para obtener instrucciones sobre la instalación.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Genere un certificado autofirmado o una solicitud de certificado y especifique el ID de símbolo. Elija una de las siguientes opciones:

Nota – La placa Sun Crypto Accelerator 4000 admite claves de hasta 2048 bits para RSA. Para DSA, esta placa admite claves de hasta 1024 bits.

- **Para un certificado autofirmado, utilice esta sintaxis.**

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \  
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \  
> -a -T dca0-accel-stor IP=192.168.116.16  
Creating hardware private keys.
```


Enter PIN for PKCS#11 token: *Type user:password*

El argumento para la opción -T es el ID de símbolo de la placa Sun Crypto Accelerator 4000 conectada.

- **Para obtener una solicitud de certificado, utilice esta sintaxis.**

```
# ikecert certlocal -kc -m 1024 -t rsa-md5 \
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
> -a -T dca0-accel-stor IP=192.168.116.16
Creating hardware private keys.
Enter PIN for PKCS#11 token: Type user:password
```

Para ver una descripción de los argumentos para el comando `ikecert`, consulte la página del comando `man ikecert(1M)`.

- 3 Cuando se le solicite un PIN, escriba el usuario de Sun Crypto Accelerator 4000, dos puntos y la contraseña del usuario.**

Si la placa de Sun Crypto Accelerator 4000 tiene un usuario `ikemgr` cuya contraseña es `rgm4tigt`, debe escribir:

Enter PIN for PKCS#11 token: **ikemgr:rgm4tigt**

Nota – La respuesta de PIN se guarda en el disco *como texto sin cifrar*.

Una vez indicada la contraseña, se imprime el certificado:

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt
-----BEGIN X509 CERTIFICATE-----
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu
....
oKUDBbZ90/pLWYGr
-----END X509 CERTIFICATE-----
```

- 4 Envíe su certificado para que lo pueda utilizar la otra parte.**

Elija una de las siguientes opciones:

- **Envíe el certificado autofirmado al sistema remoto.**

El certificado se puede pegar en un mensaje de correo electrónico.

- **Envíe la solicitud de certificado a una organización que administre PKI.**

Siga las instrucciones de la organización de PKI para enviar la solicitud de certificado. Para obtener información más detallada, consulte el [Paso 3](#) de “[Cómo configurar IKE con certificados firmados por una autoridad de certificación](#)” en la página 602.

5 En el sistema, edite el archivo `/etc/inet/ike/config` para que reconozca los certificados.

Elija una de las siguientes opciones.

■ Certificado autofirmado

Utilice los valores que proporciona el administrador del sistema remoto para los parámetros `cert_trust`, `remote_id` y `remote_addr`. Por ejemplo, en el sistema `enigma`, el archivo `ike/config` sería similar a:

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

cert_trust "192.168.116.16"      Local system's certificate Subject Alt Name
cert_trust "192.168.13.213"     Remote system's certificate Subject Alt name

# Solaris 10 1/06 release: default path does not have to be typed in #pkcs11_path
"/usr/lib/libpkcs11.so"        Hardware connection

# Solaris 10 release: use this path
#pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
...
{
    label "JA-enigmax to US-party"
    local_id_type dn
    local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
    remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

    local_addr 192.168.116.16
    remote_addr 192.168.13.213

    pl_xform
    {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

■ Solicitud de certificado

Escriba el nombre que proporciona la organización de PKI como valor para la palabra clave `cert_root`. Por ejemplo, el archivo `ike/config` del sistema `enigma` podría ser similar a:

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

# Solaris 10 1/06 release: default path does not have to be typed in #pkcs11_path
"/usr/lib/libpkcs11.so"        Hardware connection

# Solaris 10 release: use this path
#pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
```

```

...
{
  label "JA-enigmax to US-party - Example PKI"
  local_id_type dn
  local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
  remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

  local_addr 192.168.116.16
  remote_addr 192.168.13.213

  pl_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}

```

6 Coloque los certificados de la otra parte en el hardware.

Responda a la solicitud de PIN del mismo modo que en el [Paso 3](#).

Nota – *Debe* agregar los certificados de clave pública al mismo hardware conectado que generó la clave privada.

■ Certificado autofirmado.

Agregue el certificado autofirmado al sistema remoto. En este ejemplo, el certificado se guarda en el archivo, `DCA.ACCEL.STOR.CERT`.

```
# ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CERT
Enter PIN for PKCS#11 token:      Type user:password
```

Si el certificado autofirmado utilizó `rsa_encrypt` como valor para el parámetro `auth_method`, agregue el certificado del equivalente al hardware.

■ Certificados de una organización de PKI.

Agregue el certificado que ha generado la organización a partir de la solicitud de certificado, y agregue la autoridad de certificación.

```
# ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CERT
Enter PIN for PKCS#11 token:      Type user:password
```

```
# ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CA.CERT
Enter PIN for PKCS#11 token:      Type user:password
```

Para agregar una lista de revocación de certificados (CRL) de la organización de PKI, consulte [“Cómo administrar una lista de revocación de certificados”](#) en la página 612.

▼ Cómo administrar una lista de revocación de certificados

Una lista de revocación de certificados (CRL) contiene certificados caducados o que suponen un peligro de una autoridad de certificación. Existen cuatro modos de administrar las CRL.

- Debe indicar a IKE que omita las CRL si la organización de la autoridad de certificación no emite ninguna CRL. Esta opción se muestra en el [Paso 6](#) en “[Cómo configurar IKE con certificados firmados por una autoridad de certificación](#)” en la [página 602](#).
- Puede indicar a IKE que acceda a las CRL desde un indicador de recursos uniforme (URI) cuya dirección esté integrada en el certificado de clave pública de la autoridad de certificación.
- Puede indicar a IKE que acceda a las CRL desde un servidor LDAP cuya entrada de nombre de directorio (DN) esté integrada en el certificado de clave pública de la autoridad de certificación.
- Puede proporcionar la CRL como argumento para el comando `ikecert certrl db`. Esto se ilustra en el [Ejemplo 23-7](#).

El siguiente procedimiento describe cómo indicar a IKE que utilice las CRL de un punto de distribución central.

1 Visualice el certificado que ha recibido de la autoridad de certificación.

```
# ikecert certdb -lv certspec
```

-l Enumera los certificados de la base de datos IKE.

-v Enumera los certificados en modo detallado. Utilice esta opción con precaución.

certspec Es un patrón que coincide con un certificado de la base de datos de certificados IKE.

Por ejemplo, el certificado siguiente ha sido emitido por Sun Microsystems. Los detalles se han modificado.

```
# ikecert certdb -lv example-protect.sun.com
Certificate Slot Name: 0 Type: dsa-sha1
(Private key in certlocal slot 0)
Subject Name: <O=Sun Microsystems Inc, CN=example-protect.sun.com>
Issuer Name: <CN=Sun Microsystems Inc CA (Cl B), O=Sun Microsystems Inc>
SerialNumber: 14000D93
Validity:
  Not Valid Before: 2002 Jul 19th, 21:11:11 GMT
  Not Valid After: 2005 Jul 18th, 21:11:11 GMT
Public Key Info:
  Public Modulus (n) (2048 bits): C575A...A5
  Public Exponent (e) ( 24 bits): 010001
Extensions:
  Subject Alternative Names:
    DNS = example-protect.sun.com
```

```

Key Usage: DigitalSignature KeyEncipherment
[CRITICAL]
CRL Distribution Points:
  Full Name:
    URI = #Ihttp://www.sun.com/pki/pkismica.crl#i
    DN = <CN=Sun Microsystems Inc CA (Cl B), O=Sun Microsystems Inc>
  CRL Issuer:
    Authority Key ID:
    Key ID:          4F ... 6B
    SubjectKeyID:    A5 ... FD
    Certificate Policies
    Authority Information Access

```

Observe la entrada CRL Distribution Points. La entrada URI indica que la CRL de esta organización está disponible en Internet. La entrada DN indica que la CRL está disponible en un servidor LDAP. Cuando IKE accede a la CRL, ésta se almacena en caché para futuros usos.

Para acceder a la CRL, debe alcanzar un punto de distribución.

2 Elija uno de los métodos siguientes para acceder a la CRL desde un punto de distribución central.

- **Utilice el URI.**

Agregue la palabra clave `use_http` al archivo `/etc/inet/ike/config` del host. Por ejemplo, el archivo `ike/config` tendría el siguiente aspecto:

```

# Use CRL from organization's URI
use_http
...

```

- **Utilice un proxy Web.**

Agregue la palabra clave `proxy` al archivo `ike/config`. La palabra clave `proxy` adopta una dirección URL como argumento, como en el caso siguiente:

```

# Use own web proxy
proxy "http://proxy1:8080"

```

- **Utilice un servidor LDAP.**

Configure el servidor LDAP como argumento para la palabra clave `ldap-list` del archivo `/etc/inet/ike/config` del host. Su organización proporciona el nombre del servidor LDAP. La entrada del archivo `ike/config` tendría el siguiente aspecto:

```

# Use CRL from organization's LDAP
ldap-list "ldap1.sun.com:389,ldap2.sun.com"
...

```

IKE recupera la CRL y almacena en caché la CRL hasta que caduque el certificado.

Ejemplo 23–7 Cómo pegar una CRL en la base de datos cert rldb local

Si la CRL de la organización de PKI no está disponible en un punto de distribución central, puede agregar la CRL manualmente a la base de datos cert rldb local. Siga las instrucciones de la organización de PKI para extraer la CRL en un archivo y, a continuación, agregue la CRL a la base de datos con el comando `ikecert cert rldb -a`.

```
# ikecert cert rldb -a < Sun.Cert.CRL
```

Configuración de IKE para sistemas portátiles (mapa de tareas)

La tabla siguiente incluye los procedimientos para configurar IKE para la administración de sistemas que se registran remotamente en un sitio central.

Tarea	Descripción	Para obtener instrucciones
Comunicar remotamente con un sitio central	Permite a los sistemas remotos comunicarse con un sitio central. Los sistemas remotos pueden ser portátiles.	“Cómo configurar IKE para sistemas remotos” en la página 615
Utilizar un certificado raíz e IKE en un sistema central que acepta tráfico de sistemas portátiles	Configura un sistema de portal para que acepte el tráfico de IPsec de un sistema que no tiene una dirección IP fija.	Ejemplo 23–8
Utilizar un certificado raíz e IKE en un sistema que no tiene una dirección IP fija	Configura un sistema portátil para proteger su tráfico en un sitio central, como la oficina central de una compañía.	Ejemplo 23–9
Utilizar certificados autofirmados e IKE en un sistema central que acepta tráfico de sistemas portátiles	Configura un sistema de portal con certificados autofirmados para aceptar tráfico de IPsec desde un sistema portátil.	Ejemplo 23–10
Utilizar certificados autofirmados e IKE en un sistema que no tiene una dirección IP fija	Configura un sistema portátil con certificados autofirmados para proteger su tráfico en un sitio central.	Ejemplo 23–11

Configuración de IKE para sistemas portátiles

Cuando se configuran correctamente, las oficinas domésticas y los portátiles pueden utilizar IPsec e IKE para comunicarse con los equipos centrales de la compañía. Una directiva IPsec general que se combina con un método de autenticación de claves públicas permite a los sistemas remotos proteger su tráfico en un sistema central.

▼ Cómo configurar IKE para sistemas remotos

IPsec e IKE requieren un ID único para identificar el origen y el destino. Para los sistemas remotos o portátiles que no tienen una dirección IP única, debe utilizar otro tipo de ID. Los tipos de ID como DNS, DN o email se pueden utilizar para identificar a un sistema de forma exclusiva.

Los sistemas remotos o portátiles que tienen direcciones IP exclusivas se siguen configurando mejor con un tipo de ID diferente. Por ejemplo, si los sistemas intentan conectarse a un sitio central desde un enrutador NAT, no se utilizarán sus direcciones exclusivas. Un enrutador NAT asigna una dirección IP arbitraria, que el sistema central no reconocería.

Las claves previamente compartidas tampoco funcionan bien como mecanismo de autenticación para sistemas portátiles, dado que requieren direcciones IP fijas. Los certificados autofirmados o certificados desde un PKI permiten a los sistemas portátiles comunicarse con el sitio central.

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Configure el sistema central para que reconozca los sistemas portátiles.

a. Configure el archivo `/etc/hosts`.

El sistema central no tiene que reconocer las direcciones específicas para los sistemas portátiles.

```
# /etc/hosts on central
central 192.xxx.xxx.x
```

b. Configure el archivo `ipsecinit.conf`.

El sistema central necesita una directiva que permite una amplia gama de direcciones IP. Los certificados de la directiva IKE garantizan que los sistemas conectados son legítimos.

```
# /etc/inet/ipsecinit.conf on central
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

c. Configure el archivo `ike.config`.

DNS identifica el sistema central. Se utilizan certificados para autenticar el sistema.

```
## /etc/inet/ike/ike.config on central
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root "C=US, O=Domain Org, CN=Domain STATE"
#
# List self-signed certificates - trust server and enumerated others
#cert_trust "DNS=central.domain.org"
#cert_trust "DNS=mobile.domain.org"
#cert_trust "DN=CN=Domain Org STATE (CLASS), O=Domain Org"
#cert_trust "email=root@central.domain.org"
#cert_trust "email=user1@mobile.domain.org"
#

# Rule for mobile systems with certificate
{
    label "Mobile systems with certificate"
    local_id_type DNS

# Any mobile system who knows my DNS or IP can find me.

    local_id "central.domain.org"
    local_addr 192.xxx.xxx.x

# Root certificate ensures trust,
# so allow any remote_id and any remote IP address.
    remote_id ""
    remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

3 Inicie sesión en cada sistema portátil y configure el sistema para buscar el sistema central.**a. Configure el archivo `/etc/hosts`.**

El archivo `/etc/hosts` no necesita una dirección para el sistema portátil, pero puede proporcionar una. El archivo debe contener una dirección IP pública para el sistema central.

```
# /etc/hosts on mobile
mobile 10.x.x.xx
central 192.xxx.xxx.x
```


b. Configure el archivo `ipsecinit.conf`.

El sistema portátil debe encontrar el sistema central por su dirección IP pública. Los sistemas deben configurar la misma directiva IPsec.

```
# /etc/inet/ipsecinit.conf on mobile
# Find central
{raddr 192.xxx.xxx.x} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

c. Configure el archivo `ike.config`.

El identificador no puede ser una dirección IP. Los siguientes identificadores son válidos para sistemas portátiles:

- DN=*nombre_directorio_ldap*
- DNS=*dirección_servidor_nombre_dominio*
- email=*dirección_correo_electrónico*

Se utilizan certificados para autenticar el sistema portátil.

```
## /etc/inet/ike/ike.config on mobile
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root "C=US, O=Domain Org, CN=Domain STATE"
#
# Self-signed certificates - trust me and enumerated others
#cert_trust "DNS=mobile.domain.org"
#cert_trust "DNS=central.domain.org"
#cert_trust "DN=CN=Domain Org STATE (CLASS), O=Domain Org"
#cert_trust "email=user1@domain.org"
#cert_trust "email=root@central.domain.org"
#
# Rule for off-site systems with root certificate
{
    label "Off-site mobile with certificate"
    local_id_type DNS

# NAT-T can translate local_addr into any public IP address
# central knows me by my DNS

    local_id "mobile.domain.org"
    local_addr 0.0.0.0/0

# Find central and trust the root certificate
    remote_id "central.domain.org"
    remote_addr 192.xxx.xxx.x
```

```
p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

4 Lea la configuración de IKE en el núcleo.

- A partir de la versión Solaris 10 4/09, habilite el servicio `ike`.

```
# svcadm enable svc:/network/ipsec/ike
```

- Si está ejecutando una versión anterior a la Solaris 10 4/09, reinicie el sistema.

```
# init 6
```

También puede detener e iniciar el daemon `in.iked`.

Ejemplo 23–8 Configuración de un equipo para que acepte tráfico IPsec de un sistema portátil

IKE puede iniciar negociaciones desde un enrutador NAT. Sin embargo, la configuración de IKE ideal no incluye un enrutador NAT. En el ejemplo siguiente, una autoridad de certificación ha emitido certificados raíz. Los certificados de la autoridad de certificación se colocan en el sistema portátil y el sistema central. Un sistema central acepta las negociaciones de IPsec desde un sistema con un enrutador NAT. `main1` es el sistema de la compañía que puede aceptar conexiones desde sistemas remotos. Para configurar los sistemas remotos, consulte el [Ejemplo 23–9](#).

```
## /etc/hosts on main1
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
```

```

label "Off-site system with root certificate"
local_id_type DNS
local_id "main1.domain.org"
local_addr 192.168.0.100

# Root certificate ensures trust,
# so allow any remote_id and any remote IP address.
remote_id ""
remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha1}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha1}

```

Ejemplo 23–9 Configuración de un sistema con una NAT con IPsec

En el ejemplo siguiente, una autoridad de certificación ha emitido certificados raíz y los ha colocado en el sistema portátil y el sistema central. `mobile1` se conecta a la oficina central de la compañía desde casa. La red del proveedor de servicios de Internet (ISP) utiliza un enrutador NAT para permitir al ISP asignar a `mobile1` una dirección privada. A continuación, el enrutador convierte la dirección privada en una dirección IP pública que comparte con otros nodos de red del ISP. La oficina central de la compañía no está detrás de un dispositivo NAT. Para configurar el equipo de la oficina central de la compañía, consulte el [Ejemplo 23–8](#).

```

## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate

```

```
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
    label "Off-site mobile1 with root certificate"
    local_id_type DNS
    local_id "mobile1.domain.org"
    local_addr 0.0.0.0/0

# Find main1 and trust the root certificate
    remote_id "main1.domain.org"
    remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

Ejemplo 23-10 Aceptación de certificados autofirmados de un sistema portátil

En el ejemplo siguiente, se han emitido certificados autofirmados y se encuentran en el sistema portátil y el sistema central. main1 es el sistema de la compañía que puede aceptar conexiones desde sistemas remotos. Para configurar los sistemas remotos, consulte el [Ejemplo 23-11](#).

```
## /etc/hosts on main1
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Self-signed certificates - trust me and enumerated others
cert_trust "DNS=main1.domain.org"
cert_trust "jdoe@domain.org"
cert_trust "user2@domain.org"
cert_trust "user3@domain.org"
#
# Rule for off-site systems with trusted certificate
{
    label "Off-site systems with trusted certificates"
    local_id_type DNS
    local_id "main1.domain.org"
    local_addr 192.168.0.100

# Trust the self-signed certificates
# so allow any remote_id and any remote IP address.
    remote_id ""
    remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
```

```
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

Ejemplo 23–11 Uso de certificados autofirmados para contactar con un sistema central

En el ejemplo siguiente, `mobile1` se conecta a la oficina central de la compañía desde casa. Los certificados se han emitido y se colocan en el sistema portátil y el sistema central. La red ISP utiliza un enrutador NAT para permitir al ISP asignar a `mobile1` una dirección privada. A continuación, el enrutador convierte la dirección privada en una dirección IP pública que comparte con otros nodos de red del ISP. La oficina central de la compañía no está detrás de un dispositivo NAT. Para configurar el sistema en las oficinas de la empresa, consulte el [Ejemplo 23–10](#).

```
## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters

# Self-signed certificates - trust me and the central system
cert_trust "jdoe@domain.org"
cert_trust "DNS=main1.domain.org"
#
# Rule for off-site systems with trusted certificate
{
    label "Off-site mobile1 with trusted certificate"
    local_id_type email
    local_id "jdoe@domain.org"
    local_addr 0.0.0.0/0

# Find main1 and trust the certificate
    remote_id "main1.domain.org"
    remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

Configuración de IKE para buscar el hardware conectado (mapa de tareas)

La tabla siguiente incluye los procedimientos que indican a IKE el hardware conectado. Debe informar a IKE del hardware conectado para que pueda utilizarlo. Para utilizar el hardware, siga los procedimientos de [“Configuración de IKE con certificados de clave pública” en la página 596](#).

Nota – No tiene que informar a IKE sobre el hardware en chip. Por ejemplo, el procesador UltraSPARC® T2 proporciona aceleración criptográfica. No es necesario configurar IKE para encontrar los aceleradores en chip.

Tarea	Descripción	Para obtener instrucciones
Descargar operaciones de claves IKE en la placa de Sun Crypto Accelerator 1000	Vincula IKE con la biblioteca de PKCS #11.	“Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 1000” en la página 622
Descargar operaciones de claves IKE y almacenar las claves en la placa de Sun Crypto Accelerator 4000	Vincula IKE con la biblioteca de PKCS #11 e indica el nombre del hardware conectado.	“Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 4000” en la página 623

Configuración de IKE para buscar el hardware conectado

Los certificados de claves públicas también se pueden almacenar en el hardware adjunto. La placa Sun Crypto Accelerator 1000 sólo proporciona almacenamiento. Las placas Sun Crypto Accelerator 4000 y Crypto Accelerator 6000 de Sun proporcionan almacenamiento y permiten que se descarguen operaciones de claves públicas desde el sistema a la placa.

▼ Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 1000

Antes de empezar El procedimiento siguiente presupone que hay una placa de Sun Crypto Accelerator 1000 conectada al sistema. Además, el procedimiento presupone que se ha instalado y configurado el software para la placa. Para obtener instrucciones, consulte *Sun Crypto Accelerator 1000 Board Version 2.0 Installation and User’s Guide*.

- 1 **En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

- 2 **Compruebe que esté vinculada la biblioteca de PKCS #11.**

Escriba el comando siguiente para determinar si la biblioteca de PKCS #11 está vinculada:

```
# ikeadm get stats
Phase 1 SA counts:
Current:  initiator:      0  responder:      0
Total:    initiator:      0  responder:      0
Attempted: initiator:      0  responder:      0
Failed:   initiator:      0  responder:      0
          initiator fails include 0 time-out(s)
PKCS#11 library linked in from /usr/lib/libpkcs11.so
#
```

- 3 **Solaris 10 1/06: A partir de esta versión, puede guardar las claves en el almacén de claves softtoken.**

Para obtener información sobre el almacén de claves que proporciona la estructura criptográfica de Solaris, consulte la página del comando `man cryptoadm(1M)`. Si desea ver un ejemplo del uso del almacén de claves, consulte el [Example 23–12](#).

▼ **Cómo configurar IKE para buscar la placa de Sun Crypto Accelerator 4000**

Antes de empezar

El siguiente procedimiento presupone que hay una placa de Sun Crypto Accelerator 4000 conectada al sistema. Además, el procedimiento presupone que se ha instalado y configurado el software para la placa. Para obtener instrucciones, consulte la *Sun Crypto Accelerator 4000 Board Version 1.1 Installation and User's Guide*.

Si utiliza una placa Crypto Accelerator 6000 de Sun, consulte la *Sun Crypto Accelerator 6000 Board Version 1.1 User's Guide* para obtener instrucciones.

- 1 **En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Compruebe que esté vinculada la biblioteca de PKCS #11.

IKE utiliza las rutinas de la biblioteca para administrar la generación de claves y el almacenamiento de claves en la placa de Sun Crypto Accelerator 4000. Escriba el comando siguiente para determinar si se ha vinculado una biblioteca de PKCS #11:

```
$ ikeadm get stats
...
PKCS#11 library linked in from /usr/lib/libpkcs11.so
$
```

Nota – La placa Sun Crypto Accelerator 4000 admite claves de hasta 2048 bits para RSA. Para DSA, esta placa admite claves de hasta 1024 bits.

3 Busque el ID de símbolo para la placa de Sun Crypto Accelerator 4000 conectada.

```
$ ikecert tokens
Available tokens with library "/usr/lib/libpkcs11.so":
```

```
"Sun Metaslot"
```

La biblioteca devuelve un ID de símbolo, también denominado **nombre de keystore**, de 32 caracteres. En este ejemplo, puede utilizar el símbolo `Sun Metaslot` con los comandos `ikecert` para almacenar y acelerar claves IKE.

Para obtener instrucciones sobre cómo utilizar el símbolo, consulte [“Cómo generar y almacenar certificados de clave pública en el hardware” en la página 608](#).

Los espacios finales se rellenan automáticamente con el comando `ikecert`.

Ejemplo 23–12 Búsqueda y uso de símbolos de metarranura

Los símbolos se pueden almacenar en el disco, en una placa conectada o en el almacén de claves `softtoken` que proporciona la estructura de cifrado de Solaris. El ID de símbolo del almacén de claves `softtoken` podría ser similar al siguiente.

```
$ ikecert tokens
Available tokens with library "/usr/lib/libpkcs11.so":
```

```
"Sun Metaslot"
```

Para crear una contraseña para el almacén de claves `softtoken`, consulte la página del comando `man pktool(1)`.

Un comando como el siguiente agregaría un certificado al almacén de claves softtoken. `Sun.Metaslot.cert` es un archivo que contiene un certificado de una autoridad de certificación.

```
# ikecert certdb -a -T "Sun Metaslot" < Sun.Metaslot.cert
Enter PIN for PKCS#11 token:      Type user:passphrase
```

Cambio de los parámetros de transmisión de IKE (mapa de tareas)

En la tabla siguiente se incluyen los procedimientos para configurar los parámetros de transmisión para IKE.

Tarea	Descripción	Para obtener instrucciones
Hacer la negociación de claves más eficiente	Cambia los parámetros de negociación de claves.	“Cómo cambiar la duración de la negociación de claves IKE de fase 1” en la página 626
Configurar la negociación de claves para permitir retrasos en la transmisión	Alarga los parámetros de negociación de claves.	Ejemplo 23–13
Configurar la negociación de claves para proceder con rapidez si es correcta o para mostrar los fallos rápidamente	Acorta los parámetros de negociación de claves.	Ejemplo 23–14

Cambio de los parámetros de transmisión de IKE

Cuando IKE negocia claves, la velocidad de transmisión puede afectar al éxito de la negociación. Normalmente, no necesita cambiar los valores predeterminados de los parámetros de transmisión de IKE. Sin embargo, al optimizar la negociación de claves con líneas muy codificadas o al reproducir un problema, puede cambiar los valores de transmisión.

Un tiempo más prolongado permite a IKE negociar claves en líneas de transmisión poco fiables. Puede alargar determinados parámetros para que los intentos iniciales tengan éxito. Si el intento inicial no tiene éxito, puede espaciar los siguientes intentos para que haya más tiempo.

Un tiempo más breve permite aprovechar las líneas de transmisión fiables. Puede reintentar una negociación fallida con mayor rapidez para acelerar la negociación. Al diagnosticar un problema, es posible que también desee acelerar la negociación para un fallo rápido. Un tiempo más breve también permite utilizar las SA de la fase 1.

▼ Cómo cambiar la duración de la negociación de claves IKE de fase 1

1 En la consola del sistema, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

Nota – El inicio de sesión remoto expone el tráfico cuya seguridad es crítica a intrusos. Aunque proteja de algún modo el inicio de sesión remoto, la seguridad del sistema se reducirá a la seguridad de la sesión remota. Utilice el comando `ssh` para un inicio de sesión remota seguro.

2 Cambie los valores predeterminados de los parámetros de transmisión globales de cada sistema.

En cada sistema, modifique los parámetros de duración de la fase 1 del archivo `/etc/inet/ike/config`.

```
### ike/config file on      system

## Global parameters
#
## Phase 1 transform defaults
#
#expire_timer      300
#retry_limit       5
#retry_timer_init  0.5 (integer or float)
#retry_timer_max   30  (integer or float)

expire_timer      Número de segundos que persistirá una negociación de IKE de fase 1
                  sin completar antes de eliminar el intento de negociación. De modo
                  predeterminado, el intento persiste durante 30 segundos.

retry_limit        El número de retransmisiones antes de que se cancele cualquier
                  negociación de IKE. De modo predeterminado, hay cinco intentos de
                  IKE.

retry_timer_init   Intervalo inicial entre retransmisiones. Este intervalo se dobla hasta
                  alcanzar el valor de retry_timer_max. El intervalo inicial es de 0,5
                  segundos.

retry_timer_max    El intervalo máximo en segundos entre retransmisiones. El intervalo de
                  retransmisión deja de aumentar una vez alcanzado este límite. De
                  modo predeterminado, el límite es de 30 segundos.
```

3 Lea la configuración que ha cambiado en el núcleo.

- **A partir de la versión Solaris 10 4/09 actualice el ike.**
`# svcadm refresh svc:/network/ipsec/ike`
- **Si está ejecutando una versión anterior a Solaris 10 4/09 reinicie el sistema.**
`# init 6`
 También puede detener e iniciar el daemon `in.iked`.

Ejemplo 23-13 Cómo alargar el tiempo de negociación de IKE de fase 1

En el ejemplo siguiente, un sistema se conecta a sus equivalentes IKE mediante una línea de transmisión de alta densidad de tráfico. Los parámetros originales se encuentran en los comentarios del archivo. Los nuevos parámetros alargan el tiempo de negociación.

```
### ike/config file on partym
## Global Parameters
#
## Phase 1 transform defaults
#expire_timer 300
#retry_limit 5
#retry_timer_init 0.5 (integer or float)
#retry_timer_max 30 (integer or float)
#
expire_timer 600
retry_limit 10
retry_timer_init 2.5
retry_timer_max 180
```

Ejemplo 23-14 Cómo acortar el tiempo de negociación de IKE de fase 1

En el ejemplo siguiente, un sistema se conecta a sus equivalentes IKE mediante una línea de alta velocidad con poca densidad de tráfico. Los parámetros originales se encuentran en los comentarios del archivo. Los nuevos parámetros acortan el tiempo de negociación.

```
### ike/config file on partym
## Global Parameters
#
## Phase 1 transform defaults
#expire_timer 300
#retry_limit 5
#retry_timer_init 0.5 (integer or float)
#retry_timer_max 30 (integer or float)
#
expire_timer 120
retry_timer_init 0.20
```


Intercambio de claves de Internet (referencia)

Este capítulo contiene la siguiente información de referencia sobre IKE:

- “Utilidad de gestión de servicios de IKE” en la página 629
- “Daemon IKE” en la página 630
- “Archivo de directiva IKE” en la página 630
- “Comando de administración de IKE” en la página 631
- “Archivos de claves IKE previamente compartidas” en la página 632
- “Comandos y bases de datos de claves públicas IKE” en la página 632

Para obtener instrucciones sobre la implementación de IKE, consulte el [Capítulo 23](#), “Configuración de IKE (tareas)”. Para obtener una descripción general, consulte el [Capítulo 22](#), “Intercambio de claves de Internet (descripción general)”.

Utilidad de gestión de servicios de IKE

`svc:/network/ipsec/ike:default` **servicio** – la utilidad de administración de servicios (SMF) proporciona el servicio `ike` para administrar IKE. Por defecto, este servicio está inhabilitado. Antes de habilitar este servicio, debe crear un archivo de configuración IKE, archivo `/etc/inet/ike/config`.

Las siguientes propiedades del servicio `ike` son configurables:

- Propiedad `config_file` – es la ubicación del archivo de configuración IKE. El valor inicial es `/etc/inet/ike/config`.
- Propiedad `debug_level` – es el nivel de depuración del daemon `in.iked`. El valor inicial es `op` u `operativos`. Para ver los posibles valores, consulte la tabla de niveles de depuración en *Object Types* en la página de comando `man ikedadm(1M)`.
- Propiedad `admin_privilege` – es el nivel de privilegio del daemon `in.iked`. El valor inicial es `base`. Otros valores son `modkeys` y `keymat`. Para obtener más detalles, consulte “Comando de administración de IKE” en la página 631.

Para obtener más información sobre SMF, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)”](#) de *Guía de administración del sistema: administración básica*. Consulte también las páginas de comando `man smf(5)`, `svcadm(1M)` y `svccfg(1M)`.

Daemon IKE

El daemon `in.iked` automatiza la administración de claves criptográficas para IPsec en un sistema Solaris. El daemon negocia con un sistema remoto que ejecuta el mismo protocolo para proporcionar materiales de claves autenticados para las asociaciones de seguridad de forma protegida. El daemon debe ejecutarse en todos los sistemas que tienen previsto comunicarse de forma segura.

Por defecto, el servicio `svc:/network/ipsec/ike:default` servicio no está habilitado. Después de que se haya configurado el archivo `/etc/inet/ike/config` y se haya habilitado el servicio `ike`, el daemon `in.iked` se ejecuta con el inicio del sistema.

Al ejecutar el daemon IKE, el sistema se autentica automáticamente en su entidad IKE equivalente en el intercambio de fase 1. El equivalente se define en el archivo de directiva IKE, al igual que los métodos de autenticación. A continuación, el daemon establece las claves para el intercambio de fase 2. Las claves IKE se actualizan automáticamente a un intervalo especificado en el archivo de directiva. El daemon `in.iked` escucha las solicitudes IKE entrantes de la red y las solicitudes del tráfico saliente mediante el socket `PF_KEY`. Para más información, consulte la página del comando `man pf_key(7P)`.

Dos comandos admiten el daemon IKE. El comando `ikeadm` puede utilizarse para ver y modificar temporalmente la directiva IKE. Para modificar permanentemente la directiva IKE, puede modificar las propiedades del servicio `ike`. Si desea conocer el procedimiento, consulte “[Cómo ver las claves IKE previamente compartidas](#)” en la [página 589](#).

El comando `ikecert` permite ver y administrar las bases de datos de claves públicas. Este comando administra las bases de datos locales, `ike.privatekeys` y `publickeys`. Este comando también administra operaciones de claves públicas y el almacenamiento de las claves públicas en el hardware.

Archivo de directiva IKE

El archivo de configuración para la directiva IKE, `/etc/inet/ike/config`, administra las claves para las interfaces que está protegiendo el archivo de directiva IPsec, `/etc/inet/ipsecinit.conf`. El archivo de directiva IKE administra claves para IKE y para las asociaciones de seguridad de IPsec. El daemon IKE requiere material de claves en el intercambio de fase 1.

La administración de claves con IKE incluye reglas y parámetros globales. Una regla IKE identifica los sistemas o redes que protege el material de claves. La regla también especifica el método de autenticación. Los parámetros globales incluyen elementos como la ruta a un

acelerador de hardware conectado. Para ver ejemplos de los archivos de directiva IKE, consulte [“Configuración de IKE con claves previamente compartidas \(mapa de tareas\)” en la página 584](#). Para ver ejemplos y descripciones de las entradas de directiva IKE, consulte la página del comando `man ike.config(4)`.

Las asociaciones de seguridad de IPsec que admite IKE protegen los datagramas IP de acuerdo con las directivas que se establecen en el archivo de configuración para la directiva IPsec, `/etc/inet/ipsecinit.conf`. El archivo de directiva IKE determina si se utiliza la seguridad directa perfecta (PFS) al crear las asociaciones de seguridad de IPsec.

El archivo `ike/config` puede incluir la ruta a una biblioteca que se implementa de acuerdo con el estándar siguiente: Interfaz de señal criptográfica RSA Security Inc. PKCS #11 (Cryptoki). IKE utiliza esta biblioteca de PKCS #11 con tal de acceder al hardware para la aceleración de claves y el almacenamiento de claves.

Las consideraciones de seguridad del archivo `ike/config` son similares a las consideraciones del archivo `ipsecinit.conf`. Para obtener más información, consulte [“Consideraciones de seguridad para ipsecinit.conf e ipsecconf” en la página 570](#).

Comando de administración de IKE

Puede utilizar el comando `ikeadm` para:

- Ver aspectos del proceso del daemon IKE.
- Cambiar los parámetros que se transfieren al daemon IKE.
- Ver estadísticas sobre la creación de asociaciones de seguridad durante el intercambio de fase 1.
- Depurar procesos de IKE.
- Ver aspectos del estado de IKE.
- Cambiar las propiedades del daemon IKE.
- Ver estadísticas sobre la creación de asociaciones de seguridad durante el intercambio de fase 1.
- Depurar los intercambios del protocolo IKE.

Para ver ejemplos y una descripción completa de las opciones de este comando, consulte la página del comando `man ikeadm(1M)`

El nivel de privilegio del daemon IKE en ejecución determina qué aspectos del daemon IKE pueden verse y modificarse. Hay tres niveles de privilegio posibles.

Nivel Base	No puede ver ni modificar el material de claves. El nivel base es el nivel de privilegio predeterminado.
Nivel modkeys	Puede eliminar, cambiar y agregar claves previamente compartidas.

Nivel keymat Puede ver el material de claves real con el comando `ikeadm`.

Si desea un cambio en un privilegio temporal, puede utilizar el comando `ikeadm`. Para un cambio permanente, cambie la propiedad `admin_privilege` del servicio `ike`. Si desea conocer el procedimiento, consulte [“Cómo administrar servicios de IPsec e IKE” en la página 528](#).

Las consideraciones de seguridad del comando `ikeadm` son similares a las consideraciones del comando `ipseckey`. Para más detalles, consulte [“Consideraciones de seguridad para ipseckey” en la página 572](#).

Archivos de claves IKE previamente compartidas

Al crear manualmente claves previamente compartidas, las claves se almacenan en archivos del directorio `/etc/inet/secret`. El archivo `ike.preshared` contiene las claves previamente compartidas para las asociaciones de seguridad del protocolo de administración de claves y asociaciones de seguridad de Internet (ISAKMP). El archivo `ipseckey` contiene las claves previamente compartidas para las asociaciones de seguridad de IPsec. Los archivos se protegen en `0600`. El directorio `secret` se protege en `0700`.

- El archivo `ike.preshared` se crea al configurar el archivo `ike/config` para que requiera claves previamente compartidas. El material de claves se especifica para las asociaciones de seguridad de ISAKMP, es decir, para la autenticación IKE en el archivo `ike.preshared`. Dado que se utilizan claves previamente compartidas para autenticar el intercambio de fase 1, el archivo debe ser válido antes de iniciar el daemon `in.iked`.
- El archivo `ipseckey` contiene el material de claves para las asociaciones de seguridad de IPsec. Para ver ejemplos de la administración manual del archivo, consulte [“Cómo crear manualmente asociaciones de seguridad IPsec” en la página 520](#). El daemon IKE no utiliza este archivo. El material de claves que genera IKE para las asociaciones de seguridad de IPsec se almacena en el núcleo.

Nota – Las claves previamente compartidas no pueden utilizar el almacenamiento de hardware. Las claves previamente compartidas se generan y almacenan en el sistema.

Comandos y bases de datos de claves públicas IKE

El comando `ikecert` administra las bases de datos de claves públicas del sistema local. Este comando se utiliza cuando el archivo `ike/config` requiere certificados de claves públicas. Dado que IKE utiliza estas bases de datos para autenticar el intercambio de fase 1, las bases de datos deben rellenarse antes de activar el daemon `in.iked`. Existen tres subcomandos que administran las tres bases de datos: `certlocal`, `certdb` y `certldb`.

El comando `ikecert` también administra el almacenamiento de claves. Las claves se pueden almacenar en disco, en una placa Sun Crypto Accelerator 4000 o Crypto Accelerator 6000 de Sun, o bien en un almacén de claves softtoken. El almacén de claves softtoken está disponible cuando la metarranura de la estructura criptográfica de Solaris se utilice para comunicarse con el dispositivo de hardware. El comando `ikecert` utiliza la biblioteca PKCS #11 para localizar el almacenamiento de claves.

- **Solaris 10 1/06:** a partir de esta versión, no es preciso especificar la biblioteca. De modo predeterminado, la biblioteca PKCS #11 es `/usr/lib/libpkcs11.so`.
- **Solaris 10:** en esta versión, debe especificarse la entrada PKCS #11. De lo contrario, la opción `-T` del comando `ikecert` no funcionará. La entrada tiene el siguiente aspecto:

```
pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
```

Para obtener más información, consulte la página del comando `man ikecert(1M)`. Para obtener información sobre la metarranura y el almacén de claves softtoken, consulte la página del comando `man cryptoadm(1M)`.

Comando `ikecert tokens`

El argumento `tokens` enumera los ID de testigo que están disponibles. Los ID de símbolo permiten a los comandos `ikecert certlocal` e `ikecert certdb` generar certificados de claves públicas y solicitudes de certificados. Los certificados y las solicitudes de certificados también se pueden almacenar mediante la estructura criptográfica del almacén de claves softtoken, o bien en una placa Sun Crypto Accelerator 4000 o Crypto Accelerator 6000 de Sun. El comando `ikecert` utiliza la biblioteca PKCS #11 para localizar el almacenamiento de certificados.

Comando `ikecert certlocal`

El subcomando `certlocal` administra la base de datos de claves privadas. Las opciones de este subcomando permiten agregar, ver y eliminar claves privadas. Este subcomando también crea un certificado autofirmado o una solicitud de certificado. La opción `-ks` crea un certificado autofirmado. La opción `-kc` crea una solicitud de certificado. Las claves se almacenan en el directorio `/etc/inet/secret/ike.privatekeys` del sistema o en el hardware conectado con la opción `-T`.

Al crear una clave privada, las opciones del comando `ikecert certlocal` deben tener entradas relacionadas en el archivo `ike/config`. La tabla siguiente muestra las correspondencias entre las opciones `ikecert` y las entradas `ike/config`.

TABLA 24-1 Correspondencias entre las opciones `ikecert` y las entradas `ike/config`

Opción <code>ikecert</code>	Entrada <code>ike/config</code>	Descripción
-A <i>nombre_alternativo_tema</i>	<code>cert_trust</code> <i>nombre_alternativo_tema</i>	Apodo que identifica el certificado de modo exclusivo. Los posibles valores son una dirección IP, una dirección de correo electrónico o un nombre de dominio.
-D <i>nombre_distinguido_X.509</i>	<i>nombre_distinguido_X.509</i>	El nombre completo de la autoridad de certificación que incluye el país (C), el nombre de organización (ON), la unidad organizativa (OU) y el nombre común (CN).
-t dsa-sha1	<code>auth_method dss_sig</code>	Método de autenticación que es ligeramente más lento que RSA .
-t rsa-md5 y -t rsa-sha1	<code>auth_method rsa_sig</code>	Método de autenticación que es ligeramente más lento que DSA . La clave pública RSA debe ser lo suficientemente grande para cifrar la carga útil mayor. Normalmente, una carga útil de identidad, como el nombre distinguido X.509, es la mayor carga útil.
-t rsa-md5 y -t rsa-sha1	<code>auth_method rsa_encrypt</code>	El cifrado RSA oculta las identidades de IKE de los intrusos, pero requiere que los equivalentes de IKE conozcan las claves públicas el uno del otro.
-T	<code>pkcs11_path</code>	La biblioteca PKCS #11 gestiona aceleración de claves en las placas de Sun Crypto Accelerator 1000, Crypto Accelerator 6000 de Sun y Sun Crypto Accelerator 4000. La biblioteca también proporciona los símbolos que gestionan el almacenamiento de claves en las placas de Sun Crypto Accelerator 4000 y Crypto Accelerator 6000 de Sun.

Si emite una solicitud de certificado con el comando `ikecert certlocal -kc`, envía el resultado del comando a una organización de PKI o a una autoridad de certificación. Si su compañía ejecuta su propio PKI, el resultado se envía al administrador de PKI. A continuación, la organización de PKI, la autoridad de certificación o el administrador de PKI crea los certificados. Los certificados que devuelve el PKI o la autoridad de certificación se incluyen en el subcomando `certdb`. La lista de revocación de certificados (CRL) que devuelve el PKI se incluye en el subcomando `certrlb`.

Comando `ikecert certdb`

El subcomando `certdb` administra la base de datos de claves públicas. Las opciones de este subcomando permiten agregar, ver y eliminar certificados y claves públicas. El comando acepta como entrada los certificados generados con el comando `ikecert certlocal -ks` en un sistema remoto. Para conocer el procedimiento, consulte [“Cómo configurar IKE con](#)

certificados de clave pública autofirmados” en la página 596. Este comando también acepta el certificado que recibe de un PKI o una autoridad de certificación. Para conocer el procedimiento, consulte “Cómo configurar IKE con certificados firmados por una autoridad de certificación” en la página 602.

Los certificados y las claves públicas se almacenan en el directorio `/etc/inet/ike/publickeys` del sistema. La opción `-T` almacena los certificados, las claves privadas y las claves públicas del hardware conectado.

Comando `ikecert certrladb`

El subcomando `certrladb` administra la base de datos de listas de revocación de certificados (CRL), `/etc/inet/ike/crls`. La base de datos de CRL mantiene las listas de revocación para las claves públicas. En esta lista se incluyen los certificados que dejan de ser válidos. Cuando los PKI proporcionan una CRL, puede instalar la CRL en la base de datos de CRL con el comando `ikecert certrladb`. Para conocer el procedimiento, consulte “Cómo administrar una lista de revocación de certificados” en la página 612.

Directorio `/etc/inet/ike/publickeys`

El directorio `/etc/inet/ike/publickeys` contiene la parte pública de un par de claves pública-privada y su certificado en los archivos, o *ranuras*. El directorio se protege en `0755`. El comando `ikecert certadb` rellena el directorio. La opción `-T` almacena las claves en la placa Sun Crypto Accelerator 4000 o Crypto Accelerator 6000 de Sun en lugar del directorio `publickeys`.

Las ranuras contienen, de modo codificado, el nombre distinguido X.509 de un certificado generado en otro sistema. Si está utilizando certificados autofirmados, se utiliza el certificado que se recibe del administrador del sistema remoto como entrada del comando. Si está utilizando certificados de una entidad certificadora (CA), puede instalar dos certificados firmados de ésta en la base de datos. Se instala un certificado que está basado en la solicitud de firma de certificado que envió a la entidad certificadora (CA). También se instala un certificado de la entidad certificadora (CA).

Directorio `/etc/inet/secret/ike.privatekeys`

El directorio `/etc/inet/secret/ike.privatekeys` contiene archivos de claves privadas que forman parte del par de claves pública-privada, que constituye material de claves para las asociaciones de seguridad de ISAKMP. El directorio se protege en `0700`. El comando `ikecert certlocal` rellena el directorio `ike.privatekeys`. Las claves privadas no son efectivas hasta que se instalan sus equivalentes de claves públicas, certificados autofirmados o autoridades de certificación. Los equivalentes de claves públicas se almacenan en el directorio `/etc/inet/ike/publickeys` o en una placa `&sca 4`; o Crypto Accelerator 6000 de Sun.

Directorio `/etc/inet/ike/crls`

El directorio `/etc/inet/ike/crls` contiene archivos de lista de revocación de certificados (CRL). Cada archivo corresponde a un archivo de certificado público del directorio `/etc/inet/ike/publickeys`. Las organizaciones de PKI proporcionan las CRL para sus certificados. Puede utilizar el comando `ikecert certrl db` para rellenar la base de datos.

Filtro IP en Oracle Solaris (descripción general)

En este capítulo se proporciona una visión general de filtro IP, una función de Oracle Solaris. Para conocer las tareas del filtro IP, consulte el [Capítulo 26, “Filtro IP \(tareas\)”](#).

Este capítulo contiene la información siguiente:

- “Novedades del filtro IP” en la página 637
- “Introducción al filtro” en la página 638
- “Procesamiento de paquetes del filtro IP” en la página 639
- “Directrices para utilizar el filtro IP” en la página 642
- “Uso de archivos de configuración del filtro IP” en la página 642
- “Cómo trabajar con conjuntos de reglas del filtro IP” en la página 643
- “Enlaces de filtros de paquetes” en la página 649
- “El filtro IP y el módulo `pf_l STREAMS`” en la página 649
- “IPv6 para filtro IP” en la página 650
- “Páginas del comando `man` del filtro IP” en la página 651

Novedades del filtro IP

En esta sección se describen las nuevas funciones del filtro IP.

Para ver una lista completa de las nuevas funciones y una descripción de las versiones de Oracle Solaris, consulte [Novedades de Oracle Solaris 10 8/11](#)

Enlaces de filtros de paquetes

A partir de la versión Solaris 10 7/07: se usan enlaces de filtros de paquetes para filtrado de paquetes en Oracle Solaris. Esta función ofrece las siguientes ventajas en lo que se refiere a la administración del sistema:

- Los enlaces de filtros de paquetes simplifican la configuración del filtro IP.

- Ahora se admite el uso de filtros de paquetes en las zonas.
- El uso de enlaces de filtros mejora el rendimiento del filtro IP.

Para obtener más información sobre estos enlaces, consulte [“Enlaces de filtros de paquetes” en la página 649](#). Para conocer las tareas asociadas con los enlaces de filtros de paquetes, consulte el [Capítulo 26, “Filtro IP \(tareas\)”](#).

Filtros de paquetes IPv6 para el filtro IP

SO Solaris 6/06: Para los administradores de sistemas que han configurado parte o toda la infraestructura de red con IPv6, se ha mejorado el filtro IP para que incluya filtros de paquetes IPv6. Los filtros de paquetes IPv6 pueden filtrar basándose en la dirección IPv6 de origen o destino, agrupaciones con direcciones IPv6 y encabezados de extensiones IPv6.

Se ha agregado la opción `-6` a los comandos `ipf` e `ipfstat` para utilizar con IPv6. Aunque no se ha modificado la interfaz de la línea de comandos para los comandos `ipmon` e `ippool`, estos comandos también admiten IPv6. Se ha mejorado el comando `ipmon` para admitir el registro de paquetes IPv6, y el comando `ippool` admite la inclusión de direcciones IPv6 en las agrupaciones.

Para obtener más información, consulte IPv6 para el filtro IP. Si desea conocer las tareas asociadas con los filtros de paquetes IPv6, consulte el [Capítulo 26, “Filtro IP \(tareas\)”](#).

Además, existe soporte para IPv6 en la función de traducción de direcciones de red (NAT) del filtro IP. Para obtener más información sobre NAT, consulte [“Uso de la función NAT del filtro IP” en la página 646](#).

Introducción al filtro

La función de filtro IP de Oracle Solaris sustituye el cortafuegos SunScreen en el sistema operativo. Al igual que el cortafuegos de SunScreen, el filtro IP proporciona filtros de paquetes con estado y traducción de direcciones de red (NAT). El filtro IP también incluye filtrado de paquetes sin estado y la posibilidad de crear y administrar agrupaciones de direcciones.

Los filtros de paquetes ofrecen protección básica contra ataques de la red. El filtro IP puede filtrar por dirección IP, puerto, protocolo, interfaz de red y dirección de tráfico. El filtro IP también puede filtrar por dirección IP de origen individual, dirección IP de destino, por intervalo de direcciones IP o por agrupaciones de direcciones.

El filtro IP se deriva de software de filtro IP de código abierto. Para ver las condiciones de la licencia, las atribuciones y los copyrights para el filtro IP de código abierto, la ruta predeterminada es `/usr/lib/ipf/IPFILTER.LICENCE`. Si se ha instalado Oracle Solaris en una ubicación que no sea la predeterminada, modifique la ruta para acceder al archivo en la ubicación correcta.

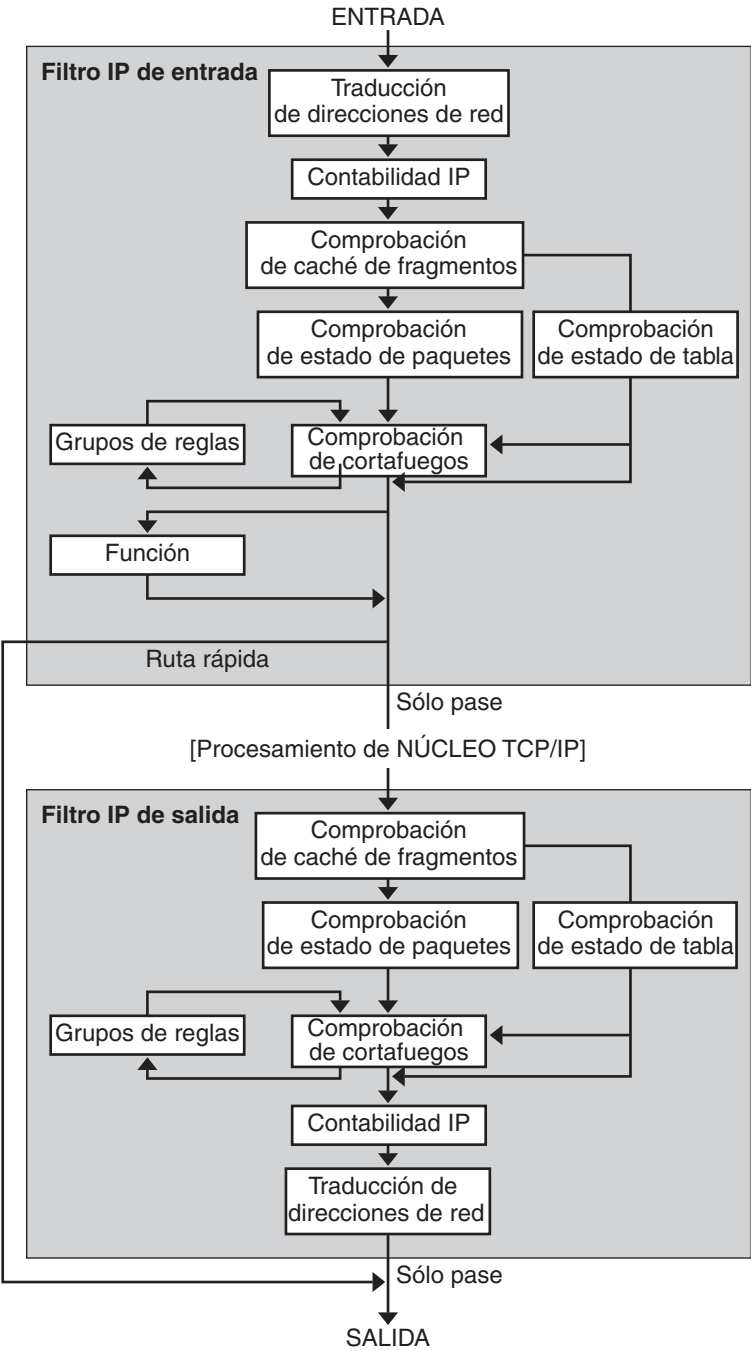
Orígenes de información para el filtro IP de código abierto

Encontrará la página de inicio del software de filtro IP de código abierto de Darren Reed en <http://coombs.anu.edu.au/~avalon/ip-filter.html>. Este sitio incluye información para el filtro IP de código abierto, incluido un vínculo a un tutorial llamado "IP Filter Based Firewalls HOWTO" (Brendan Conoboy y Erik Fichtner, 2002). Este tutorial incluye instrucciones paso a paso para configurar cortafuegos en un entorno BSD UNIX. Aunque el tutorial se ha escrito para un entorno BSD UNIX, también es necesario para la configuración de la función de filtro IP de Oracle Solaris.

Procesamiento de paquetes del filtro IP

El filtro IP ejecuta una secuencia de pasos cuando se procesa un paquete. El diagrama siguiente ilustra los pasos del procesamiento de paquetes y el modo en que los filtros se integran con la pila de protocolo TCP/IP.

FIGURA 25-1 Secuencia de procesamiento de paquetes



La secuencia de procesamiento de paquetes incluye lo siguiente:

- **Traducción de direcciones de red (NAT)**

La traducción de una dirección IP privada a una dirección pública distinta, o la asignación de alias de múltiples direcciones privadas a una sola dirección pública. NAT permite a una organización resolver el problema del agotamiento de direcciones IP cuando cuenta con redes y necesita acceder a Internet.

- **Cuentas IP**

Es posible configurar las reglas de entrada y salida por separado, y registrar el número de bytes que se transfieren. Cada vez que se produce una coincidencia de regla, el número de bytes del paquete se agrega a la regla y permite obtener las estadísticas de cascadas.

- **Comprobación de caché de fragmentación**

Si el siguiente paquete del tráfico actual es un paquete y se ha permitido el paquete anterior, también se permitirá el fragmento de paquete y se omitirá la tabla de estado y la comprobación de reglas.

- **Comprobación de estado de paquete**

Si en una regla se incluye keep state, todos los paquetes de una sesión específica se transfieren o bloquean automáticamente, según si la regla incluye pass o block.

- **Comprobación de cortafuegos**

Las reglas de entrada y salida se pueden configurar por separado, y determinar si un paquete podrá transferirse a través del filtro IP, a las rutinas TCP/IP del núcleo o hacia la red.

- **Grupos**

Los grupos permiten escribir un conjunto de reglas a modo de árbol.

- **Función**

Una función es la acción que se va a emprender. Las posibles funciones son block, pass, literal y send ICMP response.

- **Ruta rápida**

La ruta rápida señala al filtro IP que no debe transferir el paquete a la pila IP de UNIX para el enrutamiento, lo cual significa una reducción de TTL.

- **Autenticación IP**

Los paquetes que se autentican sólo se transfieren una vez a través de bucles de cortafuegos para evitar el procesamiento doble.

Directrices para utilizar el filtro IP

- Los servicios SMF `svc:/network/pfil` y `svc:/network/ipfilter` administran el filtro IP. Para ver una descripción completa de SMF, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)” de Guía de administración del sistema: administración básica](#). Si desea información detallada sobre los procedimientos asociados con SMF, consulte el [Capítulo 19, “Gestión de servicios \(tareas\)” de Guía de administración del sistema: administración básica](#).
- El filtro IP requiere la edición directa de los archivos de configuración.
- El filtro IP se instala como parte de Oracle Solaris. De modo predeterminado, el filtro IP no está activo en una instalación desde cero. Para configurar los filtros, debe editar los archivos de configuración y activar manualmente el filtro IP. Puede activar los filtros reiniciando el sistema o sondeando las interfaces con el comando `ifconfig`. Si desea más información, consulte la página de comando `man ifconfig(1M)`. Para conocer las tareas asociadas con la activación del filtro IP, consulte [“Configuración de filtro IP” en la página 653](#).
- Para administrar el filtro IP, debe asumir un rol que incluya el perfil de derechos de administración del filtro IP o convertirse en superusuario. Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- Las rutas múltiples de redes IP (IPMP) sólo admiten filtros sin estado.
- Las configuraciones de Sun Cluster no admiten filtros con el filtro IP.
- Los filtros entre zonas no se admiten con el filtro IP.

Uso de archivos de configuración del filtro IP

Puede utilizarse el filtro IP para proporcionar servicios de cortafuegos o traducción de direcciones de red (NAT). El filtro IP se puede implementar utilizando archivos de configuración que se puedan cargar. El filtro IP incluye un directorio denominado `/etc/ipf`. Puede crear y guardar archivos de configuración denominados `ipf.conf`, `ipnat.conf` e `ippool.conf` en el directorio `/etc/ipf`. Estos archivos se cargan automáticamente durante el proceso de inicio cuando residen en el directorio `/etc/ipf`. También puede guardar los archivos de configuración en otra ubicación y cargarlos manualmente. Para ver ejemplos de archivos de configuración, consulte [“Creación y edición de archivos de configuración del filtro IP” en la página 685](#).

Cómo trabajar con conjuntos de reglas del filtro IP

Para administrar el cortafuegos, utilice el filtro IP para especificar los conjuntos de reglas que se utilizarán para filtrar el tráfico de red. Puede crear los siguientes tipos de conjuntos de reglas:

- Conjuntos de reglas de filtros de paquetes
- Conjuntos de reglas de traducción de direcciones de red (NAT)

Asimismo, puede crear agrupaciones de direcciones para hacer referencia a grupos de direcciones IP. Estas agrupaciones podrán utilizarse más adelante en un conjunto de reglas. Las agrupaciones de direcciones aceleran el procesamiento de reglas. Asimismo, facilitan la administración de grupos de direcciones de gran tamaño.

Uso de la función de filtros de paquetes del filtro IP

Los filtros de paquetes se configuran con los conjuntos de reglas de filtros de paquetes. Utilice el comando `ipf` para trabajar con conjuntos de reglas de filtros de paquetes. Para obtener más información sobre el comando `ipf`, consulte el comando `ipf(1M)`.

Puede crear reglas de filtros de paquetes en la línea de comandos, utilizando el comando `ipf`, o en un archivo de configuración de filtros de paquetes. Si desea que las reglas de filtros de paquetes se carguen durante el inicio, cree un archivo de configuración denominado `/etc/ipf/ipf.conf` en el que colocar las reglas de filtros de paquetes. Si no desea que las reglas de filtros de paquetes se carguen durante el inicio, coloque el archivo `ipf.conf` en la ubicación que prefiera y active manualmente los filtros de paquetes utilizando el comando `ipf`.

Puede mantener dos conjuntos de reglas de filtros de paquetes con el filtro IP: el conjunto de reglas activo y el conjunto de reglas inactivo. En la mayoría de los casos, se trabaja con el conjunto de reglas activo. Sin embargo, el comando `ipf -I` permite aplicar la acción del comando a la lista de reglas inactivas. El filtro IP no utiliza la lista de reglas inactivas a menos que lo seleccione. La lista de reglas inactivas es un lugar donde guardar las reglas para que no afecten a los filtros de paquetes activos.

El filtro IP procesa las reglas de la lista de reglas desde el principio de la lista de reglas configuradas hasta el final, antes de transferir o bloquear un paquete. El filtro IP incluye un indicador que determina si se transferirá un paquete. Se aplica a todo el conjunto de reglas y determina si se transferirá o bloqueará el paquete basándose en la última regla coincidente.

Existen dos excepciones para este proceso. La primera tiene lugar si el paquete coincide con una regla que contenga la palabra clave `quick`. Si una regla incluye la palabra clave `quick`, se lleva a cabo la acción de dicha regla y no se comprueban las reglas subsiguientes. La segunda excepción se produce si el paquete coincide con una regla que contenga la palabra clave `group`. Si un paquete coincide con un grupo, sólo se comprueban las reglas etiquetadas con el grupo.

Configuración de reglas de filtros de paquetes

Utilice la sintaxis siguiente para crear reglas de filtros de paquetes:

acción [in|out] opción palabra clave, palabra clave...

1. Cada regla empieza por una acción. El filtro IP aplica la acción al paquete si éste coincide con la regla. La lista siguiente incluye las acciones utilizadas comúnmente que se aplican a un paquete.

block	Impide que el paquete se transfiera a través del filtro.
pass	Permite que el paquete se transfiera a través del filtro.
log	Registra el paquete pero no determina si se bloquea o se transfiere. Utilice el comando <code>ipmon</code> para ver el registro.
count	Incluye el paquete en las estadísticas de filtro. Utilice el comando <code>ipfstat</code> para ver las estadísticas.
skip <i>número</i>	Hace que el filtro omita <i>número</i> reglas de filtros.
auth	Solicita la autenticación de paquetes por parte de un programa de usuario que valida la información de paquetes. El programa determina si el paquete se transferirá o se bloqueará.

2. Según la acción que se lleve a cabo, la siguiente palabra debe ser `in` o `out`. Su elección determina si la regla de filtro de paquetes se aplica a un paquete entrante o saliente.
3. A continuación, puede elegir en una lista de opciones. Si utiliza más de una opción, debe hacerlo en el orden siguiente.

log	Registra el paquete si la regla es la última regla coincidente. Utilice el comando <code>ipmon</code> para ver el registro.
quick	Ejecuta la regla que contiene la opción <code>quick</code> si hay coincidencia de paquetes. Se detiene cualquier comprobación de reglas adicional.
on <i>nombre_interfaz</i>	Aplica la regla sólo si el paquete se transfiere a la interfaz especificada o desde ella.
dup- to <i>nombre_interfaz</i>	Copia el paquete y envía el duplicado de <i>nombre_interfaz</i> a una dirección IP especificada opcionalmente.
to <i>nombre_interfaz</i>	Transfiere el paquete a una cola de salida en <i>nombre_interfaz</i> .

4. Una vez especificadas las opciones, puede elegir entre varias palabras clave que determinan si el paquete coincide con la regla. Las siguientes palabras clave deben utilizarse en el orden que se indica.

Nota – De modo predeterminado, cualquier paquete que no coincida con ninguna regla en el archivo de configuración se transfiere a través del filtro.

<code>tos</code>	Filtra el paquete basándose en el valor de tipo de servicio expresado como entero decimal o hexadecimal.
<code>ttl</code>	Hace coincidir el paquete basándose en su valor de tiempo de vida. El valor de tiempo de vida que se guarda en un paquete indica el tiempo que puede permanecer un paquete en la red antes de que se descarte.
<code>proto</code>	Coincide con un protocolo específico. Puede utilizar cualquier nombre de protocolo especificado en el archivo <code>/etc/protocols</code> , o utilizar un número decimal para representar el protocolo. La palabra clave <code>tcp/udp</code> se puede utilizar para hacer coincidir un paquete TCP o UDP.
<code>from/to/all/ any</code>	Hace coincidir cualquiera o todos los elementos siguientes: la dirección IP de origen, la dirección IP de destino y el número de puerto. La palabra clave <code>all</code> se utiliza para aceptar paquetes de todos los orígenes y con todos los destinos.
<code>with</code>	Hace coincidir los atributos especificados asociados con el paquete. Inserte las palabras <code>not</code> o <code>no</code> delante de la palabra clave para que el paquete coincida sólo si no está presente la opción.
<code>flags</code>	Se utiliza para que TCP filtra basándose en los indicadores TCP configurados. Para obtener más información sobre los indicadores TCP, consulte la página del comando <code>man ipf(4)</code> .
<code>icmp-type</code>	Filtra de acuerdo con el tipo de ICMP. Esta palabra clave sólo se utiliza cuando la opción <code>proto</code> se configura como <code>icmp</code> y no se utiliza si se usa la opción <code>flags</code> .
<code>keep <i>opciones_guardado</i></code>	Determina la información que se guarda para un paquete. Las <i>opciones_guardado</i> disponibles incluyen las opciones <code>state</code> y <code>frags</code> . La opción <code>state</code> guarda información sobre la sesión y se puede guardar en paquetes TCP, UDP e ICMP. La opción <code>frags</code> guarda información sobre los fragmentos de paquetes y la aplica a fragmentos posteriores. <i>opciones_guardado</i> permite la transferencia de los paquetes coincidentes sin pasar por la lista de control de acceso.
<code>head <i>número</i></code>	Crea un grupo para las reglas de filtros, que se indica mediante el número <i>número</i> .

group *número*

Agrega la regla al número de grupo *número* en lugar de agregarla al grupo predeterminado. Todas las reglas de filtros se colocan en el grupo 0 si no se especifica otro.

El ejemplo siguiente ilustra cómo agrupar la sintaxis de reglas de filtros de paquetes para crear una regla. Para bloquear el tráfico entrante de la dirección IP 192.168.0.0/16, debe incluir la siguiente regla en la lista:

```
block in quick from 192.168.0.0/16 to any
```

Para ver la gramática y la sintaxis completas que se utiliza para escribir reglas de filtros de paquetes, consulte la página del comando `man ipf(4)`. Para conocer las tareas asociadas con los filtros de paquetes, consulte [“Gestión de conjunto de reglas de filtro de paquetes para filtro IP” en la página 667](#). Para ver una explicación del esquema de direcciones IP (192.168.0.0/16) de este ejemplo, consulte el [Capítulo 2, “Planificación de la red TCP/IP \(tareas\)”](#).

Uso de la función NAT del filtro IP

NAT establece las reglas de asignación que traducen las direcciones IP de origen y destino en otras direcciones de Internet o intranet. Estas reglas modifican las direcciones de origen y destino de los paquetes IP entrantes o salientes y envían los paquetes. También puede utilizar NAT para redirigir el tráfico de un puerto a otro. NAT mantiene la integridad del paquete durante cualquier modificación o redirección que se lleve a cabo en el paquete.

Utilice el comando `ipnat` para trabajar con listas de reglas NAT. Para obtener más información sobre el comando `ipnat`, consulte el comando [ipnat\(1M\)](#).

Puede crear reglas NAT en la línea de comandos, utilizando el comando `ipnat`, o en un archivo de configuración de NAT. Las reglas de configuración de NAT residen en el archivo `ipnat.conf`. Si desea que las reglas NAT se carguen durante el inicio, cree un archivo denominado `/etc/ipf/ipnat.conf` en el que colocar las reglas NAT. Si no desea que las reglas NAT se carguen durante el inicio, coloque el archivo `ipnat.conf` en la ubicación que prefiera y active manualmente los filtros de paquetes utilizando el comando `ipnat`.

Las reglas NAT pueden aplicarse tanto a direcciones IPv4 como IPv6. Sin embargo, no puede especificar los dos tipos de direcciones en una única regla. En lugar de ello, debe definir reglas separadas para cada tipo de dirección. En una regla NAT que incluye las direcciones IPv6, no puede utilizar los comandos NAT `mapproxy` y `rdproxy` simultáneamente.

Configuración de reglas NAT

La sintaxis siguiente permite crear reglas NAT:

comando nombre_interfaz parámetros

1. Cada regla empieza con uno de los comandos siguientes:

<code>map</code>	Asigna una red o dirección IP a otra red o dirección IP en un proceso por turnos.
<code>rdr</code>	Redirige los paquetes de una dirección IP y un par de puertos a otra dirección IP y otro par de puertos.
<code>bimap</code>	Establece una NAT bidireccional entre una dirección IP externa y una dirección IP interna.
<code>map-block</code>	Establece una traducción basada en una dirección IP estática. Este comando se basa en un algoritmo que fuerza la traducción de las direcciones en un intervalo de destino.

2. Después del comando, la siguiente palabra es el nombre de la interfaz, por ejemplo `hme0`.
3. A continuación, puede elegir entre una serie de parámetros, que determinan la configuración de NAT. Algunos de los parámetros son:

<code>ipmask</code>	Designa la máscara de red.
<code>dstipmask</code>	Designa la dirección a la que se traduce <code>ipmask</code> .
<code>mapport</code>	Designa los protocolos <code>tcp</code> , <code>udp</code> o <code>tcp/udp</code> , junto con una serie de números de puerto.

El ejemplo siguiente muestra cómo agrupar la sintaxis de reglas NAT para crear una regla NAT. Para volver a escribir un paquete saliente en el dispositivo `de0` con una dirección de origen de `192.168.1.0/24` y mostrar externamente su dirección de origen como `10.1.0.0/16`, debe incluir la siguiente regla en el conjunto de reglas NAT:

```
map de0 192.168.1.0/24 -> 10.1.0.0/16
```

Se aplican las siguientes reglas a las direcciones IPv6:

```
map ppp0 fec0:1::/64 -> 2000:1:2::/72 portmap tcp/udp 1025:65000
map-block ppp0 fe80:0:0:209::/64 -> 209:1:2::/72 ports auto
rdr ce0 209::ffff:fe13:e43e port 80 -> fec0:1::e,fec0:1::f port 80 tcp round-robin
```

Para ver la gramática y la sintaxis completas que se utilizan para escribir las reglas NAT, consulta la página del comando `man ipnat(4)`.

Uso de la función de agrupaciones de direcciones del filtro IP

Las agrupaciones de direcciones establecen una única referencia que se utiliza para asignar un nombre a un grupo de pares de direcciones/máscaras de red. Las agrupaciones de direcciones

proporcionan los procesos para reducir el tiempo necesario para hacer coincidir las direcciones IP con las reglas. Asimismo, facilitan la administración de grupos de direcciones de gran tamaño.

Las reglas de configuración de agrupaciones de direcciones residen en el archivo `ippool.conf`. Si desea que las reglas de agrupaciones de direcciones se carguen durante el inicio, cree un archivo denominado `/etc/ipf/ippool.conf` en el que colocar las reglas de agrupaciones de direcciones. Si no desea que las reglas de agrupaciones de direcciones se carguen durante el inicio, coloque el archivo `ippool.conf` en la ubicación que prefiera y active manualmente los filtros de paquetes con el comando `ippool`.

Configuración de agrupaciones de direcciones

Utilice la sintaxis siguiente para crear una agrupación de direcciones:

`table role = role-name type = storage-format number = reference-number`

table Define la referencia para las diferentes direcciones.

role Especifica el rol de la agrupación en el filtro IP. En este punto, el único rol al que se puede hacer referencia es `ipf`.

type Especifica el formato de almacenamiento de la agrupación.

number Especifica el número de referencia que utiliza la regla de filtros.

Por ejemplo, para hacer referencia al grupo de direcciones `10.1.1.1` y `10.1.1.2` y la red `192.16.1.0` como número de agrupación 13, debe incluir la siguiente regla en el archivo de configuración de agrupaciones de direcciones:

```
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24 };
```

A continuación, para hacer referencia al número de agrupación 13 en una regla de filtros, debe estructurar la regla de un modo similar al siguiente:

```
pass in from pool/13 to any
```

Observe que debe cargar el archivo de agrupaciones antes de cargar el archivo de reglas que contiene una referencia a la agrupación. Si no lo hace, la agrupación no estará definida, como en el ejemplo siguiente:

```
# ipfstat -io
empty list for ipfilter(out)
block in from pool/13(!) to any
```

Aunque agregue la agrupación más adelante, no se actualizará el conjunto de reglas del núcleo. También necesita volver a cargar el archivo de reglas que hace referencia a la agrupación.

Para ver la gramática y sintaxis completas que se utilizan para escribir las reglas de filtros de paquetes, consulte la página del comando `man ippool(4)`.

Enlaces de filtros de paquetes

A partir de la versión Solaris 10 7/07, los enlaces de filtros de paquetes reemplazan al módulo `pfil` para habilitar el filtro IP. En versiones anteriores de Solaris, se requería la configuración del módulo `pfil` como paso adicional para configurar el filtro IP. Este requisito de configuración adicional aumentaba el riesgo de errores que ocasionarían un funcionamiento incorrecto del filtro IP. La inserción del módulo `pfil` STREAMS entre la dirección IP y el controlador de dispositivos también afectaba al rendimiento. Por último, el módulo `pfil` no podía interceptar paquetes entre zonas.

El uso de los enlaces de filtros de paquetes mejora el procedimiento para habilitar el filtro IP. A través de estos enlaces, el filtro IP utiliza bifurcaciones de filtros previas al enrutamiento (entrada) y posteriores al enrutamiento (salida) para controlar el flujo de paquetes que entran y salen del sistema Oracle Solaris.

Los enlaces de filtros de paquetes acaban con la necesidad del módulo `pfil`. Por tanto, también se eliminan los siguientes componentes asociados con el módulo.

- Controlador `pfil`
- Daemon `pfil`
- Servicio SMF `svc:/network/pfil`

Para conocer las tareas asociadas con la activación del filtro IP de , consulte el [Capítulo 26](#), “Filtro IP (tareas)”.

El filtro IP y el módulo `pfil` STREAMS

Nota – El módulo `pfil` se utiliza con el filtro IP en las siguientes versiones de Solaris:

- Solaris 10 3/05
- Solaris 10 1/06
- Solaris 10 6/06
- Solaris 10 11/06

A partir de la versión Solaris 10 7/07, el módulo `pfil` se ha sustituido por los enlaces de filtros de paquetes y ya no se utiliza con el filtro IP.

El módulo `pfil STREAMS` es necesario para habilitar el filtro IP. Sin embargo, el filtro IP no proporciona un mecanismo automático para utilizar el módulo en cada interfaz. En lugar de ello, el módulo `pfil STREAMS` lo administra el servicio SMF `svc:/network/pfil`. Para activar los filtros en una interfaz de red, primero debe configurar el archivo `pfil.ap`. A continuación, active el servicio `svc:/network/pfil` para proporcionar el módulo `pfil STREAMS` a la interfaz de red. Para que el módulo `STREAMS` surta efecto, es necesario reiniciar el sistema o desconectar y volver a sondear cada interfaz de red en la que desee aplicar los filtros. Para activar las funciones de los filtros de paquetes IPv6, debe sondear la versión `inet6` de la interfaz.

Si no se encuentra ningún módulo `pfil` para las interfaces de red, los servicios SMF se colocan en el estado de mantenimiento. La causa más común de esta situación es un archivo `/etc/ipf/pfil.ap` editado de forma incorrecta. Si el servicio se coloca en el modo de mantenimiento, su aparición se registra en los archivos de registro de filtros.

Para ver las tareas asociadas con la activación del filtro IP, consulte “[Configuración de filtro IP](#)” en la [página 653](#).

IPv6 para filtro IP

A partir de Solaris 6/06, el filtro IP de Solaris es compatible con IPv6. Los filtros de paquetes IPv6 pueden filtrar basándose en la dirección IPv6 de origen o destino, agrupaciones con direcciones IPv6 y encabezados de extensiones IPv6.

IPv6 es similar a IPv4 en muchos aspectos. Sin embargo, el tamaño del paquete y el encabezado son diferentes en las dos versiones de IP, lo cual es una consideración importante para el filtro IP. Los paquetes IPv6 conocidos como *jumbogramas* contienen un datagrama de más de 65.535 bytes. El filtro IP no admite jumbogramas de IPv6. Para obtener más información sobre otras funciones de IPv6, consulte “[Características principales de IPv6](#)” en la [página 72](#).

Nota – Si desea más información sobre los jumbogramas, consulte el documento IPv6 Jumbograms, RFC 2675 de Internet Engineering Task Force (IETF). [<http://www.ietf.org/rfc/rfc2675.txt>]

Las tareas del filtro IP asociadas con IPv6 no son muy diferentes de IPv4. La diferencia más notable es el uso de la opción `-6` con determinados comandos. Tanto los comandos `ipf` como `ipfstat` incluyen la opción `-6` para utilizar los filtros de paquetes IPv6. Utilice la opción `-6` con el comando `ipf` para cargar y vaciar las reglas de filtros de paquetes IPv6. Para ver las estadísticas de IPv6, utilice la opción `-6` con el comando `ipfstat`. Los comandos `ipmon` e `ippool` también admiten IPv6, aunque no hay ninguna opción asociada para la compatibilidad con IPv6. El comando `ipmon` se ha mejorado para permitir el registro de paquetes IPv6. El

comando `ippool` admite las agrupaciones con las direcciones IPv6. Puede crear agrupaciones sólo de direcciones IPv4 o IPv6, o una agrupación que contenga tanto direcciones IPv4 como IPv6.

Puede utilizar el archivo `ipf6.conf` para crear conjuntos de reglas de filtros de paquetes para IPv6. De modo predeterminado, el archivo de configuración `ipf6.conf` se incluye en el directorio `/etc/ipf`. Al igual que con los demás archivos de configuración de filtros, el archivo `ipf6.conf` se carga automáticamente durante el proceso de inicio cuando se almacena en el directorio `/etc/ipf`. También puede crear y guardar un archivo de configuración IPv6 en otra ubicación y cargar el archivo manualmente.

Una vez configuradas las reglas de filtros de paquetes para IPv6, active las funciones de filtros de paquetes IPv6 sondeando la versión `inet6` de la interfaz.

Para obtener más información sobre IPv6, consulte el [Capítulo 3, “Introducción a IPv6 \(descripción general\)”](#). Para conocer las tareas asociadas con el filtro IP, consulte el [Capítulo 26, “Filtro IP \(tareas\)”](#).

Páginas del comando man del filtro IP

La tabla siguiente incluye la documentación de la página del comando man relativa al filtro IP.

Página de comando man	Descripción
ipf(1M)	Utilice el comando <code>ipf</code> para: <ul style="list-style-type: none">■ Trabajar con conjuntos de reglas de filtros de paquetes.■ Desactivar y activar los filtros.■ Restablecer las estadísticas y volver a sincronizar la lista de interfaces del núcleo con la lista de estado de la interfaz actual.
ipf(4)	Contiene la gramática y la sintaxis para crear reglas de filtros de paquetes del filtro IP.
ipfilter(5)	Proporciona información de licencia del filtro IP de código abierto.
ipfs(1M)	Utilice el comando <code>ipfs</code> para guardar y restablecer la información NAT y la de la tabla de estado tras los reinicios.
ipfstat(1M)	Utilice el comando <code>ipfstat</code> para recuperar y mostrar las estadísticas de procesamiento de paquetes.
ipmon(1M)	Utilice el comando <code>ipmon</code> para abrir el dispositivo de registro y ver los paquetes registrados para NAT y los filtros de paquetes.

Página de comando man	Descripción
ipnat(1M)	Utilice el comando <code>ipnat</code> para: <ul style="list-style-type: none">■ Trabajar con reglas NAT.■ Recuperar y ver las estadísticas de NAT.
ipnat(4)	Contiene la gramática y sintaxis para crear reglas NAT.
ippool(1M)	Utilice el comando <code>ippool</code> para crear y administrar agrupaciones de direcciones.
ippool(4)	Contiene la gramática y la sintaxis para crear agrupaciones de direcciones del filtro IP.
nnd(1M)	Muestra los parámetros de filtros actuales del módulo <code>pf il</code> STREAMS y los valores actuales de los parámetros ajustables.

Filtro IP (tareas)

Este capítulo proporciona instrucciones detalladas para las tareas. Para obtener información general sobre el Filtro IP, consulte el [Capítulo 25, “Filtro IP en Oracle Solaris \(descripción general\)”](#).

Este capítulo contiene la información siguiente:

- “Configuración de filtro IP” en la página 653
- “Desactivación y deshabilitación de filtro IP” en la página 657
- “Cómo trabajar con el módulo `pf il`” en la página 659
- “Cómo trabajar con conjuntos de reglas del filtro IP” en la página 666
- “Cómo visualizar las estadísticas e información sobre el filtro IP” en la página 678
- “Cómo trabajar con archivos de registro para el filtro IP” en la página 681
- “Creación y edición de archivos de configuración del filtro IP” en la página 685

Configuración de filtro IP

El siguiente mapa de tareas identifica los procedimientos asociados con la configuración del filtro IP.

TABLA 26–1 Configuración del filtro IP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Habilitar inicialmente el filtro IP	El filtro IP no está habilitado de modo predeterminado. Debe habilitarlo manualmente o utilizar los archivos de configuración del directorio <code>/etc/ipf/</code> y reiniciar el sistema. A partir de la versión Solaris 10 7/07, los enlaces de filtros de paquetes reemplazan al módulo <code>pf il</code> para habilitar el filtro IP.	“Cómo habilitar el filtro IP” en la página 654

TABLA 26-1 Configuración del filtro IP (mapa de tareas) <i>(Continuación)</i>		
Tarea	Descripción	Para obtener instrucciones
Volver a habilitar el filtro IP	Si el filtro IP está desactivado o deshabilitado, puede volver a activarlo reiniciando el sistema o utilizando el comando <code>ipf</code> .	“Cómo reabilitar el filtro IP” en la página 655
Habilitar filtrado de bucle de retorno	De modo opcional, puede activar el filtrado en bucle, por ejemplo, para filtrar el tráfico entre zonas.	“Cómo habilitar los filtros en bucle de retorno” en la página 656

▼ Cómo habilitar el filtro IP

- Utilice este procedimiento para habilitar el filtro IP en un sistema en el que se ejecute como mínimo el sistema operativo Solaris 10 7/07. Para habilitar los filtros IP si el sistema tiene una versión de Oracle Solaris 10 anterior a la Solaris 10 7/07, consulte [“Cómo trabajar con el módulo `pf`” en la página 659](#).
- 1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de *Guía de administración del sistema: servicios de seguridad*](#).
 - 2 Cree un conjunto de reglas de filtros de paquetes.**

El conjunto de reglas de filtros de paquetes contiene reglas de filtros de paquetes que utiliza el filtro IP. Si desea cargar las reglas de filtros de paquetes en el momento de iniciar, edite el archivo `/etc/ipf/ipf.conf` para implementar los filtros de paquetes IPv4. Utilice el archivo `/etc/ipf/ipf6.conf` para las reglas de filtros de paquetes IPv6. Si no desea cargar las reglas de filtros de paquetes al iniciar, colóquelas en un archivo y active manualmente los filtros de paquetes. Para obtener información sobre los filtros de paquetes, consulte [“Uso de la función de filtros de paquetes del filtro IP” en la página 643](#). Para obtener información sobre cómo trabajar con los archivos de configuración, consulte [“Creación y edición de archivos de configuración del filtro IP” en la página 685](#).
 - 3 (Opcional) Cree un archivo de configuración de traducción de direcciones de red (NAT).**

Nota – La traducción de direcciones de red (NAT) no admite IPv6.

Cree un archivo `ipnat.conf` si desea utilizar la traducción de direcciones de red. Si desea que las reglas NAT se carguen durante el inicio, cree un archivo denominado `/etc/ipf/ipnat.conf` en el que colocar las reglas NAT. Si no desea cargar las reglas NAT al iniciar, coloque el archivo `ipnat.conf` en la ubicación que desee y active manualmente las reglas NAT.

Para obtener más información sobre NAT, consulte [“Uso de la función NAT del filtro IP” en la página 646](#).

4 (Opcional) Cree un archivo de configuración de agrupaciones de direcciones.

Cree un archivo `ipool.conf` si desea hacer referencia a una agrupación de direcciones como una única agrupación. Si desea que el archivo de configuración de agrupaciones de direcciones se cargue al inicio, cree un archivo denominado `/etc/ipf/ippool.conf` en el que colocar la agrupación de direcciones. Si no desea cargar el archivo de configuración de la agrupación de direcciones al inicio, coloque el archivo `ippool.conf` en la ubicación que desee y active las reglas manualmente.

Una agrupación de direcciones sólo puede contener direcciones IPv4 o IPv6. También puede contener tanto direcciones IPv4 como direcciones IPv6.

Para obtener más información sobre las agrupaciones de direcciones, consulte [“Uso de la función de agrupaciones de direcciones del filtro IP” en la página 647](#).

5 (Opcional) Habilite el filtro de tráfico en bucle de retorno.

Si desea filtrar el tráfico entre zonas que están configuradas en el sistema, debe activar los filtros en bucle. Consulte [“Cómo habilitar los filtros en bucle de retorno” en la página 656](#). Asegúrese de definir también los conjuntos de reglas adecuados que se aplican a las zonas.

6 Active el filtro IP.

```
# svcadm enable network/ipfilter
```

▼ Cómo rehabilitar el filtro IP

Puede volver a habilitar los filtros de paquetes que estén deshabilitados temporalmente.

1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Habilite el filtro IP y los filtros utilizando uno de los métodos siguientes:

- Reinicie el equipo.

```
# reboot
```

Nota – Al habilitar el filtro IP, tras reiniciar se cargan los siguientes archivos si están presentes: el archivo `/etc/ipf/ipf.conf`, el archivo `/etc/ipf/ipf6.conf` cuando se utiliza IPv6 o el archivo `/etc/ipf/ipnat.conf`.

- Ejecute la siguiente serie de comandos para habilitar el filtro IP y activar los filtros:

- a. Habilite el filtro IP.

```
# ipf -E
```

- b. Active los filtros de paquetes.

```
# ipf -f filename
```

- c. (Opcional) Active NAT.

```
# ipnat -f filename
```

Nota – La traducción de direcciones de red (NAT) no admite IPv6.

▼ Cómo habilitar los filtros en bucle de retorno

Nota – Sólo se puede filtrar tráfico de bucle de retorno si el sistema ejecuta como mínimo Solaris 10 7/07. En las versiones anteriores de Oracle Solaris 10 no se admite el filtro en bucle.

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Detenga el filtro IP de si se está ejecutando.**

```
# svcadm disable network/ipfilter
```

- 3 **Edite los archivos `/etc/ipf.conf` o `/etc/ipf6.conf` agregando la línea siguiente al principio del archivo:**

```
set intercept_loopback true;
```

Esta línea debe preceder a todas las reglas de filtros IP que se definan en el archivo. Sin embargo, puede insertar comentarios delante de la línea, como en el ejemplo siguiente:

```
#  
# Enable loopback filtering to filter between zones  
#
```



```
set intercept_loopback true;
#
# Define policy
#
block in all
block out all
<other rules>
...
```

4 Inicie el filtro IP.

```
# svcadm enable network/ipfilter
```

5 Para comprobar el estado de los filtros en bucle de retorno, utilice el comando siguiente:

```
# ipf -T ipf_loopback
ipf_loopback min 0 max 0x1 current 1
#
```

Si el filtro en bucle de retorno está deshabilitado, el comando producirá el resultado siguiente:

```
ipf_loopback min 0 max 0x1 current 0
```

Desactivación y deshabilitación de filtro IP

La deshabilitación del filtro de paquetes y NAT resulta útil en las siguientes circunstancias:

- Para realizar pruebas
- Para resolver problemas del sistema cuando se cree que los causa el filtro IP

El siguiente mapa de tareas identifica los procedimientos asociados con la desactivación de las funciones del filtro IP.

TABLA 26-2 Desactivación del filtro IP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Desactive los filtros de paquetes.	Desactive los filtros de paquetes utilizando el comando ipf.	“Cómo desactivar los filtros de paquetes” en la página 657
Desactive NAT.	Desactive NAT utilizando el comando ipnat.	“Cómo desactivar NAT” en la página 658
Desactive los filtros de paquetes y NAT.	Desactive los filtros de paquetes y NAT utilizando el comando ipf.	“Cómo deshabilitar los filtros de paquetes” en la página 659

▼ Cómo desactivar los filtros de paquetes

El siguiente procedimiento desactiva los filtros de paquetes del filtro IP vaciando las reglas de filtros de paquetes desde el conjunto de reglas de filtros activo. Este procedimiento no deshabilita el filtro IP. Puede volver a activar el filtro IP agregando reglas al conjunto de reglas.

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Use uno de los métodos siguientes para desactivar las reglas de filtro IP:**

- Elimine el conjunto de reglas activo desde el núcleo.

```
# ipf -Fa
```

Este comando desactiva todas las reglas de filtros de paquetes.

- Elimine las reglas de filtros de paquetes entrantes.

```
# ipf -Fi
```

Este comando desactiva las reglas de filtros de paquetes para los paquetes entrantes.

- Elimine las reglas de filtros de paquetes salientes.

```
# ipf -Fo
```

Este comando desactiva las reglas de filtros de paquetes para los paquetes salientes.

▼ **Cómo desactivar NAT**

Con el procedimiento siguiente se desactivan las reglas NAT del filtro IP vaciándolas desde el conjunto de reglas NAT activo. Este procedimiento no deshabilita el filtro IP. Puede volver a activar el filtro IP agregando reglas al conjunto de reglas.

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Elimine NAT del núcleo.**

```
# ipnat -FC
```

La opción -C elimina todas las entradas de la lista de reglas NAT actual. La opción -F elimina todas las entradas activas de la tabla de traducciones NAT activa, que muestra las asignaciones NAT activas.

▼ Cómo deshabilitar los filtros de paquetes

Al ejecutar este procedimiento, se eliminan del núcleo tanto los filtros de paquetes como NAT. Si utiliza este procedimiento, debe volver a habilitar el filtro IP para reactivar el filtro de paquetes y NAT. Para más información, consulte [“Cómo rehabilitar el filtro IP” en la página 655](#).

- 1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**
Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 Desactive los filtros de paquetes y permita a todos los paquetes pasar a la red.**

`ipf -D`

Nota – El comando `ipf -D` vacía las reglas del conjunto de reglas. Al volver a activar los filtros, debe agregar reglas al conjunto de reglas.

Cómo trabajar con el módulo `pf`

En esta sección se describe cómo utilizar el módulo `pf` STREAMS para activar o desactivar el filtro IP y cómo ver las estadísticas de `pf`. Los procedimientos sólo se aplican a los sistemas que ejecutan una de las siguientes versiones de Solaris:

- Solaris 10 3/05
- Solaris 10 1/06
- Solaris 10 6/06
- Solaris 10 11/06

El siguiente mapa de tareas identifica los procedimientos asociados con la configuración del módulo `pf`.

TABLA 26-3 Módulo `pf` (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Habilitar filtro IP	El filtro IP no está habilitado de modo predeterminado. Debe habilitarlo manualmente o utilizar los archivos de configuración del directorio <code>/etc/ipf/</code> y reiniciar el sistema.	“How to Enable IP Filter in Previous Solaris Releases” en la página 660

TABLA 26-3 Módulo pfil (mapa de tareas) (Continuación)

Tarea	Descripción	Para obtener instrucciones
Activar una NIC para los filtros de paquetes	Configure el módulo pfil para activar los filtros de paquetes e una tarjeta NIC.	“Cómo activar una NIC para los filtros de paquetes” en la página 662
Desactivar filtro IP en una NIC	Elimine una tarjeta NIC y permita que todos los paquetes pasen a través de ella.	“Cómo desactivar el filtro IP en una NIC” en la página 664
Visualice las estadísticas de pfil.	Visualice las estadísticas del módulo pfil para poder resolver los problemas relativos al filtro IP utilizando el comando ndd.	“Cómo visualizar las estadísticas de pfil para el filtro IP” en la página 665

▼ How to Enable IP Filter in Previous Solaris Releases

El filtro IP se instala con Oracle Solaris. Sin embargo, los filtros de paquetes no están habilitados de modo predeterminado. Siga este procedimiento para activar el filtro IP.

Nota – Si el sistema ejecuta como mínimo la versión Solaris 10 7/07, siga el procedimiento [“Cómo habilitar el filtro IP” en la página 654](#) que utiliza los enlaces de filtros de paquetes.

1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Inicie el editor de archivos que prefiera y edite el archivo /etc/ipf/pfil.ap.

Este archivo contiene los nombres de las tarjetas de interfaz de red (NIC) del host. De modo predeterminado, los nombres están comentados. Elimine el comentario de los nombres de dispositivo que llevan el tráfico de red que desea filtrar. Si el nombre de la NIC del sistema no aparece en la lista, agregue una línea para especificar la tarjeta NIC.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major minor lastminor modules

#le      -1      0      pfil
#qe      -1      0      pfil
hme      -1      0      pfil (Device has been uncommented for filtering)
```

```
#qfe -1 0 pfil
#eri -1 0 pfil
#ce -1 0 pfil
#bge -1 0 pfil
#be -1 0 pfil
#vge -1 0 pfil
#ge -1 0 pfil
#nf -1 0 pfil
#fa -1 0 pfil
#ci -1 0 pfil
#el -1 0 pfil
#ipdptp -1 0 pfil
#lane -1 0 pfil
#dmfe -1 0 pfil
```

3 Active los cambios en el archivo `/etc/ipf/pfil.conf` ap reiniciando la instancia del servicio `network/pfil`.

```
# svcadm restart network/pfil
```

4 Cree un conjunto de reglas de filtros de paquetes.

El conjunto de reglas de filtros de paquetes contiene reglas de filtros de paquetes que utiliza el filtro IP. Si desea cargar las reglas de filtros de paquetes en el momento de iniciar, edite el archivo `/etc/ipf/ipf.conf` para implementar los filtros de paquetes IPv4. Utilice el archivo `/etc/ipf/ipf6.conf` para las reglas de filtros de paquetes IPv6. Si no desea cargar las reglas de filtros de paquetes al iniciar, colóquelas en un archivo y active manualmente los filtros de paquetes. Para obtener información sobre los filtros de paquetes, consulte [“Uso de la función de filtros de paquetes del filtro IP” en la página 643](#). Para obtener información sobre cómo trabajar con los archivos de configuración, consulte [“Creación y edición de archivos de configuración del filtro IP” en la página 685](#).

5 (Opcional) Cree un archivo de configuración de traducción de direcciones de red (NAT).

Nota – La traducción de direcciones de red (NAT) no admite IPv6.

Cree un archivo `ipnat.conf` si desea utilizar la traducción de direcciones de red. Si desea que las reglas NAT se carguen durante el inicio, cree un archivo denominado `/etc/ipf/ipnat.conf` en el que colocar las reglas NAT. Si no desea cargar las reglas NAT al iniciar, coloque el archivo `ipnat.conf` en la ubicación que desee y active manualmente las reglas NAT.

Para obtener más información sobre NAT, consulte [“Uso de la función NAT del filtro IP” en la página 646](#).

6 (Opcional) Cree un archivo de configuración de agrupaciones de direcciones.

Cree un archivo `ipool.conf` si desea hacer referencia a una agrupación de direcciones como una única agrupación. Si desea que el archivo de configuración de agrupaciones de direcciones se cargue al inicio, cree un archivo denominado `/etc/ipf/ippool.conf` en el que colocar la

agrupación de direcciones. Si no desea cargar el archivo de configuración de la agrupación de direcciones al inicio, coloque el archivo `ippool.conf` en la ubicación que desee y active las reglas manualmente.

Una agrupación de direcciones sólo puede contener direcciones IPv4 o IPv6. También puede contener tanto direcciones IPv4 como direcciones IPv6.

Para obtener más información sobre las agrupaciones de direcciones, consulte [“Uso de la función de agrupaciones de direcciones del filtro IP” en la página 647](#).

7 Active el filtro IP siguiendo uno de estos métodos:

- Habilite el filtro IP y reinicie el equipo.

```
# svcadm enable network/ipfilter
# reboot
```

Nota – Es necesario reiniciar si no puede utilizar los comandos `ifconfig unplumb` y `ifconfig plumb` con seguridad en las tarjetas NIC.

- Active las tarjetas NIC utilizando los comandos `ifconfig unplumb` e `ifconfig plumb`. A continuación, active el filtro IP. La versión `inet6` de la interfaz debe estar sondeada para poder implementar los filtros de paquetes IPv6.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20 netmask 255.255.255.0 up
# ifconfig hme0 inet6 unplumb
# ifconfig hme0 inet6 plumb fec3:f849::1/96 up
# svcadm enable network/ipfilter
```

Para obtener más información sobre el comando `ifconfig`, consulte la página del comando `man ifconfig(1M)`.

▼ Cómo activar una NIC para los filtros de paquetes

El filtro IP está habilitado durante el arranque cuando existe el archivo `/etc/ipf/ipf.conf` (o el archivo `/etc/ipf/ipf6.conf` si se utiliza IPv6). Si necesita habilitar los filtros en una NIC después de habilitar el filtro IP, utilice el procedimiento siguiente.

1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Inicie el editor de archivos que prefiera y edite el archivo `/etc/ipf/pfil.ap`.

Este archivo contiene los nombres de las NIC del host. De modo predeterminado, los nombres están comentados. Elimine el comentario de los nombres de dispositivo que llevan el tráfico de red que desea filtrar. Si el nombre de la NIC del sistema no aparece en la lista, agregue una línea para especificar la tarjeta NIC.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor  lastminor  modules

#le      -1      0      pfil
#qe      -1      0      pfil
hme      -1      0      pfil (Device has been uncommented for filtering)
#qfe     -1      0      pfil
#eri     -1      0      pfil
#ce      -1      0      pfil
#bge     -1      0      pfil
#be      -1      0      pfil
#vge     -1      0      pfil
#ge      -1      0      pfil
#nf      -1      0      pfil
#fa      -1      0      pfil
#ci      -1      0      pfil
#el      -1      0      pfil
#ipdptp  -1      0      pfil
#lane    -1      0      pfil
#dmfe    -1      0      pfil
```

3 Active los cambios en el archivo `/etc/ipf/pfil.ap` reiniciando la instancia del servicio `network/pfil`.

```
# svcadm restart network/pfil
```

4 Active la NIC siguiendo uno de estos métodos:

- Reinicie el equipo.

```
# reboot
```

Nota – Es necesario reiniciar si no puede utilizar los comandos `ifconfig unplumb` y `ifconfig plumb` con seguridad en las tarjetas NIC.

- Active las NIC que desee filtrar utilizando el comando `ifconfig` con las opciones `unplumb` y `plumb`. La versión `inet6` de cada interfaz debe estar sondeada para poder implementar los filtros de paquetes IPv6.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20 netmask 255.255.255.0 up
```

```
# ifconfig hme0 inet6 unplumb
# ifconfig hme0 inet6 plumb fec3:f840::1/96 up
```

Para obtener más información acerca del comando `ifconfig`, consulte la página del comando `man ifconfig(1M)`.

▼ Cómo desactivar el filtro IP en una NIC

Siga el procedimiento a continuación para detener los paquetes de filtros en una tarjeta NIC.

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Inicie el editor de archivos que prefiera y edite el archivo `/etc/ipf/pfil.ap`.**

Este archivo contiene los nombres de las NIC del host. Se eliminan los comentarios de las NIC que se han utilizando para filtrar el tráfico de red. Elimine los comentarios de los nombres de dispositivos que ya no desee utilizar para filtrar el tráfico de red.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major minor lastminor modules

#le -1 0 pfil
#qe -1 0 pfil
#hme -1 0 pfil (Commented-out device no longer filters network traffic)
#qfe -1 0 pfil
#eri -1 0 pfil
#ce -1 0 pfil
#bge -1 0 pfil
#be -1 0 pfil
#vge -1 0 pfil
#ge -1 0 pfil
#nf -1 0 pfil
#fa -1 0 pfil
#ci -1 0 pfil
#el -1 0 pfil
#ipdptp -1 0 pfil
#lane -1 0 pfil
#dmfe -1 0 pfil
```

- 3 **Desactive la NIC utilizando uno de estos métodos:**

- Reinicie el equipo.


```
# reboot
```

Nota – Es necesario reiniciar si no puede utilizar los comandos `ifconfig unplumb` y `ifconfig plumb` con seguridad en las tarjetas NIC.

- Desactive las tarjetas NIC utilizando el comando `ifconfig` con las opciones `unplumb` y `plumb`. La versión `inet6` de cada interfaz no debe estar sondeada para poder desactivar los filtros de paquetes IPv6. realice los siguientes pasos. El dispositivo de ejemplo del sistema es `hme`:

- a. Identifique el "major number" del dispositivo que está desactivando.

```
# grep hme /etc/name_to_major
hme 7
```

- b. Visualice la configuración actual de `autopush` para `hme0`.

```
# autopush -g -M 7 -m 0
Major      Minor      Lastminor      Modules
7          ALL        -              pfil
```

- c. Elimine la configuración de `autopush`.

```
# autopush -r -M 7 -m 0
```

- d. Abra el dispositivo y asígnele las direcciones IP.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20 netmask 255.255.255.0 up
# ifconfig hme0 inet6 unplumb
# ifconfig hme0 inet6 plumb fec3:f840::1/96 up
```

Para obtener más información acerca del comando `ifconfig`, consulte la página del comando `man ifconfig(1M)`.

▼ Cómo visualizar las estadísticas de `pfil` para el filtro IP

Cuando esté resolviendo problemas del filtro IP, puede ver las estadísticas de `pfil`.

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Visualice las estadísticas de `pfil`.**

```
# ndd -get /dev/pfil qif_status
```

Ejemplo 26-1 Visualización de las estadísticas de `pfil` para el filtro IP

El ejemplo siguiente muestra cómo visualizar las estadísticas de `pfil`.

```
# ndd -get /dev/pfil qif_status
ifname ill q OTHERQ num sap hl nr nw bad copy copyfail drop notip nodata
notdata
QIF6 0 300011247b8 300011248b0 6 806 0 4 9 0 0 0 0 0 0 0
dmfel 3000200a018 30002162a50 30002162b48 5 800 14 171 13681 0 0 0 0 0 0 0
```

Cómo trabajar con conjuntos de reglas del filtro IP

El siguiente mapa de tareas identifica los procedimientos asociados con los conjuntos de reglas del filtro IP.

TABLA 26-4 Cómo trabajar con conjuntos de reglas del filtro IP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Administre, vea y modifique los conjuntos de reglas de filtros de paquetes del filtro IP.		“Gestión de conjunto de reglas de filtro de paquetes para filtro IP” en la página 667
	Visualiza un conjunto de reglas de filtros de paquetes activo.	“Cómo visualizar el conjunto de reglas de filtros de paquetes activo” en la página 668
	Visualiza un conjunto de reglas de filtros de paquetes inactivo.	“Cómo visualizar el conjunto de reglas de filtros de paquetes inactivo” en la página 668
	Activa un conjunto de reglas activo distinto.	“Cómo activar un conjunto de reglas de filtros de paquetes diferente o actualizado” en la página 668
	Elimina un conjunto de reglas.	“Cómo eliminar un conjunto de reglas de filtros de paquetes” en la página 670
	Agrega reglas a los conjuntos de reglas.	“Cómo anexar reglas al conjunto de reglas de filtros de paquetes activo” en la página 671 “Cómo anexar reglas al conjunto de reglas de filtros de paquetes inactivo” en la página 672
	Pasa de los conjuntos de reglas activos a los inactivos y viceversa.	“Cómo alternar entre los conjuntos de reglas de filtros de paquetes activo e inactivo” en la página 672

TABLA 26-4 Cómo trabajar con conjuntos de reglas del filtro IP (mapa de tareas) *(Continuación)*

Tarea	Descripción	Para obtener instrucciones
Administre, vea y modifique las reglas NAT del filtro IP.	Elimina un conjunto de reglas inactivo del núcleo.	“Cómo eliminar un conjunto de reglas de filtros de paquetes inactivo del núcleo” en la página 673
	Visualiza las reglas NAT activas.	“Gestión de reglas NAT para filtro IP” en la página 674
	Elimina las reglas NAT.	“Cómo eliminar reglas NAT” en la página 675
	Agrega las reglas adicionales a las reglas NAT.	“Como anexar reglas a las reglas NAT” en la página 675
Administre, vea y modifique las agrupaciones de direcciones del filtro IP.		“Gestión de agrupaciones de direcciones para el filtro IP” en la página 676
	Visualiza las agrupaciones de direcciones activas.	“Cómo ver las agrupaciones de direcciones activas” en la página 676
	Elimina una agrupación de direcciones.	“Cómo eliminar una agrupación de direcciones” en la página 677
	Agrega reglas adicionales a una agrupación de direcciones.	“Cómo anexar reglas a una agrupación de direcciones” en la página 677

Gestión de conjunto de reglas de filtro de paquetes para filtro IP

Cuando está habilitado, tanto los conjuntos de reglas de filtros de paquetes activos como los inactivos pueden residir en el núcleo. El conjunto de reglas activo determina el filtro que se está aplicando en los paquetes entrantes y salientes. El conjunto de reglas inactivo también guarda las reglas. Estas reglas no se utilizan a menos que convierta el conjunto de reglas inactivo en el conjunto activo. Puede administrar, ver y modificar los conjuntos de reglas de filtros de paquetes activos e inactivos.

▼ **Cómo visualizar el conjunto de reglas de filtros de paquetes activo**

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Visualice el conjunto de reglas de filtros de paquetes activo que se ha cargado en el núcleo.**

```
# ipfstat -io
```

Ejemplo 26–2 Visualización del conjunto de reglas de filtros de paquetes activo

En el ejemplo siguiente se muestra el resultado del conjunto de reglas de filtros de paquetes activo que está cargado en el núcleo.

```
# ipfstat -io
empty list for ipfilter(out)
pass in quick on dmfe1 from 192.168.1.0/24 to any
pass in all
block in on dmfe1 from 192.168.1.10/32 to any
```

▼ **Cómo visualizar el conjunto de reglas de filtros de paquetes inactivo**

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Visualice el conjunto de reglas de filtros de paquetes inactivo.**

```
# ipfstat -I -io
```

Ejemplo 26–3 Visualización del conjunto de reglas de filtros de paquetes inactivo

El ejemplo siguiente muestra el resultado del conjunto de reglas de filtros de paquetes inactivo.

```
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
```

▼ **Cómo activar un conjunto de reglas de filtros de paquetes diferente o actualizado**

Siga este procedimiento para llevar a cabo una de las tareas siguientes:

- Active un conjunto de reglas de filtros de paquetes que no sea el que está utilizando el filtro IP.
- Vuelva a cargar el mismo conjunto de reglas de filtros que se ha actualizado.

1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

2 Elija uno de estos pasos:

- Cree un conjunto de reglas en un archivo diferente si desea activar un conjunto de reglas completamente distinto.
- Actualice el conjunto de reglas actual editando el archivo de configuración que lo contiene.

3 Elimine el conjunto de reglas actual y cargue el nuevo.

```
# ipf -Fa -f filename
```

El *nombre_archivo* puede ser el nuevo archivo con el nuevo conjunto de reglas o el archivo actualizado que contenga el conjunto de reglas activo.

El conjunto de reglas activo se elimina del núcleo. Las reglas del archivo *nombre_archivo* pasan a ser el conjunto de reglas activo.

Nota – Es preciso ejecutar el comando aunque esté volviendo a cargar el archivo de configuración actual. De lo contrario, el antiguo conjunto de reglas seguirá funcionando, y no se aplicará el conjunto de reglas modificado en el archivo de configuración actualizado.

No utilice comandos como `ipf -D` o `svcadm restart` para cargar el conjunto de reglas actualizado. Dichos comandos ponen en peligro la red al desactivar el cortafuegos antes de cargar el nuevo conjunto de reglas.

Ejemplo 26–4 Activación de un conjunto de reglas de filtros de paquetes diferente

El ejemplo siguiente muestra cómo reemplazar un conjunto de reglas de filtros de paquetes por otro en un archivo de configuración distinto, `/etc/ipf/ipf.conf`.

```
# ipfstat -io
empty list for ipfilter(out)
pass in quick on dmfe all
# ipf -Fa -f /etc/ipf/ipf.conf
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
```

Ejemplo 26-5 Cómo volver a cargar un conjunto de reglas de filtros de paquetes actualizado

El ejemplo siguiente muestra cómo volver a cargar un conjunto de reglas de filtros de paquetes activo y luego actualizarlo. En este ejemplo, el archivo en uso es `/etc/ipf/ipf.conf`.

```
# ipfstat -io (Optional)
empty list for ipfilter (out)
block in log quick from 10.0.0.0/8 to any

(Edit the /etc/ipf/ipf.conf configuration file.)

# ipf -Fa -f /etc/ipf/ipf.conf
# ipfstat -io (Optional)
empty list for ipfilter (out)
block in log quick from 10.0.0.0/8 to any
block in quick on elx10 from 192.168.0.0/12 to any
```

▼ Cómo eliminar un conjunto de reglas de filtros de paquetes

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Elimine el conjunto de reglas.**

```
# ipf -F [a|i|o]

-a    Elimina todas las reglas de filtros del conjunto de reglas.
-i    Elimina las reglas de filtros de los paquetes entrantes.
-o    Elimina las reglas de filtros de los paquetes salientes.
```

Ejemplo 26-6 Eliminación de un conjunto de reglas de filtros de paquetes

El ejemplo siguiente muestra cómo eliminar todas las reglas de filtros del conjunto de reglas de filtros activo.

```
# ipfstat -io
block out log on dmfc0 all
block in log quick from 10.0.0.0/8 to any
# ipf -Fa
# ipfstat -io
empty list for ipfilter(out)
empty list for ipfilter(in)
```

▼ Cómo anexar reglas al conjunto de reglas de filtros de paquetes activo

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Utilice uno de los métodos siguientes para anexar reglas al conjunto de reglas activo:**

- **Anexe reglas al conjunto de reglas en la línea de comandos con el comando `ipf -f -`.**

```
# echo "block in on dmfe1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
```

- **Ejecute los comandos siguientes:**

- a. Cree un conjunto de reglas en el archivo que desee.
- b. Agregue las reglas que ha creado al conjunto de reglas activo.

```
# ipf -f filename
```

Las reglas de *nombre de archivo* se agregan al final del conjunto de reglas activo. Dado que el filtro IP utiliza un algoritmo de "última regla coincidente", las reglas que agregue determinan las prioridades de los filtros, a menos que utilice la palabra clave `quick`. Si el paquete coincide con una regla que contiene la palabra clave `quick`, se lleva a cabo la acción de dicha regla y no se comprueban las reglas subsiguientes.

Ejemplo 26-7 Cómo anexar reglas al conjunto de reglas de filtros de paquetes activo

El ejemplo siguiente muestra cómo agregar una regla al conjunto de reglas de filtros de paquetes activo desde la línea de comandos.

```
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
# echo "block in on dmfe1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
```

▼ Cómo anexar reglas al conjunto de reglas de filtros de paquetes inactivo

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Cree un conjunto de reglas en el archivo que desee.**

- 3 **Agregue las reglas que ha creado al conjunto de reglas inactivo.**

```
# ipf -I -f filename
```

Las reglas de *nombre_archivo* se agregan al final del conjunto de reglas inactivo. Dado que el filtro IP utiliza un algoritmo de "última regla coincidente", las reglas que agregue determinan las prioridades de los filtros, a menos que utilice la palabra clave *quick*. Si el paquete coincide con una regla que contiene la palabra clave *quick*, se lleva a cabo la acción de dicha regla y no se comprueban las reglas subsiguientes.

Ejemplo 26–8 Cómo anexar reglas al conjunto de reglas inactivo

El ejemplo siguiente muestra cómo agregar una regla al conjunto de reglas inactivo desde un archivo.

```
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
# ipf -I -f /etc/ipf/ipf.conf
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
```

▼ Cómo alternar entre los conjuntos de reglas de filtros de paquetes activo e inactivo

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Alterne los conjuntos de reglas activo e inactivo.

```
# ipf -s
```

Este comando permite alternar entre los conjuntos de reglas activo e inactivo del núcleo. Si el conjunto de reglas inactivo está vacío, no se aplicará ningún filtro de paquetes.

Ejemplo 26-9 Cómo alternar entre los conjuntos de reglas de filtros de paquetes activo e inactivo

El ejemplo siguiente muestra cómo el uso del comando `ipf -s` convierte el conjunto de reglas inactivo en el conjunto activo y viceversa.

- Antes de ejecutar el comando `ipf -s`, el resultado del comando `ipfstat -I -io` muestra las reglas en el conjunto de reglas inactivo. El resultado del comando `ipfstat -io` muestra las reglas en el conjunto de reglas activo.

```
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
```

- Después de ejecutar el comando `ipf -s`, el resultado de los comandos `ipfstat -I -io` y `ipfstat -io` muestra que el contenido de los dos conjuntos de reglas ha cambiado.

```
# ipf -s
Set 1 now inactive
# ipfstat -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
# ipfstat -I -io
empty list for inactive ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
```

▼ Cómo eliminar un conjunto de reglas de filtros de paquetes inactivo del núcleo

1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Especifique el conjunto de reglas inactivo en el comando "flush all".

```
# ipf -I -Fa
```

Este comando vacía el conjunto de reglas inactivo del núcleo.

Nota – Si ejecuta posteriormente `ipf -s`, el conjunto de reglas inactivo vacío se convertirá en el conjunto de reglas activo. Un conjunto de reglas activo vacío implica que *no* se aplicará ningún filtro.

Ejemplo 26–10 Cómo eliminar un conjunto de reglas de filtros de paquetes inactivo del núcleo

El ejemplo siguiente muestra cómo vaciar el conjunto de reglas de filtros de paquetes inactivo para eliminar todas las reglas.

```
# ipfstat -I -io
empty list for inactive ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
# ipf -I -Fa
# ipfstat -I -io
empty list for inactive ipfilter(out)
empty list for inactive ipfilter(in)
```

Gestión de reglas NAT para filtro IP

Utilice el procedimiento siguiente para administrar, ver y modificar las reglas NAT.

▼ **Cómo ver las reglas NAT activas**

- 1** Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2** Visualice las reglas NAT activas.

```
# ipnat -l
```

Ejemplo 26–11 Visualización de las reglas NAT activas

El ejemplo siguiente muestra el resultado del conjunto de reglas NAT activo.

```
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32
```

List of active sessions:

▼ Cómo eliminar reglas NAT

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Elimine las reglas NAT actuales.**

```
# ipnat -C
```

Ejemplo 26–12 Eliminación de reglas NAT

Con el ejemplo siguiente aprenderá a eliminar las entradas de las reglas NAT actuales.

```
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
# ipnat -C
1 entries flushed from NAT list
# ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
```

▼ Como anexar reglas a las reglas NAT

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Utilice uno de los métodos siguientes para anexar reglas al conjunto de reglas activo:**

- Anexe reglas al conjunto de reglas NAT en la línea de comandos con el comando `ipnat -f -`.


```
# echo "map dmfe0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
```
- Ejecute los comandos siguientes:

- a. Cree reglas NAT adicionales en el archivo que desee.
- b. Agregue las reglas que ha creado al conjunto de reglas NAT activo.

```
# ipnat -f filename
```

Las reglas de *nombre_archivo* se agregan al final de las reglas NAT.

Ejemplo 26–13 Cómo anexar reglas al conjunto de reglas NAT

El ejemplo siguiente muestra cómo agregar una regla al conjunto de reglas NAT desde la línea de comandos.

```
# ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
# echo "map dmfe0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

Gestión de agrupaciones de direcciones para el filtro IP

Utilice los procedimientos siguientes para gestionar, ver y modificar las agrupaciones de direcciones.

▼ Cómo ver las agrupaciones de direcciones activas

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Visualice la agrupación de direcciones activa.**

```
# ippool -l
```

Ejemplo 26–14 Visualización de la agrupación de direcciones activa

El ejemplo siguiente muestra cómo visualizar el contenido de la agrupación de direcciones activa.

```
# ippool -l
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

▼ Cómo eliminar una agrupación de direcciones

- 1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 Elimine las entradas de la agrupación de direcciones actual.

```
# ippool -F
```

Ejemplo 26–15 Cómo eliminar una agrupación de direcciones

El ejemplo siguiente muestra cómo eliminar una agrupación de direcciones.

```
# ippool -l
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
# ippool -F
1 object flushed
# ippool -l
```

▼ Cómo anexar reglas a una agrupación de direcciones

- 1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 Utilice uno de los métodos siguientes para anexar reglas al conjunto de reglas activo:

- Anexe reglas al conjunto de reglas en la línea de comandos utilizando el comando `ippool -f -`.

```
# echo "table role = ipf type = tree number = 13
{10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24};" | ippool -f -
```

- Ejecute los comandos siguientes:
 - a. Cree agrupaciones de direcciones adicionales en el archivo que desee.
 - b. Agregue las reglas que ha creado al conjunto de direcciones activo.

```
# ippool -f filename
```

Las reglas de *nombre_archivo* se agregan al final de la agrupación de direcciones activa.

Ejemplo 26–16 Cómo anexar reglas a una agrupación de direcciones

El ejemplo siguiente muestra cómo agregar una agrupación de direcciones al conjunto de reglas de la agrupación de direcciones desde la línea de comandos.

```
# ippool -l
table role = ipf type = tree number = 13
    { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
# echo "table role = ipf type = tree number = 100
    {10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24};" | ippool -f -
# ippool -l
table role = ipf type = tree number = 100
    { 10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24; };
table role = ipf type = tree number = 13
    { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

Cómo visualizar las estadísticas e información sobre el filtro IP

TABLA 26–5 Cómo visualizar las estadísticas e información sobre el filtro IP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Ver las tablas de estado.	Visualiza las tablas de estado para obtener información sobre los filtros de paquetes con el comando ipfstat.	“Cómo ver las tablas de estado para el filtro IP” en la página 679
Ver las estadísticas de estado.	Visualiza las estadísticas sobre el estado de los paquetes utilizando el comando ipfstat -s.	“Cómo ver las tablas de estado para el filtro IP” en la página 679
Ver las estadísticas de NAT.	Visualiza las estadísticas de NAT utilizando el comando ipnat -s.	“Cómo visualizar las estadísticas de NAT para el filtro IP” en la página 680
Ver las estadísticas de la agrupación de direcciones.	Visualiza las estadísticas de la agrupación de direcciones utilizando el comando ippool -s.	“Cómo visualizar las estadísticas de la agrupación de direcciones para el filtro IP” en la página 681

▼ Cómo ver las tablas de estado para el filtro IP

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Visualice la tabla de estado.**

```
# ipfstat
```

Nota – Puede utilizar la opción -t para ver la tabla de estado en el formato de la utilidad.

Ejemplo 26–17 Visualización de tablas de estado para el filtro IP

El ejemplo siguiente muestra cómo visualizar una tabla de estado.

```
# ipfstat
bad packets:           in 0      out 0
  input packets:       blocked 160 passed 11 nomatch 1 counted 0 short 0
output packets:       blocked 0 passed 13681 nomatch 6844 counted 0 short 0
  input packets logged: blocked 0 passed 0
output packets logged: blocked 0 passed 0
  packets logged:      input 0 output 0
  log failures:        input 0 output 0
fragment state(in):   kept 0 lost 0
fragment state(out):  kept 0 lost 0
packet state(in):     kept 0 lost 0
packet state(out):    kept 0 lost 0
ICMP replies: 0      TCP RSTs sent: 0
Invalid source(in):   0
Result cache hits(in): 152      (out): 6837
IN Pullups succeeded: 0      failed: 0
OUT Pullups succeeded: 0      failed: 0
Fastroute successes: 0      failures: 0
TCP cksum fails(in): 0      (out): 0
IPF Ticks:           14341469
Packet log flags set: (0)
                     none
```

▼ Cómo ver las tablas de estado para el filtro IP

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Visualice las estadísticas de estado.

```
# ipfstat -s
```

Ejemplo 26–18 Visualización de las estadísticas de estado para el filtro IP

El ejemplo siguiente muestra cómo visualizar las estadísticas de estado.

```
# ipfstat -s
IP states added:
    0 TCP
    0 UDP
    0 ICMP
    0 hits
    0 misses
    0 maximum
    0 no memory
    0 max bucket
    0 active
    0 expired
    0 closed
State logging enabled

State table bucket statistics:
    0 in use
    0.00% bucket usage
    0 minimal length
    0 maximal length
    0.000 average length
```

▼ Cómo visualizar las estadísticas de NAT para el filtro IP

1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Visualice las estadísticas de NAT.

```
# ipnat -s
```

Ejemplo 26–19 Visualización de estadísticas de NAT para el filtro IP

El ejemplo siguiente muestra cómo visualizar las estadísticas de NAT.

```
# ipnat -s
mapped in      0      out      0
added  0      expired 0
no memory      0      bad nat 0
```



```
inuse    0
rules    1
wilds    0
```

▼ **Cómo visualizar las estadísticas de la agrupación de direcciones para el filtro IP**

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**
Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 **Ver las estadísticas de la agrupación de direcciones.**

```
# ippool -s
```

Ejemplo 26–20 Visualización de las estadísticas de la agrupación de direcciones para el filtro IP

El ejemplo siguiente muestra cómo visualizar las estadísticas de la agrupación de direcciones.

```
# ippool -s
Pools:    3
Hash Tables:    0
Nodes:    0
```

Cómo trabajar con archivos de registro para el filtro IP

TABLA 26–6 Cómo trabajar con archivos de registro para el filtro IP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Crear un archivo de registro.	Crear un archivo de registro del filtro IP independiente.	“Cómo configurar un archivo de registro para el filtro IP” en la página 682
Visualizar archivos de registro.	Visualizar el estado, la NAT y los archivos de registro normales utilizando el comando <code>ipmon</code> .	“Cómo visualizar los archivos de registro del filtro IP” en la página 683
Vaciar el búfer de registro de paquetes.	Eliminar el contenido del búfer de registro de paquetes utilizando el comando <code>ipmon - F</code> .	“Cómo vaciar el archivo de registro de paquetes” en la página 684

TABLA 26-6 Cómo trabajar con archivos de registro para el filtro IP (mapa de tareas) <i>(Continuación)</i>		
Tarea	Descripción	Para obtener instrucciones
Guardar los paquetes registrados en un archivo.	Guardar los paquetes registrados en un archivo para poder consultarlos posteriormente.	“Cómo guardar paquetes registrados en un archivo” en la página 684

▼ Cómo configurar un archivo de registro para el filtro IP

De modo predeterminado, toda la información de registro del filtro IP se guarda en el archivo `syslogd`. Debe configurar un archivo de registro para que guarde la información de tráfico del filtro IP de forma independiente de los demás datos que se puedan registrar en el archivo predeterminado. Realice los siguientes pasos.

- 1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**
Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 Edite el archivo `/etc/syslog.conf` agregando las dos líneas siguientes:**

```
# Save IPFilter log output to its own file
local0.debug      /var/log/log-name
```

Nota – En la segunda línea, asegúrese de utilizar la tecla de tabulación y no la barra espaciadora para separar `local0.debug` de `/var/log/nombre_registro`.

- 3 Cree el nuevo archivo de registro.**
`# touch /var/log/log-name`
- 4 Reinicie el servicio de registro del sistema.**
`# svcadm restart system-log`

Ejemplo 26-21 Creación de un registro del filtro IP

En el ejemplo siguiente se muestra cómo crear `ipmon.log` para archivar información de filtro de IP.

En `/etc/syslog.conf`:

```
# Save IPFilter log output to its own file
local0.debug      /var/log/ipmon.log
```

En la línea de comandos:

```
# touch /var/log/ipmon.log
# svcadm restart system-log
```

▼ Cómo visualizar los archivos de registro del filtro IP

Antes de empezar Debe crear un archivo de registro independiente para guardar los datos del filtro IP. Consulte “[Cómo configurar un archivo de registro para el filtro IP](#)” en la [página 682](#).

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Visualice el estado, la NAT o los archivos de registro normales. Para ver un archivo de registro, escriba el comando siguiente con la opción adecuada:**

```
# ipmon -o [S|N|I] filename
```

S Muestra el archivo de registro de estado.

N Muestra al archivo de registro de NAT.

I Muestra el archivo de registro de IP normal.

Para ver todos los archivos de estado, NAT y registro normal, utilice todas las opciones:

```
# ipmon -o SNI filename
```

- Si ha detenido manualmente el daemon `ipmon` en primer lugar, también puede utilizar el siguiente comando para ver los archivos de registro de estado, NAT y filtro IP:

```
# ipmon -a filename
```

Nota – No utilice la sintaxis `ipmon -a` si el daemon `ipmon` sigue ejecutándose. Normalmente, el daemon se inicia automáticamente durante el inicio del sistema. Al ejecutar el comando `ipmon -a` también se abre otra copia de `ipmon`. En tal caso, ambas copias leen el mismo registro, y sólo una obtiene un mensaje de registro específico.

Si desea más información sobre cómo visualizar archivos de registro, consulte la página del comando `man ipmon(1M)`.

Ejemplo 26–22 Visualización de archivos de registro del filtro IP

El ejemplo siguiente muestra el resultado de `/var/ipmon.log`.

```
# ipmon -o SNI /var/ipmon.log
02/09/2004 15:27:20.606626 hme0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

O

```
# pkill ipmon
# ipmon -aD /var/ipmon.log
02/09/2004 15:27:20.606626 hme0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

▼ Cómo vaciar el archivo de registro de paquetes

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Vacíe el búfer de registro de paquetes.**

```
# ipmon -F
```

Ejemplo 26–23 Vaciado del archivo de registro de paquetes

El siguiente ejemplo muestra el resultado cuando se elimina un archivo de registro. El sistema crea un informe incluso cuando no hay nada en el archivo de registro, como es el caso de este ejemplo.

```
# ipmon -F
0 bytes flushed from log buffer
0 bytes flushed from log buffer
0 bytes flushed from log buffer
```

▼ Cómo guardar paquetes registrados en un archivo

- 1 **Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.**

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Guarde los paquetes registrados en un archivo.

```
# cat /dev/ipl > filename
```

Siga registrando paquetes en el archivo *nombre_archivo* hasta interrumpir el procedimiento escribiendo `Ctrl-C` para que vuelva a aparecer la línea de comandos.

Ejemplo 26–24 Cómo guardar los paquetes registrados en un archivo

El ejemplo siguiente muestra el resultado que se obtiene al guardar paquetes registrados en un archivo.

```
# cat /dev/ipl > /tmp/logfile
^C#

# ipmon -f /tmp/logfile
02/09/2004 15:30:28.708294 hme0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 52 -S IN
02/09/2004 15:30:28.708708 hme0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.792611 hme0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 70 -AP IN
02/09/2004 15:30:28.872000 hme0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872142 hme0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 43 -AP IN
02/09/2004 15:30:28.872808 hme0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872951 hme0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 47 -AP IN
02/09/2004 15:30:28.926792 hme0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 40 -A IN
.
.
(output truncated)
```

Creación y edición de archivos de configuración del filtro IP

Debe editar directamente los archivos de configuración para crear y modificar conjuntos de reglas y agrupaciones de direcciones. Los archivos de configuración siguen reglas de sintaxis de UNIX estándar:

- El signo `#` indica que una línea contiene comentarios.
- Los comentarios y las reglas pueden coexistir en la misma línea.
- También se permite agregar espacios en blanco para facilitar la lectura de las reglas.
- Las reglas pueden ocupar más de una línea. Utilice la barra inclinada inversa (`\`) al final de una línea para indicar que la regla continúa en la línea siguiente.

▼ Cómo crear un archivo de configuración para el filtro IP

El procedimiento siguiente describe cómo configurar:

- Los archivos de configuración de filtros de paquetes
- Los archivos de configuración de reglas NAT
- Los archivos de configuración de agrupaciones de direcciones

1 Asuma un rol que incluya el perfil con derechos de administración del filtro IP, o conviértase en superusuario.

Puede asignar el perfil con derechos de administración del filtro IP a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 Inicie el editor de archivos que prefiera. Cree o edite el archivo de configuración para la función que desee configurar.

- Para crear un archivo de configuración para las reglas de filtros de paquetes, edite el archivo `ipf.conf`.

El filtro IP utiliza las reglas de filtros de paquetes que se colocan en el archivo `ipf.conf`. Si coloca las reglas para los filtros de paquetes en el archivo `/etc/ipf/ipf.conf`, dicho archivo se carga al iniciar el sistema. Si no desea que las reglas de filtros se carguen durante el inicio, colóquelas en el archivo que prefiera. A continuación, puede activar las reglas con el comando `ipf`, tal como se describe en [“Cómo activar un conjunto de reglas de filtros de paquetes diferente o actualizado” en la página 668](#).

Consulte [“Uso de la función de filtros de paquetes del filtro IP” en la página 643](#) para obtener información sobre cómo crear reglas de filtros de paquetes.

Nota – Si el archivo `ipf.conf` está vacío, no se aplica ningún filtro. Un archivo `ipf.conf` vacío equivale a tener un conjunto de reglas como el siguiente:

```
pass in all
pass out all
```

- Para crear un archivo de configuración para las reglas NAT, edite el archivo `ipnat.conf`.

El filtro IP utiliza las reglas NAT que se colocan en el archivo `ipnat.conf`. Si coloca las reglas para NAT en el archivo `/etc/ipf/ipnat.conf`, dicho archivo se carga al iniciar el sistema. Si no desea que las reglas NAT se carguen durante el inicio, coloque el archivo `ipnat.conf` en la ubicación que prefiera. A continuación, puede activar las reglas NAT con el comando `ipnat`.

Consulte “Uso de la función NAT del filtro IP” en la página 646 para obtener información sobre cómo crear reglas para la NAT.

- Para crear un archivo de configuración para las agrupaciones de direcciones, edite el archivo `ippool.conf`.

El filtro IP utiliza la agrupación de direcciones que se coloca en el archivo `ippool.conf`. Si coloca las reglas para la agrupación de direcciones en el archivo `/etc/ipf/ippool.conf`, dicho archivo se carga al iniciar el sistema. Si no desea que la agrupación de direcciones se cargue durante el inicio, coloque el archivo `ippool.conf` en la ubicación que prefiera. A continuación, puede activar la agrupación de direcciones con el comando `ippool`.

Consulte “Uso de la función de agrupaciones de direcciones del filtro IP” en la página 647 para obtener información sobre la creación de agrupaciones de direcciones.

Ejemplos de archivos de configuración del filtro IP

Los ejemplos siguientes ilustran las reglas de filtros de paquetes que se utilizan en las configuraciones de filtros.

EJEMPLO 26–25 Configuración de host del filtro IP

Este ejemplo muestra una configuración en un equipo host con una interfaz `elxl`.

```
# pass and log everything by default
pass in log on bge0 all
pass out log on bge0 all

# block, but don't log, incoming packets from other reserved addresses
block in quick on bge0 from 10.0.0.0/8 to any
block in quick on bge0 from 172.16.0.0/12 to any

# block and log untrusted internal IPs. 0/32 is notation that replaces
# address of the machine running Solaris IP Filter.
block in log quick from 192.168.1.15 to <thishost>
block in log quick from 192.168.1.43 to <thishost>

# block and log X11 (port 6000) and remote procedure call
# and portmapper (port 111) attempts
block in log quick on bge0 proto tcp from any to bge0/32 port = 6000 keep state
block in log quick on bge0 proto tcp/udp from any to bge0/32 port = 111 keep state
```

Este conjunto de reglas comienza con dos reglas sin restricciones que permiten la transferencia de todos los datos con la interfaz `elxl`. El segundo conjunto de reglas bloquea todos los paquetes entrantes de los espacios de direcciones privadas `10.0.0.0` y `172.16.0.0` mediante el cortafuegos. El siguiente conjunto de reglas bloquea direcciones internas específicas del equipo host. Finalmente, el último conjunto de reglas bloquea los paquetes que provienen de los puertos `6000` y `111`.

EJEMPLO 26-26 Configuración del servidor del filtro IP

Este ejemplo muestra una configuración para un equipo host que actúa como servidor Web. Este equipo cuenta con una interfaz de red eri.

```
# web server with an eri interface
# block and log everything by default; then allow specific services
# group 100 - inbound rules
# group 200 - outbound rules
# (0/32) resolves to our IP address)
*** FTP proxy ***

# block short packets which are packets fragmented too short to be real.
block in log quick all with short

# block and log inbound and outbound by default, group by destination
block in log on eri0 from any to any head 100
block out log on eri0 from any to any head 200

# web rules that get hit most often
pass in quick on eri0 proto tcp from any \
to eri0/32 port = http flags S keep state group 100
pass in quick on eri0 proto tcp from any \
to eri0/32 port = https flags S keep state group 100

# inbound traffic - ssh, auth
pass in quick on eri0 proto tcp from any \
to eri0/32 port = 22 flags S keep state group 100
pass in log quick on eri0 proto tcp from any \
to eri0/32 port = 113 flags S keep state group 100
pass in log quick on eri0 proto tcp from any port = 113 \
to eri0/32 flags S keep state group 100

# outbound traffic - DNS, auth, NTP, ssh, WWW, smtp
pass out quick on eri0 proto tcp/udp from eri0/32 \
to any port = domain flags S keep state group 200
pass in quick on eri0 proto udp from any port = domain to eri0/32 group 100

pass out quick on eri0 proto tcp from eri0/32 \
to any port = 113 flags S keep state group 200
pass out quick on eri0 proto tcp from eri0/32 port = 113 \
to any flags S keep state group 200

pass out quick on eri0 proto udp from eri0/32 to any port = ntp group 200
pass in quick on eri0 proto udp from any port = ntp to eri0/32 port = ntp group 100

pass out quick on eri0 proto tcp from eri0/32 \
to any port = ssh flags S keep state group 200

pass out quick on eri0 proto tcp from eri0/32 \
to any port = http flags S keep state group 200
pass out quick on eri0 proto tcp from eri0/32 \
```


EJEMPLO 26-26 Configuración del servidor del filtro IP (Continuación)

```

to any port = https flags S keep state group 200

pass out quick on eri0 proto tcp from eri0/32 \
to any port = smtp flags S keep state group 200

# pass icmp packets in and out
pass in quick on eri0 proto icmp from any to eri0/32 keep state group 100
pass out quick on eri0 proto icmp from eri0/32 to any keep state group 200

# block and ignore NETBIOS packets
block in quick on eri0 proto tcp from any \
to any port = 135 flags S keep state group 100

block in quick on eri0 proto tcp from any port = 137 \
to any flags S keep state group 100
block in quick on eri0 proto udp from any to any port = 137 group 100
block in quick on eri0 proto udp from any port = 137 to any group 100

block in quick on eri0 proto tcp from any port = 138 \
to any flags S keep state group 100
block in quick on eri0 proto udp from any port = 138 to any group 100

block in quick on eri0 proto tcp from any port = 139 to any flags S keep state
group 100
block in quick on eri0 proto udp from any port = 139 to any group 100

```

EJEMPLO 26-27 Configuración del enrutador del filtro IP

El ejemplo siguiente muestra una configuración para un enrutador con una interfaz interna (ce0) y otra externa (ce1).

```

# internal interface is ce0 at 192.168.1.1
# external interface is ce1 IP obtained via DHCP
# block all packets and allow specific services
*** NAT ***
*** POOLS ***

# Short packets which are fragmented too short to be real.
block in log quick all with short

# By default, block and log everything.
block in log on ce0 all
block in log on ce1 all
block out log on ce0 all
block out log on ce1 all

# Packets going in/out of network interfaces that aren't on the loopback
# interface should not exist.
block in log quick on ce0 from 127.0.0.0/8 to any

```

EJEMPLO 26-27 Configuración del enrutador del filtro IP *(Continuación)*

```
block in log quick on ce0 from any to 127.0.0.0/8
block in log quick on ce1 from 127.0.0.0/8 to any
block in log quick on ce1 from any to 127.0.0.0/8

# Deny reserved addresses.
block in quick on ce1 from 10.0.0.0/8 to any
block in quick on ce1 from 172.16.0.0/12 to any
block in log quick on ce1 from 192.168.1.0/24 to any
block in quick on ce1 from 192.168.0.0/16 to any

# Allow internal traffic
pass in quick on ce0 from 192.168.1.0/24 to 192.168.1.0/24
pass out quick on ce0 from 192.168.1.0/24 to 192.168.1.0/24

# Allow outgoing DNS requests from our servers on .1, .2, and .3
pass out quick on ce1 proto tcp/udp from ce1/32 to any port = domain keep state
pass in quick on ce0 proto tcp/udp from 192.168.1.2 to any port = domain keep state
pass in quick on ce0 proto tcp/udp from 192.168.1.3 to any port = domain keep state

# Allow NTP from any internal hosts to any external NTP server.
pass in quick on ce0 proto udp from 192.168.1.0/24 to any port = 123 keep state
pass out quick on ce1 proto udp from any to any port = 123 keep state

# Allow incoming mail
pass in quick on ce1 proto tcp from any to ce1/32 port = smtp keep state
pass in quick on ce1 proto tcp from any to ce1/32 port = smtp keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = smtp keep state

# Allow outgoing connections: SSH, WWW, NNTP, mail, whois
pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 22 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 22 keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 443 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 443 keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = nntp keep state
block in quick on ce1 proto tcp from any to any port = nntp keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = nntp keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = smtp keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = whois keep state
pass out quick on ce1 proto tcp from any to any port = whois keep state

# Allow ssh from offsite
pass in quick on ce1 proto tcp from any to ce1/32 port = 22 keep state
```

EJEMPLO 26-27 Configuración del enrutador del filtro IP (Continuación)

```
# Allow ping out
pass in quick on ce0 proto icmp all keep state
pass out quick on ce1 proto icmp all keep state

# allow auth out
pass out quick on ce1 proto tcp from ce1/32 to any port = 113 keep state
pass out quick on ce1 proto tcp from ce1/32 port = 113 to any keep state

# return rst for incoming auth
block return-rst in quick on ce1 proto tcp from any to any port = 113 flags S/SA

# log and return reset for any TCP packets with S/SA
block return-rst in log on ce1 proto tcp from any to any flags S/SA

# return ICMP error packets for invalid UDP packets
block return-icmp(net-unr) in proto udp all
```


P A R T E V

IP móvil

En esta parte se presenta el Protocolo de Internet móvil (IP móvil) y se indican las tareas de administración de IP móvil. Puede instalar IP móvil en sistemas como equipos portátiles y sistemas con comunicación inalámbrica para que puedan operar en redes externas.

Nota – La función IP móvil se ha suprimido de las actualizaciones de Oracle Solaris 10 posteriores a Solaris 10 8/07.

IP para móviles (Descripción general)

El protocolo de Internet (IP) para móviles permite transferir información entre sistemas móviles. El concepto *sistemas móviles* incluye portátiles y comunicaciones inalámbricas. El sistema móvil puede cambiar su ubicación a una red externa. Mientras está en la red externa, el sistema móvil se sigue pudiendo comunicar con la red principal del sistema. La implementación Solaris del IP móvil sólo es compatible con IPv4.

Este capítulo contiene la información siguiente:

- “Introducción a IP para móviles” en la página 696
- “Entidades funcionales de IP para móviles” en la página 698
- “Funcionamiento de IP para móviles” en la página 698
- “Descubrimiento de agentes” en la página 701
- “Direcciones de auxilio” en la página 702
- “IP para móviles con túnel inverso” en la página 703
- “Registro de IP para móviles” en la página 705
- “Encaminamiento de datagramas entre nodos móviles” en la página 709
- “Consideraciones de seguridad para IP para móviles” en la página 711

Para tareas relacionadas con IP para móviles, consulte el [Capítulo 28, “Administración de IP móvil \(tareas\)”](#). Para acceder a material de referencia de IP para móviles, consulte el [Capítulo 29, “Archivos y comandos de IP para móviles \(referencia\)”](#).

Novedades de IP para móviles

La función IP móvil se suprime de las actualizaciones de Solaris 10 posteriores a Solaris 10 8/07.

Introducción a IP para móviles

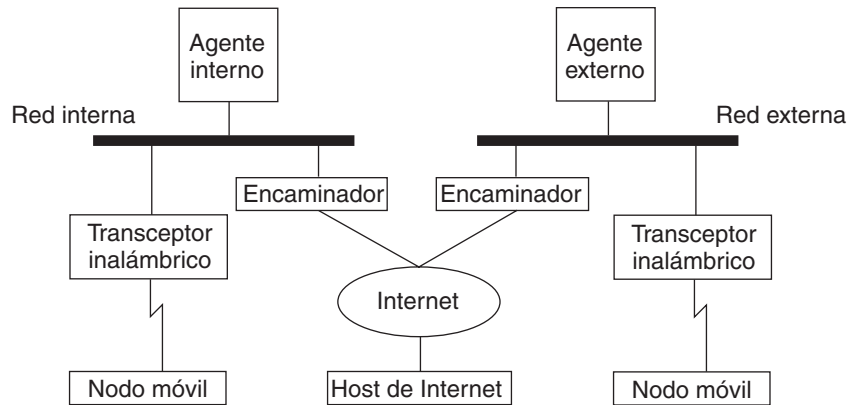
Las versiones actuales del protocolo de Internet (IP) dan por supuesto que el punto en el que un sistema se conecta a Internet o a una red es fijo. IP asume también que la dirección IP del sistema identifica la red a la que este está conectado. Los datagramas que se envían a un sistema se basan en la información de ubicación contenida en la dirección IP. Muchos protocolos de Internet exigen que la dirección IP de un nodo no cambie. Si alguno de estos protocolos está activado en un sistema con IP móvil, sus aplicaciones no funcionarán. Ni siquiera HTTP funcionaría si no fuese porque la vida de sus conexiones TCP es muy breve. En ese caso, actualizar una dirección IP y renovar la página web no supone una carga.

Si un sistema móvil, o *nodo móvil*, se traslada a una nueva red y su dirección IP no cambia, la dirección del nodo no refleja el nuevo punto de conexión. En consecuencia, los protocolos de enrutamiento en vigor no pueden enrutar los datagramas correctamente al nodo móvil. Deberá reconfigurar el nodo móvil con una dirección IP distinta que represente la nueva ubicación. La asignación de una dirección IP distinta es una tarea farragosa. Por tanto, con el protocolo de Internet actual, si el nodo móvil se traslada sin cambiar su dirección, pierde el enrutamiento. Si el nodo móvil cambia de dirección, pierde las conexiones.

IP para móviles resuelve el problema permitiendo que el nodo móvil utilice dos direcciones IP. La primera es una *dirección permanente* fija. La segunda es una *dirección de auxilio* que cambia en cada nuevo punto de conexión. IP para móviles permite que un sistema se mueva libremente en Internet. También le permite moverse libremente en la red de una organización manteniendo la misma dirección permanente. En consecuencia, las comunicaciones no se interrumpen cuando el usuario cambia el punto de conexión del sistema. En vez de eso, la red se actualiza con la nueva ubicación del nodo móvil. Consulte el [Glosario](#) para ver definiciones de términos relacionados con IP para móviles.

En la figura siguiente se ilustra la topología general de IP para móviles.

FIGURA 27-1 Topología de IP para móviles



Si se utiliza la topología de IP para móviles de esta figura, la situación siguiente muestra cómo se mueve un datagrama de un punto a otro de la estructura de IP para móviles:

1. El host de Internet envía datagramas al nodo móvil a través de la dirección permanente del nodo (proceso de enrutamiento IP normal).
2. Si el nodo móvil se encuentra en su red principal, el datagrama se entrega al nodo a través del proceso IP normal. En caso contrario, es el agente interno el que recibe el datagrama.
3. Si el nodo móvil se encuentra en una red externa, el agente interno reenvía el datagrama al agente externo. El agente interno debe encapsular el datagrama en un datagrama exterior para que la dirección IP del agente externo aparezca en el encabezado IP externo.
4. El agente externo entrega el datagrama al nodo móvil.
5. Los datagramas del nodo móvil hacia el host de Internet se envían mediante los procedimientos de enrutamiento IP normales. Si el nodo móvil se encuentra en una red externa, los paquetes se entregan al agente externo. El agente externo reenvía el datagrama al host de Internet.
6. En situaciones en las que haya filtrado de entrada, la dirección de origen debe ser topológicamente correcta para la subred de la que procede el datagrama, o el enrutador no podrá reenviarlo. Si se da esta situación en enlaces entre el nodo móvil y el nodo de destino, el agente externo deberá ofrecer el servicio de túnel inverso. Así, el agente externo podrá entregar todos los datagramas que el nodo móvil envíe a su agente interno. El agente interno reenviará entonces el datagrama a través de la ruta que hubiese tomado si el nodo móvil residiese en la red principal. Este proceso garantiza la corrección de la dirección de origen para todos los enlaces que debe atravesar el datagrama.

En lo concerniente a las comunicaciones inalámbricas, la [Figura 27-1](#) ilustra el uso de transceptores inalámbricos para transmitir los datagramas al nodo de móviles. Asimismo, los datagramas entre el host de Internet y el nodo móvil utilizan la dirección permanente del nodo móvil. La dirección permanente se utiliza aunque el nodo móvil se encuentre en la red externa.

La dirección de auxilio se utiliza únicamente para la comunicación con agentes de movilidad.
La dirección de auxilio es invisible para el host de Internet.

Entidades funcionales de IP para móviles

IP para móviles presenta las siguientes entidades funcionales:

- **Nodo móvil (NM):** host o enrutador que cambia su punto de conexión de una red a otra al tiempo que conserva las comunicaciones existentes mediante el uso de su dirección IP permanente.
- **Agente interno (AI):** enrutador o servidor de la red principal de un nodo móvil. El enrutador intercepta los datagramas que van destinados al nodo móvil. A continuación el enrutador entrega los datagramas a través de la dirección de auxilio. El agente interno mantiene también información actualizada de la ubicación del nodo móvil.
- **Agente externo (AE):** enrutador o servidor ubicado en la red externa que visita el nodo móvil. Ofrece servicios de enrutamiento de host al nodo móvil. El agente externo puede proporcionar también una dirección de auxilio al nodo móvil mientras este esté registrado.

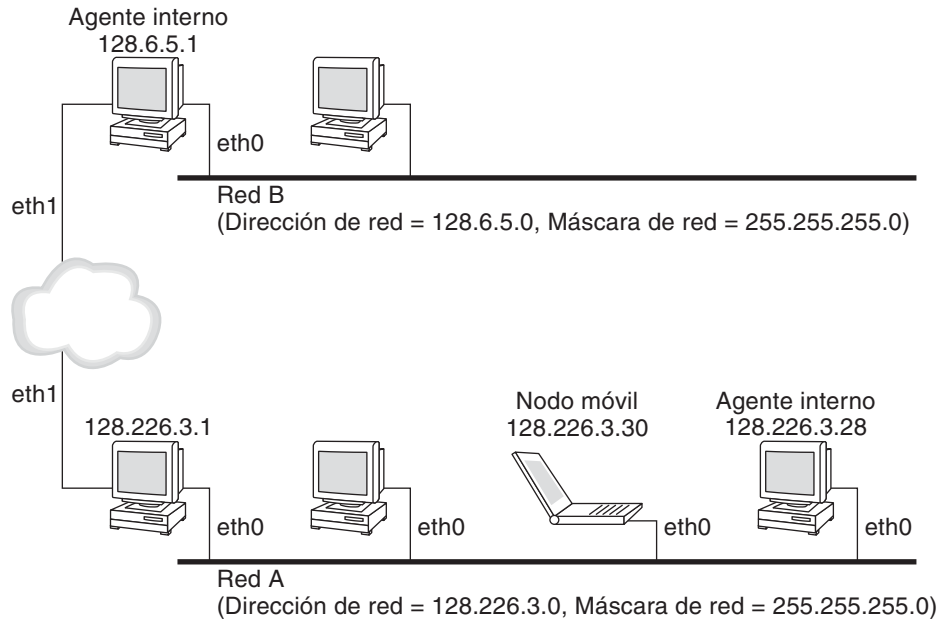
Funcionamiento de IP para móviles

IP para móviles permite enrutar los datagramas IP a nodos móviles. La dirección permanente del nodo móvil identifica siempre al nodo, independientemente del punto de conexión de este. Cuando el nodo no está en su lugar habitual, una dirección de auxilio se asocia con la dirección permanente del nodo móvil. La dirección de auxilio proporciona información acerca del actual punto de conexión del nodo móvil. IP para móviles utiliza un mecanismo para registrar la dirección de auxilio con un agente interno.

El agente interno redirige los datagramas de la red principal a la dirección de auxilio. El agente interno construye un nuevo encabezado IP que contiene la dirección de auxilio del nodo móvil como dirección IP de destino. Este nuevo encabezado encapsula el datagrama IP original. Así, la dirección permanente del nodo móvil no tiene efecto alguno en el enrutamiento del datagrama encapsulado hasta que el datagrama llega a la dirección de auxilio. Este tipo de encapsulado se denomina *creación de túneles*. Una vez llega a la dirección de auxilio, el datagrama es desencapsulado. A continuación se entrega al nodo móvil.

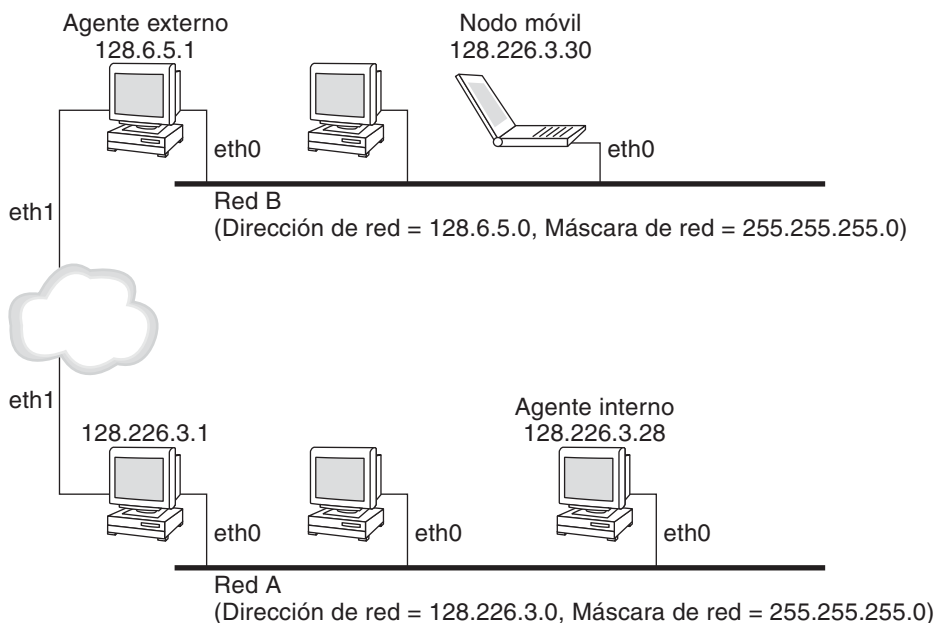
En la figura siguiente se muestra un nodo móvil que reside en su red principal, Network A, antes de que se traslade a una red externa, Network B. Ambas redes son compatibles con IP para móviles. El nodo móvil está siempre asociado con su dirección permanente, 128.226.3.30.

FIGURA 27-2 Nodo móvil que reside en su red principal



En la figura siguiente se muestra un nodo móvil que se ha trasladado a una red externa, Network B. Los datagramas destinados al nodo móvil son interceptados por el agente interno en la red principal, Network A, y encapsulados. A continuación, los datagramas se envían al agente externo en Network B, y el agente externo filtra el encabezado exterior. A continuación, el agente externo entrega el datagrama al nodo móvil, ubicado en Network B.

FIGURA 27-3 Nodo móvil que se traslada a una red externa



Es posible que la dirección de auxilio pertenezca a un agente externo. La dirección de auxilio puede adquirirse mediante el Protocolo dinámico de configuración de host (DHCP) o el Protocolo punto a punto (PPP). En el segundo caso, un nodo móvil posee una dirección de auxilio coubicada.

Los agentes de movilidad (agentes internos y externos) anuncian su presencia mediante mensajes de *anuncio de agente*. Un nodo móvil tiene también la opción de solicitar un mensaje de anuncio de agente. El nodo utiliza cualquier agente de movilidad conectado localmente a través de un mensaje de *solicitud de agente*. Los nodos móviles utilizan los anuncios de agente para determinar si se encuentran en su red principal o en una red externa.

El nodo móvil utiliza un proceso de registro especial para informar al agente interno acerca de la actual ubicación del nodo. El nodo móvil siempre está atento a los anuncios de los agentes de movilidad advirtiéndolo de su presencia. El nodo utiliza estos anuncios para determinar cuándo se ha trasladado a otra subred. Cuando un nodo móvil determina que el nodo móvil ha cambiado de ubicación, el nodo utiliza el nuevo agente externo para reenviar un mensaje de registro al agente interno. El nodo móvil utiliza el mismo proceso cuando el nodo móvil se mueve de una red externa a otra.

Cuando el nodo móvil detecta que se encuentra en la red principal, el nodo deja de utilizar los servicios de movilidad. Cuando el nodo móvil vuelve a su red principal, *anula su registro* con el agente interno.

Descubrimiento de agentes

Los nodos móviles utilizan el método denominado *descubrimiento de agentes* para determinar la información siguiente:

- Cuándo se ha trasladado el nodo de una red a otra
- Si la red es la principal o una red externa
- La dirección de auxilio de agente externo que ofrece cada agente externo de esa red
- Los servicios de movilidad que ofrece el agente de movilidad, anunciados en forma de indicadores, y las extensiones adicionales en el anuncio de agente

Los agentes de movilidad transmiten *anuncios de agentes* para avisar de sus servicios en una red. En ausencia de anuncios de agente, un nodo móvil puede solicitarlos. Esta función se denomina *solicitud de agente*. Si un nodo móvil admite su propia dirección de auxilio coubicada, el nodo puede utilizar anuncios de enrutador normales para la misma finalidad.

Anuncio de agente

Los nodos móviles utilizan anuncios de agentes para determinar el punto de conexión actual a Internet o a la red de una organización. Un anuncio de agente es un anuncio de enrutador del protocolo de mensajes de control de Internet (ICMP) que se ha ampliado para llevar también una extensión de anuncio de agente de movilidad.

Un agente externo puede estar demasiado ocupado para servir a otros nodos móviles. Sin embargo, el agente externo debe seguir enviando anuncios de agente. Así, el nodo móvil, ya registrado con un agente externo, sabe que no se ha movido fuera del ámbito del agente externo. El nodo móvil sabe también de este modo que no ha habido un fallo del agente externo. Un nodo móvil registrado con un agente externo del que ya no recibe anuncios de agente probablemente sabe que ha perdido el contacto con ese agente.

Anuncios de agente a través de interfaces dinámicas

Se puede configurar la implementación del agente externo de modo que envía anuncios a través de interfaces creadas dinámicamente. También se pueden habilitar o inhabilitar anuncios no solicitados limitados a través de las interfaces de anuncios. Las interfaces creadas dinámicamente se definen como aquellas interfaces que se configuran después de que se inicie el daemon `mipagent`. Los anuncios a través de interfaces dinámicas son útiles en el caso de aplicaciones compatibles con interfaces de movilidad transitorios. Además, la limitación de anuncios no solicitados ayuda a ahorrar ancho de banda.

Solicitud de agente

Todos los nodos móviles deberían implementar la solicitud de agentes. El nodo móvil utiliza los mismos procedimientos, valores predeterminados y constantes que se especifican para los mensajes de solicitud de enrutadores ICMP.

El ritmo de envío de solicitudes por parte del nodo móvil está limitado por el nodo en sí. El nodo móvil puede enviar tras solicitudes iniciales al ritmo máximo de una solicitud por segundo mientras el nodo busca un agente. Una vez que el nodo móvil se registra con un agente, el ritmo de envío de solicitudes se reduce para limitar la carga sobre la red local.

Direcciones de auxilio

IP para móviles ofrece los siguientes modos alternativos para la obtención de direcciones de auxilio:

- Un agente externo proporciona una *dirección de auxilio de agente externo*, que se notifica al nodo móvil mediante mensajes de anuncio de agentes. La dirección de auxilio suele ser la dirección IP del agente externo que envía el anuncio. El agente externo es el extremo final del túnel. Cuando el agente externo recibe datagramas a través de un túnel, los desencapsula. A continuación, el agente entrega el datagrama interno al nodo móvil. Por tanto, varios nodos móviles pueden compartir la misma dirección de auxilio. En los enlaces inalámbricos, el ancho de banda es un factor importante. Desde los enlaces inalámbricos, los agentes externos pueden ofrecer servicios de IP para móviles a enlaces con un mayor ancho de banda.
- Un nodo móvil obtiene una *dirección de auxilio coubicada* como dirección IP local a través de algún medio externo. El nodo móvil se asocia a continuación con alguna de sus propias interfaces de red. El nodo puede obtener la dirección en forma temporal mediante DHCP. La dirección puede también ser propiedad del nodo móvil a largo plazo. Sin embargo, el nodo solo puede utilizar la dirección mientras se halla de visita en la subred a la que pertenece la dirección de auxilio. Al utilizar una dirección de auxilio coubicada, el nodo móvil actúa como extremo final del túnel. El nodo efectúa el desencapsulado de los datagramas que le envían a través del túnel.

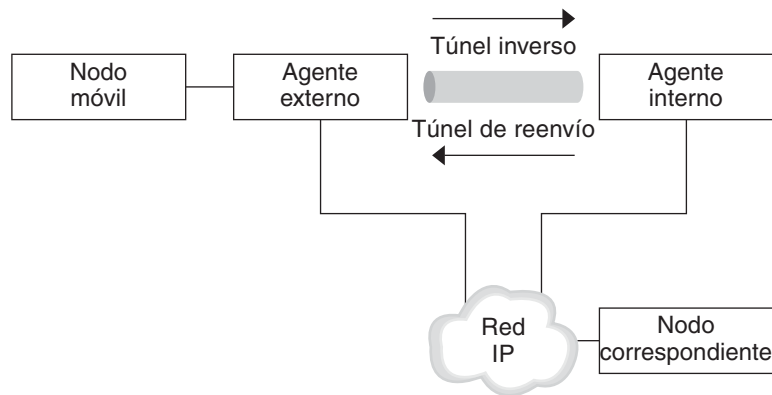
Una dirección de auxilio coubicada permite que el nodo móvil funcione sin necesidad de agente externo. Por tanto, un nodo móvil puede utilizar una dirección de auxilio coubicada en redes que no tienen implementado un agente externo.

Si un nodo móvil utiliza una dirección de auxilio coubicada, el nodo debe hallarse en un enlace identificado por el prefijo de red de la dirección de auxilio. En caso contrario, los datagramas que vayan destinados a la dirección de auxilio no se podrán entregar.

IP para móviles con túnel inverso

En la sección “[Funcionamiento de IP para móviles](#)” en la [página 698](#) se asume que el enrutamiento dentro de Internet es independiente de la dirección de origen del datagrama. Sin embargo, es posible que un enrutador intermedio compruebe si la dirección de origen es topológicamente correcta. Si un enrutador intermedio efectúa esa comprobación, el nodo móvil deberá configurar un túnel inverso. Al configurar un túnel inverso desde la dirección de auxilio al agente interno, se garantiza que la dirección de origen del paquete de datos IP es topológicamente correcta. Los agentes externos e internos anuncian su compatibilidad con la función de túnel inverso. Un nodo móvil puede solicitar un túnel inverso entre al agente externo y el interno cuando el nodo se registra. Un túnel inverso empieza en la dirección de auxilio del nodo móvil y termina en el agente interno. En la figura siguiente se muestra la topología de IP para móviles que utiliza un túnel inverso.

FIGURA 27-4 IP para móviles con túnel inverso



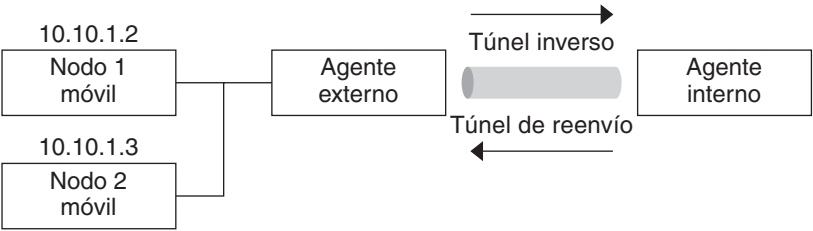
Admisión limitada de direcciones privadas

Los nodos móviles con direcciones privadas que no son enrutables globalmente a través de Internet requieren el uso de túneles inversos. IP para móviles de Solaris es compatible con nodos móviles con direcciones privadas. Consulte “[Descripción general de la implementación de IP para móviles en Solaris](#)” en la [página 729](#) para conocer qué funciones no son compatibles con IP para móviles de Solaris.

Las empresas suelen emplear direcciones privadas si no necesitan conectividad externa. Las direcciones privadas no se pueden enrutar a través de Internet. Cuando un nodo móvil tiene una dirección privada, el nodo sólo puede comunicarse con un nodo de destino si su agente interno hace pasar sus datagramas a través de un túnel inverso. El agente interno entrega entonces el datagrama al otro nodo de la misma forma que se entrega cuando el nodo móvil está

en su red principal. En la figura siguiente se muestra una topología de red con dos nodos móviles con direcciones privadas. Los dos nodos utilizan la misma dirección de auxilio cuando se registran con el mismo agente externo.

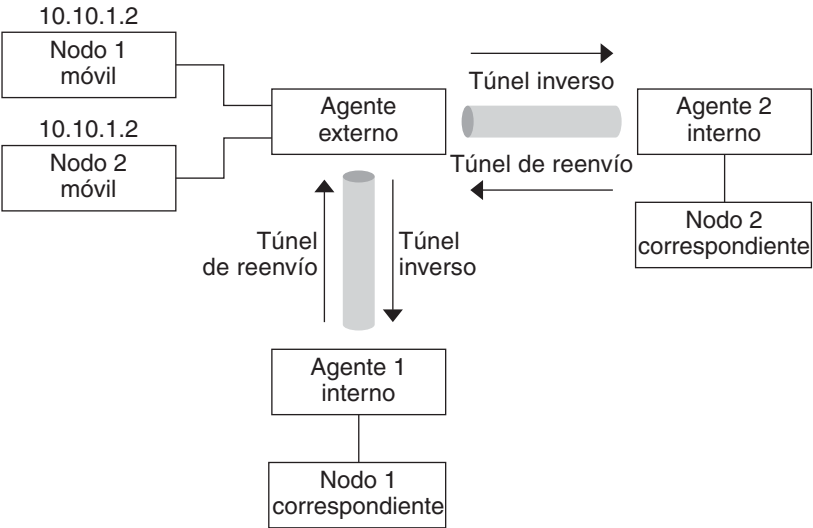
FIGURA 27-5 Nodos móviles con dirección privada ubicados en la misma red externa



La dirección de auxilio y la dirección del agente interno deben ser direcciones enrutables globalmente si pertenecen a dominios distintos conectados por Internet pública.

La misma red externa puede incluir dos nodos móviles con direcciones privadas que tengan la misma dirección IP. Sin embargo, cada nodo móvil debe tener un agente interno distinto. Asimismo, cada dirección debe hallarse en una subred de anuncios distinta de un único agente externo. En la figura siguiente se muestra una topología de red en la que se muestra esta situación.

FIGURA 27-6 Nodos móviles con dirección privada ubicados en redes externas distintas



Registro de IP para móviles

Los nodos móviles detectan si se han trasladado de una subred a otra mediante el uso de anuncios de agentes. Cuando el nodo móvil recibe un anuncio de agente que indica que ha cambiado de ubicación, el nodo se registra a través de un agente externo. Aunque es posible que el nodo móvil haya obtenido su propia dirección de auxilio coubicada, esta función se ofrece para restringir el acceso a servicios de movilidad.

El registro de IP para móviles ofrece un mecanismo flexible para que los nodos móviles comuniquen al agente interno la información de su actual estado de accesibilidad. El proceso de registro permite a los nodos móviles efectuar las siguientes tareas:

- Solicitar servicios de reenvío al visitar una red externa
- Informar al agente interno de su dirección de auxilio actual
- Renovar un registro que esté a punto de caducar
- Anular el registro cuando el nodo móvil vuelve a su red principal
- Solicitar un túnel inverso

En los mensajes de registro se intercambia información entre un nodo móvil, un agente externo y el agente interno. El registro crea o modifica un enlace de movilidad en el agente interno. El proceso de registro asocia la dirección permanente del nodo móvil durante la vida útil especificada.

El proceso de registro permite también a los nodos móviles efectuar las siguientes funciones:

- Registrarse con varios agentes externos
- Anular direcciones de auxilio específicas al tiempo que se conservan otros enlaces de movilidad
- Descubrir la dirección de un agente interno si el nodo móvil no está configurado con esta información

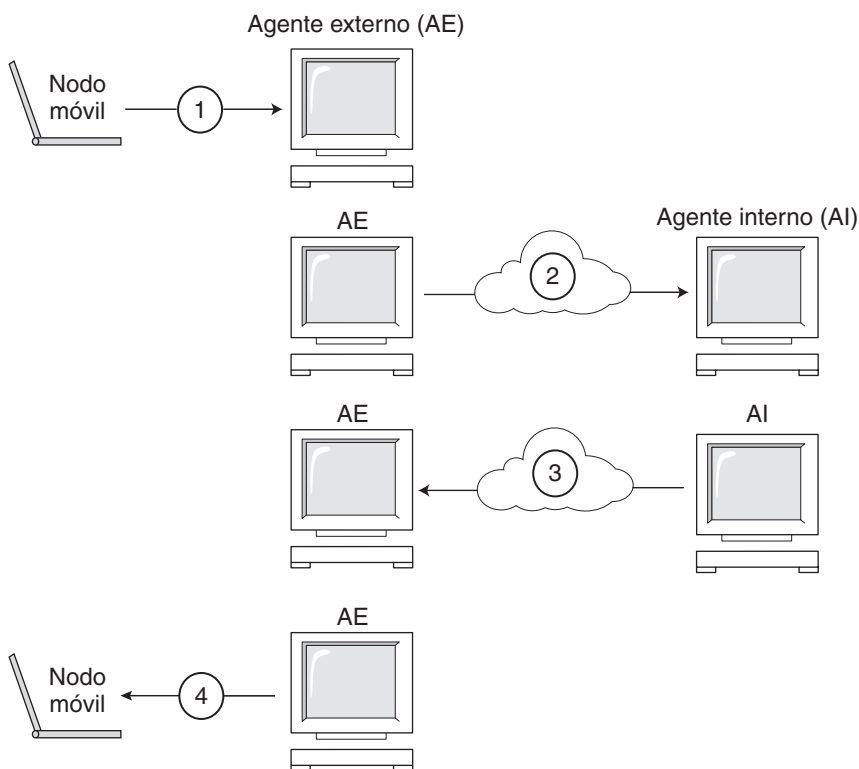
IP para móviles define los siguientes procesos de registro para un nodo móvil:

- Si un nodo móvil registra la dirección de auxilio de un agente externo, el nodo móvil está indicando al agente interno que está accesible a través de dicho agente externo.
- Si un nodo móvil recibe un anuncio de agente que exige que el nodo se registre a través de un agente externo, el nodo móvil puede aún intentar obtener una dirección de auxilio coubicada. El nodo móvil puede también registrarse con ese agente externo o cualquier otro en ese enlace.
- Si un nodo móvil utiliza una dirección de auxilio coubicada, el nodo se registra directamente con el agente interno.
- Si un nodo móvil vuelve a su red principal, el nodo anula su registro con el agente interno.

Estos procesos de registro implican el intercambio de solicitudes de registro y de mensajes de respuesta de registro. Cuando el nodo móvil se registra mediante un agente externo, el proceso de registro recorre los pasos siguientes, que se muestran en la figura a continuación:

1. El nodo móvil envía una solicitud de registro al agente externo previsto para iniciar el proceso de registro.
2. El agente externo procesa la solicitud de registro y a continuación la envía al agente interno.
3. El agente interno envía una respuesta de registro al agente externo para conceder o denegar la solicitud.
4. El agente externo procesa la respuesta de registro y a continuación la envía al nodo móvil para indicarle la disposición de la solicitud.

FIGURA 27-7 Proceso de registro de IP para móviles



Cuando el nodo móvil se registra directamente en el agente interno, el proceso de registro se compone únicamente de estos pasos:

- El nodo móvil envía una solicitud de registro al agente interno.
- El agente interno envía una respuesta de registro al nodo móvil que concede o deniega la solicitud.

Asimismo, el agente externo o el interno pueden requerir un túnel inverso. Si el agente externo es compatible con la función de túnel inverso, el nodo móvil utiliza el proceso de registro para solicitar un túnel inverso. El nodo móvil activa el indicador de túnel inverso en la solicitud de registro para pedir un túnel inverso.

Identificador de acceso de red (NAI)

Los servidores de autenticación, autorización y contabilidad (en inglés, AAA) utilizados en Internet proporcionan servicios de autenticación y autorización para sistemas de acceso telefónico. Estos servicios son también válidos para nodos móviles que utilizan IP para móviles cuando los nodos intentan conectarse a dominios externos con servidores AAA. Los servidores AAA utilizan el Identificador de acceso de red (NAI) para identificar a los clientes. Un nodo móvil puede identificarse a sí mismo si incluye el NAI en la solicitud de registro de IP para móviles.

El NAI se suele utilizar como identificador exclusivo del nodo móvil, por lo que no siempre es necesaria la dirección permanente del nodo para proporcionar dicha función. Así, un nodo móvil se puede autenticar a sí mismo. Por tanto, se puede autorizar a un nodo móvil la conexión a un dominio externo sin siquiera disponer de una dirección permanente. Para solicitar la asignación de una dirección permanente, un mensaje que contenga la extensión NAI del nodo móvil puede poner a cero el de .campo de dirección permanente de la solicitud de registro.

Autenticación mediante mensaje de IP para móviles

Cada nodo móvil, agente interno y externo admiten una asociación de seguridad de movilidad entre los distintos componentes de IP para móviles. La asociación de seguridad está indexada por el índice de parámetro de seguridad (SPI) y la dirección IP. En el caso del nodo móvil, esta dirección es la dirección permanente del nodo. Los mensajes de registro entre un nodo móvil y el agente interno se autentican con la extensión de autenticación nodo móvil-agente interno. Aparte de la autenticación nodo móvil-agente interno, que es obligatoria, puede utilizar las autenticaciones opcionales nodo móvil-agente externo y agente externo-agente interno.

Solicitud de registro del nodo móvil

Los nodos móviles utilizan un mensaje de *solicitud de registro* para registrarse con el agente interno. Así, el agente interno puede crear o modificar un enlace de movilidad para ese nodo móvil (por ejemplo, con un nuevo valor de vida útil). El agente externo puede transmitir la solicitud de registro al agente interno. Sin embargo, si el nodo móvil está registrando una dirección de auxilio couchada, el nodo puede enviar la solicitud de registro directamente al agente interno. Si el agente externo anuncia que los mensajes de registro se deben enviar al agente externo, el nodo móvil deberá enviar la solicitud de registro al agente externo.

Mensaje de respuesta de registro

Un agente de movilidad devuelve un mensaje de *respuesta de registro* a un nodo móvil que ha enviado un mensaje de solicitud de registro. Si el nodo móvil solicita servicio de un agente externo, ese agente recibe la respuesta del agente interno. A continuación, el agente externo transmite la respuesta al nodo móvil. El mensaje de respuesta contiene los códigos necesarios para informar al agente externo del estado de la solicitud de registro. El mensaje contiene también la vida útil que concede el agente interno. Dicha vida puede ser inferior a la solicitud original. La respuesta de registro puede contener también una asignación de dirección permanente dinámica.

Consideraciones del agente externo

El agente externo tiene mayoritariamente un papel pasivo en el proceso de registro de IP para móviles. El agente externo agrega todos los nodos móviles registrados a la tabla de visitantes. El agente externo transmite las solicitudes de registro entre nodos móviles y agentes internos. Asimismo, cuando el agente interno proporciona la dirección de auxilio, el agente externo desencapsula los datagramas para su entrega al nodo móvil. El agente externo envía también mensajes periódicos de anuncio de agente para advertir de su presencia.

Si los agentes internos y los externos admiten túneles inversos y el nodo móvil solicita un túnel inverso, el agente externo envía por el túnel todos los paquetes del nodo móvil al agente interno. A continuación, el agente interno envía los paquetes al nodo de destino. Este proceso es inverso al del agente interno enviando por túnel todos los paquetes del nodo móvil al agente externo para su entrega al nodo móvil. Un agente externo compatible con túneles inversos anuncia esta compatibilidad para el registro. A causa de las directrices locales, el agente externo puede denegar una solicitud de registro si el indicador de túnel inverso no está activado. El agente externo sólo puede distinguir varios nodos móviles con la misma dirección IP (privada) si dichos nodos visitan interfaces distintas del agente externo. En la situación del túnel directo, el agente externo distingue entre los diversos nodos móviles que comparten la misma dirección privada consultando la interfaz del túnel entrante. La interfaz del túnel entrante está asociada unívocamente con una dirección de agente interno.

Consideraciones del agente interno

El agente interno tiene una tarea activa en el proceso de registro. El agente interno recibe solicitudes de registro del nodo móvil. La solicitud de registro puede haber sido transmitida por el agente externo. El agente interno actualiza su registro de los enlaces de movilidad de este nodo móvil. El agente interno emite una respuesta de registro adecuada para cada solicitud de registro. El agente interno reenvía también paquetes al nodo móvil cuando este no está en la red principal.

Un agente interno puede no tener configurada una subred física para los nodos móviles. Sin embargo, el agente debe reconocer la dirección permanente del nodo móvil mediante el archivo `mipagent.conf` u otro mecanismo cuando concede el registro. Para obtener más información acerca de `mipagent.conf`, consulte [“Creación del archivo de configuración de IP móvil” en la página 714](#).

Un agente interno puede admitir nodos móviles con direcciones privadas configurando estos nodos en el archivo `mipagent.conf`. Las direcciones permanentes que utiliza el agente interno deben ser exclusivas.

Descubrimiento dinámico de agente interno

En ciertas situaciones, es posible que el nodo móvil no conozca la dirección del agente interno cuando el nodo intenta registrarse. Si el nodo móvil no sabe la dirección del agente interno, puede utilizar la resolución dinámica de la dirección del agente para averiguarla. En esta situación, el nodo móvil asigna como valor del campo de agente interno en la solicitud de registro la dirección de multidifusión de su red principal dirigida a la subred. Cada agente interno que reciba una solicitud de registro con una dirección de destino que sea una dirección de multidifusión rechazará el registro del nodo móvil devolviendo una respuesta de rechazo de registro. De esta forma, el nodo móvil puede utilizar la dirección IP de unidifusión del agente interno indicada en la respuesta de rechazo la siguiente vez que el nodo intente registrarse.

Encaminamiento de datagramas entre nodos móviles

En esta sección se describe de qué modo los nodos móviles y los agentes externos cooperan para enrutar los datagramas de los nodos móviles conectados a una red externa.

Consulte [“Descripción general de la implementación de IP para móviles en Solaris” en la página 729](#) para conocer qué funciones son compatibles con el SO Solaris.

Métodos de encapsulado

Los agentes internos y externos utilizan alguno de los métodos de encapsulado disponibles para admitir datagramas que utilicen túnel. Los métodos de encapsulado definidos son Encapsulado de IP en IP, Encapsulado mínimo y Encapsulado de enrutamiento genérico (GRE). El agente interno y el externo, o el nodo móvil coubicado indirecto y el agente interno, deben admitir el mismo método de encapsulado. Todas las entidades de IP para móviles deben admitir el encapsulado de IP en IP.

Encaminamiento de datagramas de unidifusión

Al registrarse en una red externa, el nodo móvil utiliza las siguientes reglas para elegir un enrutador predeterminado:

- Si el nodo móvil está registrado y utiliza una dirección de auxilio de un agente externo, el proceso es directo. El nodo móvil elige su enrutador predeterminado de entre las direcciones de enrutador anunciado en la parte de anuncio de enrutador ICMP del anuncio del agente. El nodo móvil puede también tener en cuenta la dirección IP de origen del anuncio del agente como otra posible opción para la dirección IP de un enrutador predeterminado.
- El nodo móvil puede registrarse directamente con el agente interno mediante el uso de una dirección de auxilio coubicada. A continuación, el nodo móvil elige su enrutador predeterminado entre los que están anunciados en cualquier mensaje de anuncio de enrutador ICMP que reciba. El prefijo de red del enrutador predeterminado elegido debe coincidir con el prefijo de red de la dirección de auxilio del nodo móvil que se obtiene de forma externa. La dirección debe coincidir con la dirección IP de origen del anuncio de agente bajo el prefijo de red. El nodo puede asimismo considerar esa dirección IP de origen como otra posible alternativa de dirección IP de un enrutador predeterminado.
- Si el nodo móvil está registrado, un agente externo que admita túnel inverso enruta los datagramas de unidifusión del nodo móvil al agente interno a través del túnel inverso. Si el nodo móvil está registrado con un agente externo que admite túnel inverso, el nodo deberá utilizar ese agente como enrutador predeterminado.

Datagramas de multidifusión

Cuando un agente interno recibe un datagrama de multidifusión o de difusión, el agente interno reenvía únicamente el datagrama a los nodos móviles que han solicitado específicamente recibirlos. El modo en que el agente interno envía estos datagramas a los nodos móviles depende principalmente de dos factores. Bien el nodo móvil utiliza una dirección de auxilio proporcionada por un agente externo o bien utiliza su propia dirección de auxilio coubicada. El primer caso implica que el datagrama debe tener un doble encapsulado. El primer encabezado IP identifica el nodo móvil para el que se debe entregar el datagrama. El primer encabezado IP no está presente en el datagrama de multidifusión o difusión. El segundo encabezado IP identifica la dirección de auxilio y es el encabezado de túnel habitual. En el segundo caso, el nodo móvil desencapsula sus propios datagramas, y basta con enviar el datagrama a través del túnel usual.

Encaminamiento de datagramas de multidifusión

Para empezar a recibir tráfico de multidifusión cuando un nodo móvil está visitando una subred externa, el nodo puede unirse a un grupo de multidifusión mediante uno de estos métodos:

- Si el nodo móvil utiliza una dirección de auxilio coubicada, puede utilizarla como dirección IP de origen de cualquier mensaje de entrada del Protocolo de gestión de grupos de Internet (IGMP). Sin embargo, la subred visitada debe disponer de un enrutador de multidifusión.

- Si el nodo móvil quiere unirse al grupo de ICMP desde su subred principal, deberá utilizar un túnel inverso para enviar mensajes de entrada IGMP al agente interno. Sin embargo, el agente interno del nodo móvil debe ser un enrutador de multidifusión. El agente interno reenvía entonces los datagramas de multidifusión al nodo móvil a través del túnel.
- Si el nodo móvil utiliza una dirección de auxilio coubicada, puede utilizarla como dirección IP de origen de los mensajes de entrada IGMP. Sin embargo, la subred visitada debe disponer de un enrutador de multidifusión. Una vez que el nodo móvil ha entrado en el grupo, puede participar enviando sus propios paquetes de multidifusión directamente en la red visitada.
- Enviar directamente en la red visitada.
- Enviar al agente interno a través de un túnel.

El enrutamiento de multidifusión depende de la dirección IP de origen. Un nodo móvil que envía un datagrama de multidifusión debe enviarlo desde una dirección de origen válida en ese enlace. Así, un nodo móvil que envíe datagramas de multidifusión directamente en la red visitada debe utilizar una dirección de auxilio coubicada como dirección IP de origen. Asimismo, el nodo móvil debe haberse unido al grupo de multidifusión asociado con la dirección. De forma similar, un nodo móvil que se haya unido a un grupo de multidifusión mientras estaba en su subred, antes de trasladarse, o se haya unido a un grupo de multidifusión utilizando itinerancia a través de un túnel inverso con su agente interno, deberá utilizar su dirección permanente como dirección IP de origen del datagrama de multidifusión. Así, el nodo móvil deberá enviar también estos datagramas por túnel inverso a su subred principal, ya sea él mismo mediante su dirección de auxilio coubicada o a través del túnel inverso de un agente externo.

Aunque parece más eficiente que un nodo móvil se una siempre desde la subred que está visitando, sigue siendo un nodo móvil. En consecuencia, el nodo debería repetir la entrada cada vez que cambiase de subred. La forma más eficiente es que el nodo móvil se una a través de su agente interno, sin tener que encargarse de la carga adicional. Asimismo, puede haber sesiones de multidifusión solo disponibles desde la subred principal. Otros factores pueden también exigir que el nodo móvil participe de un modo específico.

Consideraciones de seguridad para IP para móviles

En numerosas situaciones, los equipos móviles utilizan enlaces inalámbricos para conectarse a la red. Los enlaces inalámbricos son especialmente vulnerables a intrusiones pasivas, ataques de repetición activos y otros ataques activos.

IP para móviles carece de capacidad para reducir o eliminar esta vulnerabilidad, de modo que utiliza un tipo de autenticación para proteger los mensajes de registro de IP para móviles contra estos ataques. El algoritmo predeterminado utilizado es MD5, con una clave de 128 bits. El modo de funcionamiento predeterminado exige que la clave preceda y remate los datos del hash. El agente externo utiliza MD5 para la autenticación. Este agente utiliza también claves de

128 bits o mayores, con distribución de claves manual. IP para móviles puede admitir otros algoritmos de autenticación, modos de algoritmo, métodos de distribución de claves y tamaños de clave.

Estos métodos impiden la modificación de los mensajes de registro de IP para móviles. Sin embargo, IP para móviles utiliza también una forma de protección de repetición para avisar a las entidades de IP para móviles cuando reciben duplicados de mensajes de registro anteriores. Sin este método de protección, el nodo móvil y su agente interno podrían perder la sincronización cuando alguno de ellos recibiese un mensaje de registro. Así, IP para móviles actualiza su estado. Por ejemplo, un agente interno recibe un mensaje de anulación de registro duplicado mientras el nodo móvil está registrado a través de un agente externo.

La protección de repetición se efectúa mediante un método denominado *nonces o indicaciones de hora*. Los agentes internos y los nodos móviles intercambian nonces e indicaciones de hora dentro de los mensajes de registro de IP para móviles. Las nonces e indicaciones de hora están protegidas contra modificaciones por un algoritmo de autenticación. Por consiguiente, si un agente interno recibe un mensaje duplicado, el mensaje puede descartarse.

El uso de túneles puede suponer una vulnerabilidad significativa, en especial si el registro no está autenticado. Asimismo, el Protocolo de resolución de direcciones (ARP) no está autenticado, y se puede utilizar para robar el tráfico de otro host.

Administración de IP móvil (tareas)

En este capítulo se ofrecen procedimientos para modificar, agregar, eliminar y mostrar parámetros del archivo de configuración de IP móvil. En él se indica también como mostrar el estado del agente de movilidad.

Este capítulo contiene la información siguiente:

- “Creación del archivo de configuración de IP móvil (mapa de tareas)” en la página 713
- “Creación del archivo de configuración de IP móvil” en la página 714
- “Modificación del archivo de configuración de IP móvil” en la página 719
- “Modificación del archivo de configuración de IP móvil (mapa de tareas)” en la página 718
- “Presentación del estado del agente de movilidad” en la página 725
- “Presentación de las rutas de movilidad de un agente externo” en la página 727

Para ver una introducción a IP para móviles, consulte el [Capítulo 27, “IP para móviles \(Descripción general\)”](#). Para ver información detallada sobre IP para móviles, consulte el [Capítulo 29, “Archivos y comandos de IP para móviles \(referencia\)”](#).

Nota – La función IP móvil se suprime de las actualizaciones de Solaris 10 posteriores a Solaris 10 8/07.

Creación del archivo de configuración de IP móvil (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Crear el archivo de configuración de IP móvil.	Implica crear el archivo <code>/etc/inet/mipagent.conf</code> o copiar uno de los archivos de ejemplo.	“Creación del archivo de configuración de IP móvil” en la página 715

Tarea	Descripción	Para obtener instrucciones
Configurar la sección General.	Implica escribir el número de versión en la sección General del archivo de configuración de IP móvil.	“Cómo configurar la sección General” en la página 715
Configurar la sección Advertisements.	Implica agregar etiquetas y valores, o modificarlos, en la sección Advertisements del archivo de configuración de IP móvil.	“Cómo configurar la sección Advertisements” en la página 716
Configurar la sección GlobalSecurityParameters.	Implica agregar etiquetas y valores, o modificarlos, en la sección GlobalSecurityParameters del archivo de configuración de IP móvil.	“Cómo configurar la sección GlobalSecurityParameters” en la página 716
Configurar la sección Pool.	Implica agregar etiquetas y valores, o modificarlos, en la sección Pool del archivo de configuración de IP móvil.	“Cómo configurar la sección Pool” en la página 717
Configurar la sección SPI.	Implica agregar etiquetas y valores, o modificarlos, en la sección SPI del archivo de configuración de IP móvil.	“Cómo configurar la sección SPI” en la página 717
Configurar la sección Address.	Implica agregar etiquetas y valores, o modificarlos, en la sección Address del archivo de configuración de IP móvil.	“Cómo configurar la sección Address” en la página 717

Creación del archivo de configuración de IP móvil

En esta sección se explica cómo planificar para IP móvil y crear el archivo `/etc/inet/mipagent.conf`.

▼ Cómo planificar para IP móvil

Cuando se configura el archivo `mipagent.conf` por primera vez, se deben efectuar las tareas siguientes:

- 1 **En función de las necesidades de su organización, determinar qué funciones puede ofrecer su agente de IP móvil:**
 - solo funcionalidad de agente externo
 - sólo funcionalidad de agente interno
 - Funcionalidad de agente interno y externo

- 2 Cree el archivo `/etc/inet/mipagent.conf` y especifique los parámetros necesarios mediante los procedimientos descritos en esta sección. También puede copiar uno de los archivos siguientes en `/etc/inet/mipagent.conf` y modificarlo según sus necesidades:
 - Para funcionalidad de agente externo, copie `/etc/inet/mipagent.conf.fa-sample`.
 - Para funcionalidad de agente interno, copie `/etc/inet/mipagent.conf.ha-sample`.
 - Para funcionalidad de agente externo y de agente interno, copie `/etc/inet/mipagent.conf-sample`.
- 3 Puede reiniciar el equipo e invocar la secuencia de inicio que inicia el daemon `mipagent`. También puede iniciar `mipagent` escribiendo el comando siguiente:


```
# /etc/inet.d/mipagent start
```

▼ Creación del archivo de configuración de IP móvil

- 1 Asuma la función de administrador principal, o conviértase en superusuario, en el sistema en el que quiera activar IP móvil.
La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.
- 2 Cree el archivo `/etc/inet/mipagent.conf` mediante una de estas opciones:
 - En el directorio `/etc/inet`, cree un archivo vacío con el nombre `mipagent.conf`.
 - Copie el archivo de la lista siguiente que ofrezca la funcionalidad que desee para el archivo `/etc/inet/mipagent.conf`.
 - `/etc/inet/mipagent.conf.fa-sample`
 - `/etc/inet/mipagent.conf.ha-sample`
 - `/etc/inet/mipagent.conf-sample`
- 3 Agregue o modifique parámetros de configuración en el archivo `/etc/inet/mipagent.conf` para adaptarse a sus requisitos.
En el resto de procedimientos de esta sección se describen los pasos para modificar las secciones de `/etc/inet/mipagent.conf`.

▼ Cómo configurar la sección General

Si ha copiado uno de los archivos de ejemplo del directorio `/etc/inet`, puede hacer caso omiso de este procedimiento, porque el archivo de ejemplo ya contiene esta entrada. “[Sección General](#)” en la [página 735](#) proporciona descripciones de las etiquetas y valores que se utilizan en esta sección.

- **Edite el archivo `/etc/inet/mipagent.conf` y agregue las líneas siguientes:**

```
[General]
  Version = 1.0
```

Nota – El archivo `/etc/inet/mipagent.conf` debe contener esta entrada.

▼ **Cómo configurar la sección `Advertisements`**

“[Sección `Advertisements`](#)” en la [página 735](#) proporciona descripciones de las etiquetas y valores que se utilizan en esta sección.

- **Edite el archivo `/etc/inet/mipagent.conf` y agregue o modifique las siguientes líneas utilizando los valores requeridos para su configuración.**

```
[Advertisements interface]
  HomeAgent = <yes/no>
  ForeignAgent = <yes/no>
  PrefixFlags = <yes/no>
  AdvertiseOnBcast = <yes/no>
  RegLifetime = n
  AdvLifetime = n
  AdvFrequency = n
  ReverseTunnel = <yes/no/FA/HA/both>
  ReverseTunnelRequired = <yes/no/FA/HA>
```

Nota – Deberá incluir una sección `Advertisements` distinta para cada interfaz del host local que ofrezca servicios de IP móvil.

▼ **Cómo configurar la sección `GlobalSecurityParameters`**

“[Sección `GlobalSecurityParameters`](#)” en la [página 736](#) proporciona descripciones de las etiquetas y valores que se utilizan en esta sección.

- **Edite el archivo `/etc/inet/mipagent.conf` y agregue o modifique las siguientes líneas utilizando los valores requeridos para su configuración.**

```
[GlobalSecurityParameters]
  MaxClockSkew = n
  HA-FAauth = <yes/no>
  MN-FAauth = <yes/no>
  Challenge = <yes/no>
  KeyDistribution = files
```

▼ Cómo configurar la sección Pool

“Sección Pool” en la página 737 proporciona descripciones de las etiquetas y valores que se utilizan en esta sección:

- 1 Edite el archivo `/etc/inet/mipagent.conf`
- 2 Agregue o modifique las siguientes líneas utilizando los valores necesarios para su configuración:

```
[Pool pool-identifier]
    BaseAddress = IP-address
    Size = size
```

▼ Cómo configurar la sección SPI

“Sección SPI” en la página 738 proporciona descripciones de las etiquetas y valores que se utilizan en esta sección.

- 1 Edite el archivo `/etc/inet/mipagent.conf`.
- 2 Agregue o modifique las siguientes líneas utilizando los valores necesarios para su configuración:

```
[SPI SPI-identifier]
    ReplayMethod = <none/timestamps>
    Key = key
```

Nota – Deberá incluir una sección SPI distinta para cada contexto de seguridad implementado.

▼ Cómo configurar la sección Address

“Sección Address” en la página 739 proporciona descripciones de las etiquetas y valores que se utilizan en esta sección.

- 1 Edite el archivo `/etc/inet/mipagent.conf`.
- 2 Agregue o modifique las siguientes líneas utilizando los valores necesarios para su configuración:

- Para un nodo móvil, utilice lo siguiente:

```
[Address address]
    Type = node
    SPI = SPI-identifier
```

- Para un agente, utilice lo siguiente:

[Address address]
Type = agent
SPI = SPI-identifier

- **Para un nodo móvil identificado por su NAI, utilice lo siguiente:**

[Address NAI]
Type = Node
SPI = SPI-identifier
Pool = pool-identifier

- **Para un nodo móvil predeterminado, utilice lo siguiente:**

[Address Node-Default]
Type = Node
SPI = SPI-identifier
Pool = pool-identifier

Modificación del archivo de configuración de IP móvil (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Modificar la sección General.	Utiliza el comando mipagentconfig change para cambiar el valor de una etiqueta en la sección General del archivo de configuración de IP móvil.	“Cómo modificar la sección General” en la página 719
Modificar la sección Advertisements.	Utiliza el comando mipagentconfig change para cambiar el valor de una etiqueta en la sección Advertisements del archivo de configuración de IP móvil.	“Cómo modificar la sección Advertisements” en la página 720
Modificar la sección GlobalSecurityParameters.	Utiliza el comando mipagentconfig change para cambiar el valor de una etiqueta en la sección GlobalSecurityParameters del archivo de configuración de IP móvil.	“Cómo modificar la sección GlobalSecurityParameters” en la página 720
Modificar la sección Pool.	Utiliza el comando mipagentconfig change para cambiar el valor de una etiqueta en la sección Pool del archivo de configuración de IP móvil.	“Cómo modificar la sección Pool” en la página 721
Modificar la sección SPI.	Utiliza el comando mipagentconfig change para cambiar el valor de una etiqueta en la sección SPI del archivo de configuración de IP móvil.	“Cómo modificar la sección SPI” en la página 721

Modificar la sección Address.	Utiliza el comando <code>mipagentconfig change</code> para cambiar el valor de una etiqueta en la sección Address del archivo de configuración de IP móvil.	“Cómo modificar la sección Address” en la página 722
Agregar o eliminar parámetros.	Utiliza el comando <code>mipagentconfig add o delete</code> para agregar nuevos parámetros, etiquetas y valores o para eliminar los existentes en cualquier sección del archivo de configuración de IP móvil.	“Cómo agregar o eliminar parámetros del archivo de configuración” en la página 723
Mostrar los valores actuales de los destinos de parámetros.	Utiliza el comando <code>mipagentconfig get</code> para ver los valores actuales de cualquier sección del archivo de configuración de IP móvil.	“Cómo mostrar los valores actuales de los parámetros del archivo de configuración” en la página 724

Modificación del archivo de configuración de IP móvil

En esta sección se indica cómo modificar el archivo de configuración de IP móvil mediante el comando `mipagentconfig`. También se indica cómo mostrar los valores actuales de los destinos de parámetros.

En [“Configuración del agente de movilidad IP” en la página 743](#) se ofrece una descripción conceptual del uso del comando `mipagentconfig`. También puede consultar la página de comando `man mipagentconfig(1M)`.

▼ Cómo modificar la sección General

- 1 Asuma la función de Administrador principal, o conviértase en superusuario, en el sistema en el que quiera activar IP móvil.**
La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).
- 2 En una línea de comandos, escriba el comando siguiente para cada etiqueta de la sección General que quiera modificar.**

```
# mipagentconfig change <label> <value>
```

Ejemplo 28–1 Modificación de un parámetro de la sección General

En el ejemplo siguiente se muestra cómo modificar el número de versión en la sección General del a. de configuración.

```
# mipagentconfig change version 2
```

▼ Cómo modificar la sección **Advertisements**

- 1 **Asuma la función de administrador principal, o conviértase en superusuario, en el sistema en el que quiera activar IP móvil.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Escriba el comando siguiente para cada una de las etiquetas que quiera modificar en la sección **Advertisements**:**

```
# mipagentconfig change adv device-name <label> <value>
```

Por ejemplo, si va a modificar la vida útil anunciada del agente a 300 segundos para el dispositivo hme0, utilice el siguiente comando.

```
# mipagentconfig change adv hme0 AdvLifetime 300
```

Ejemplo 28–2 Modificación de la sección **Advertisements**

En el ejemplo siguiente se muestra cómo modificar otros parámetros en la sección **Advertisements** del a. de configuración.

```
# mipagentconfig change adv hme0 HomeAgent yes
# mipagentconfig change adv hme0 ForeignAgent no
# mipagentconfig change adv hme0 PrefixFlags no
# mipagentconfig change adv hme0 RegLifetime 300
# mipagentconfig change adv hme0 AdvFrequency 4
# mipagentconfig change adv hme0 ReverseTunnel yes
```

▼ Cómo modificar la sección **GlobalSecurityParameters**

- 1 **Asuma la función de administrador principal, o conviértase en superusuario, en el sistema en el que quiera activar IP móvil.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Escriba el comando siguiente para cada una de las etiquetas que quiera modificar en la sección **GlobalSecurityParameters**:**

```
# mipagentconfig change <label> <value>
```


Por ejemplo, si quiere activar la autenticación para el agente interno y el externo, utilice el comando siguiente:

```
# mipagentconfig change HA-FAuth yes
```

Ejemplo 28–3 Modificación de la sección GlobalSecurityParameters

En el ejemplo siguiente se muestra cómo modificar otros parámetros en la sección GlobalSecurityParameters del a. de configuración.

```
# mipagentconfig change MaxClockSkew 200
# mipagentconfig change MN-FAuth yes
# mipagentconfig change Challenge yes
# mipagentconfig change KeyDistribution files
```

▼ Cómo modificar la sección Pool

- 1 **Asuma la función de administrador principal, o conviértase en superusuario, en el sistema en el que quiera activar IP móvil.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Escriba el comando siguiente para cada etiqueta de la sección Pool que quiera modificar.**

```
# mipagentconfig change Pool pool-identifier <label> <value>
```

Ejemplo 28–4 Modificación de la sección Pool

En el ejemplo siguiente se muestran los comandos que se utilizan para cambiar la dirección base a 192.168.1.1 y el tamaño de la agrupación 10 a 100.

```
# mipagentconfig change Pool 10 BaseAddress 192.168.1.1
# mipagentconfig change Pool 10 Size 100
```

▼ Cómo modificar la sección SPI

- 1 **Asuma la función de administrador principal, o conviértase en superusuario, en el sistema en el que quiera activar IP móvil.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Escriba el comando siguiente para cada una de las etiquetas que quiera modificar en la sección SPI:**

```
# mipagentconfig change SPI SPI-identifier <label> <value>
```

Por ejemplo, si va a cambiar la clave de SPI 257 en 5af2aee39ff0b332, utilice el comando siguiente.

```
# mipagentconfig change SPI 257 Key 5af2aee39ff0b332
```

Ejemplo 28-5 Modificación de la sección SPI

En el ejemplo siguiente se indica cómo cambiar la etiqueta ReplayMethod en la sección SPI del archivo de configuración.

```
# mipagentconfig change SPI 257 ReplayMethod timestamps
```

▼ **Cómo modificar la sección Address**

- 1 **Asuma la función de administrador principal, o conviértase en superusuario, en el sistema en el que quiera activar IP móvil.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Escriba el comando siguiente para cada una de las etiquetas que quiera modificar en la sección Address:**

```
# mipagentconfig change addr [NAI | IPaddr | node-default] <label> <value>
```

Para ver una descripción de los tres métodos de configuración (NAI, dirección IP y nodo predeterminado), consulte [“Sección Address” en la página 739](#).

Por ejemplo, para modificar el SPI de la dirección IP 10.1.1.1 a 258, utilice el siguiente comando:

```
# mipagentconfig change addr 10.1.1.1 SPI 258
```

Ejemplo 28-6 Modificación de la sección Address

En el ejemplo siguiente se muestra cómo modificar los otros parámetros incluidos en la sección Address del archivo de configuración de ejemplo.

```
# mipagentconfig change addr 10.1.1.1 Type agent
# mipagentconfig change addr 10.1.1.1 SPI 259
# mipagentconfig change addr mobilenode@abc.com Type node
# mipagentconfig change addr mobilenode@abc.com SPI 258
```

```
# mipagentconfig change addr mobilenode@abc.com Pool 2
# mipagentconfig change addr node-default SPI 259
# mipagentconfig change addr node-default Pool 3
# mipagentconfig change addr 10.68.30.36 Type agent
# mipagentconfig change addr 10.68.30.36 SPI 260
```

▼ Cómo agregar o eliminar parámetros del archivo de configuración

- 1 **Asuma la función de administrador principal, o conviértase en superusuario, en el sistema en el que quiera activar IP móvil.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Escriba el comando correspondiente para cada etiqueta que quiera agregar o eliminar en la sección designada:**

- Para la sección General, utilice el siguiente comando:

```
# mipagentconfig [add | delete] <label> <value>
```

- Para la sección Advertisements, utilice el siguiente comando:

```
# mipagentconfig [add | delete] adv device-name <label> <value>
```

Nota – Para agregar una interfaz, escriba lo siguiente:

```
# mipagentconfig add adv device-name
```

En este caso se asignan a la interfaz valores predeterminados (tanto para el agente externo como para el interno).

- Para la sección GlobalSecurityParameters, utilice el siguiente comando:

```
# mipagentconfig [add | delete] <label> <value>
```

- Para la sección Pool, utilice el siguiente comando:

```
# mipagentconfig [add | delete] Pool pool-identifier <label> <value>
```

- Para la sección SPI, utilice el siguiente comando:

```
# mipagentconfig [add | delete] SPI SPI-identifier <label> <value>
```

- Para la sección Address, utilice el siguiente comando:

```
# mipagentconfig [add | delete] addr [NAI | IP-address | node-default] \
<label> <value>
```

Nota – No cree secciones Advertisements, Pool , SPI y Address idénticas.

Ejemplo 28–7 Modificación de parámetros de archivo

Por ejemplo, para crear una nueva agrupación de direcciones, Pool 11, con una dirección base de 192.167.1.1 y un tamaño de 100, utilice estos comandos.

```
# mipagentconfig add Pool 11 BaseAddress 192.167.1.1
# mipagentconfig add Pool 11 size 100
```

Ejemplo 28–8 Eliminación de SPI

En el ejemplo siguiente se muestra cómo eliminar el parámetro de seguridad SPI SPI 257.

```
# mipagentconfig delete SPI 257
```

▼ **Cómo mostrar los valores actuales de los parámetros del archivo de configuración**

Se puede utilizar el comando `mipagentconfig get` para mostrar los valores actuales asociados con los destinos de los parámetros.

- 1 **Asuma la función de Administrador principal, o conviértase en superusuario, en el sistema en el que quiera activar IP móvil.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

- 2 **Escriba el comando siguiente para cada uno de los parámetros cuyo valor quiera mostrar:**

```
# mipagentconfig get [<parameter> | <label>]
```

Por ejemplo, si quiere mostrar los valores de anuncio del dispositivo `hme0`, utilice el siguiente comando:

```
# mipagentconfig get adv hme0
```

El resultado del comando será una pantalla similar a la siguiente:

```
[Advertisements hme0]
  HomeAgent = yes
  ForeignAgent = yes
```

Ejemplo 28-9 Uso del comando `mipagentconfig get` para mostrar valores de parámetros

En el ejemplo siguiente se muestra el resultado del uso del comando `mipagentconfig get` con otros destinos de parámetros.

```
# mipagentconfig get MaxClockSkew
[GlobalSecurityParameters]
MaxClockSkew=300

# mipagentconfig get HA-FAauth
[GlobalSecurityParameters]
HA-FAauth=no

# mipagentconfig get MN-FAauth
[GlobalSecurityParameters]
MN-FAauth=no

# mipagentconfig get Challenge
[GlobalSecurityParameters]
Challenge=no

# mipagentconfig get Pool 10
[Pool 10]
BaseAddress=192.168.1.1
Size=100

# mipagentconfig get SPI 257
[SPI 257]
Key=11111111111111111111111111111111
ReplayMethod=none

# mipagentconfig get SPI 258
[SPI 258]
Key=15111111111111111111111111111111
ReplayMethod=none

# mipagentconfig get addr 10.1.1.1
[Address 10.1.1.1]
SPI=258
Type=agent

# mipagentconfig get addr 192.168.1.200
[Address 192.168.1.200]
SPI=257
Type=node
```

Presentación del estado del agente de movilidad

Puede utilizar el comando `mipagentstat` para mostrar la lista de visitantes del agente externo y la tabla de enlace del agente interno. En [“Estado de un agente de movilidad de IP para móviles” en la página 744](#) se ofrece una descripción conceptual del uso del comando `mipagentstat`. También puede consultar la página de comando `man mipagentstat(1M)`.

▼ Cómo mostrar el estado del agente de movilidad

1 Conviértase en superusuario o asuma una función equivalente en el sistema en el que va a activar IP móvil.

Las funciones incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre las funciones, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

2 Muestre el estado del agente de movilidad.

- # mipagentstat options
- f Muestra la lista de nodos móviles activos en la lista de visitantes del agente externo.
 - h Muestra la lista de nodos móviles activos en la tabla de enlace del agente interno.
 - p Muestra la lista de asociaciones de seguridad con los agentes de movilidad equivalentes de un agente.

Ejemplo 28–10 Presentación del estado del agente de movilidad

En este ejemplo se indica cómo mostrar la lista de visitantes de todos los nodos móviles registrados con un agente externo.

mipagentstat -f

El resultado será una pantalla similar a la siguiente:

Mobile Node	Home Agent	Time (s) Granted	Time (s) Remaining	Flags
-----	-----	-----	-----	-----
foobar.xyz.com	ha1.xyz.com	600	125T.
10.1.5.23	10.1.5.1	1000	10T.

El resultado será una pantalla similar a la siguiente:

Foreign Agent Security Association(s).....			
	Requests	Replies	FTunnel	RTunnel
-----	-----	-----	-----	-----
forn-agent.eng.sun.com	AH	AH	ESP	ESP

En este ejemplo se indica cómo mostrar las asociaciones de seguridad de un agente interno.

mipagentstat -fp

El resultado será una pantalla similar a la siguiente:

Home Agent Security Association(s)			
	Requests	Replies	FTunnel	RTunnel

home-agent.eng.sun.com	AH	AH	ESP	ESP
ha1.xyz.com	AH,ESP	AH	AH,ESP	AH,ESP

Presentación de las rutas de movilidad de un agente externo

Utilice el comando `netstat` para mostrar información adicional acerca de rutas específicas de cada origen creadas mediante túneles directos e inversos. Para más información acerca de este comando consulte la página de comando `man netstat(1M)`.

▼ Cómo mostrar las rutas de movilidad de un agente externo

- 1

Conviértase en superusuario o asuma una función equivalente en el sistema en el que va a activar IP móvil.

Las funciones incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre las funciones, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)
- 2

Muestre las rutas de movilidad.

```
# netstat -rn
```

Ejemplo 28–11 Presentación de las rutas de movilidad de un agente externo

En el ejemplo siguiente se muestran las rutas para un agente externo que utiliza un túnel inverso.

Routing Table:	IPv4 Source-Specific				
Destination	In If	Source	Gateway	Flags	Use Out If
10.6.32.11	ip.tun1	--	10.6.32.97	UH	0 hme1
--	hme1	10.6.32.11	--	U	0 ip.tun1

La primera línea indica que la dirección IP de destino `10.6.32.11` y la interfaz entrante `ip.tun1` seleccionan `hme1` como interfaz de reenvío de los paquetes. La línea siguiente indica que cualquier paquete que se origine desde la interfaz `hme1` y la dirección de origen `10.6.32.11` debe reenviarse a `ip.tun1`.

Archivos y comandos de IP para móviles (referencia)

En este capítulo se describen los componentes incluidos en la implementación de Solaris de IP para móviles. Para utilizar IP para móviles deberá en primer lugar crear el archivo de configuración de IP para móviles mediante los parámetros y comandos que se describen en este capítulo.

Este capítulo contiene la información siguiente:

- “Descripción general de la implementación de IP para móviles en Solaris” en la página 729
- “Archivo de configuración de IP para móviles” en la página 730
- “Configuración del agente de movilidad IP” en la página 743
- “Estado de un agente de movilidad de IP para móviles” en la página 744
- “Información de estado de IP para móviles” en la página 744
- “Extensiones de netstat para IP para móviles” en la página 745
- “Extensiones snoop de IP para móviles” en la página 745

Nota – La función IP móvil se suprime de las actualizaciones de Solaris 10 posteriores a Solaris 10 8/07.

Descripción general de la implementación de IP para móviles en Solaris

El software de agente de movilidad incorpora las funciones de agente interno y agente externo. El software de IP móvil de Solaris no ofrece un nodo móvil cliente. Únicamente se ofrece la funcionalidad de agente. Todas las redes compatibles con movilidad deben tener al menos un host estático (no móvil) que ejecute este software.

La implementación de IP para móviles en Solaris es compatible con las siguientes funciones RFC:

- RFC 1918, "Address Allocation for Private Internets" (<http://www.ietf.org/rfc/rfc1918.txt?number=1918>)
- RFC 2002, "IP Mobility Support" (Agent only) (<http://www.ietf.org/rfc/rfc2002.txt?number=2002>)
- RFC 2003, "IP Encapsulation Within IP" (<http://www.ietf.org/rfc/rfc2003.txt?number=2003>)
- RFC 2794, "Mobile IP Network Access Identifier Extension for IPv4" (<http://www.ietf.org/rfc/rfc2794.txt?number=2794>)
- RFC 3012, "Mobile IPv4 Challenge/Response Extensions" (<http://www.ietf.org/rfc/rfc3012.txt?number=3012>)
- RFC 3024, "Reverse Tunneling for Mobile IP" (<http://www.ietf.org/rfc/rfc3024.txt?number=3024>)

El protocolo de IP para móviles básico (RFC 2002) no resuelve el problema de distribución de claves ampliable y trata la distribución de claves como un problema ortogonal. El software IP para móviles de Solaris utiliza únicamente claves configuradas manualmente, que se especifican en un archivo de configuración.

Las siguientes funciones RFC no son compatibles con la implementación Solaris de IP para móviles:

- RFC 1701, "General Routing Encapsulation" (<http://www.ietf.org/rfc/rfc1701.txt?number=1701>)
- RFC 2004, "Minimal Encapsulation Within IP" (<http://www.ietf.org/rfc/rfc2004.txt?number=2004>)

Las siguientes funciones no son compatibles con la implementación Solaris de IP para móviles:

- El reenvío de tráfico de multidifusión o de difusión del agente interno al agente externo para un .n, que está visitando una red externa.
- El enrutamiento de datagramas de difusión y multidifusión a través de túneles inversos.
- Las direcciones de auxilio privadas o las direcciones de agente interno privadas.

Para obtener más información, consulte la página de comando `man mipagent(1M)`.

Archivo de configuración de IP para móviles

El comando `mipagent` lee información de configuración del archivo `/etc/inet/mipagent.conf` al inicio. IP para móviles utiliza el archivo de configuración `/etc/inet/mipagent.conf` para inicializar el agente de movilidad de IP para móviles. Al configurarlo e implantarlo, el agente de movilidad emite anuncios de enrutador periódicos y responde a mensajes de solicitud de enrutador, y a mensajes de registro de IP para móviles.

Consulte la página de comando `man mipagent.conf(4)` para ver una descripción de los atributos de archivo. Consulte la página de comando `man mipagent(1M)` para ver una descripción del uso de este archivo.

Formato del archivo de configuración

El archivo de configuración de IP para móviles está dividido en secciones. Cada sección tiene un nombre exclusivo escrito entre corchetes. Cada sección contiene una o más etiquetas. Para asignar valores a las etiquetas, utilice el siguiente formato:

```
[Section_name]
    Label-name = value-assigned
```

“[Secciones y etiquetas del archivo de configuración](#)” en la página 734 describe los nombres de sección, las etiquetas y los posibles valores.

Ejemplos de archivos de configuración

En la instalación predeterminada de Solaris se incluyen los siguientes archivos de configuración en el directorio `/etc/inet`:

- `mipagent.conf-sample` – Contiene un ejemplo de configuración para un agente de IP para móviles que ofrece funciones de agente externo e interno
- `mipagent.conf.fa-sample` – Contiene un ejemplo de configuración para un agente de IP para móviles que ofrece únicamente funciones de agente externo
- `mipagent.conf.ha-sample` – Contiene un ejemplo de configuración para un agente de IP para móviles que ofrece únicamente funciones de agente interno

Estos archivos de configuración de ejemplo contienen parámetros de dirección y seguridad de nodo móvil. Antes de poder implementar IP para móviles, se debe crear un archivo de configuración con el nombre `mipagent.conf` y situarlo en el directorio `/etc/inet`. Este archivo contiene los valores de configuración adecuados para los requisitos de su implementación de IP para móviles. También puede elegir uno de los archivos de configuración de ejemplo, modificarlo con sus valores de direcciones y seguridad y copiarlo en `/etc/inet/mipagent.conf`.

Para más información, consulte “[Creación del archivo de configuración de IP móvil](#)” en la página 715.

Archivomipagent.conf-sample

En el listado siguiente se muestran las secciones, etiquetas y valores que contiene el archivo `mipagent.conf-sample`. “[Secciones y etiquetas del archivo de configuración](#)” en la página 734 describe la sintaxis, secciones, etiquetas y valores.

```
[General]
    Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
```

```

HomeAgent = yes
ForeignAgent = yes
PrefixFlags = yes
AdvertiseOnBcast = yes
RegLifetime = 200
AdvLifetime = 200
AdvFrequency = 5
ReverseTunnel = no
ReverseTunnelRequired = no

[GlobalSecurityParameters]
MaxClockSkew = 300
HA-FAauth = yes
MN-FAauth = yes
Challenge = no
KeyDistribution = files

[Pool 1]
BaseAddress = 10.68.30.7
Size = 4

[SPI 257]
ReplayMethod = none
Key = 11111111111111111111111111111111

[SPI 258]
ReplayMethod = none
Key = 15111111111111111111111111111111

[Address 10.1.1.1]
Type = node
SPI = 258

[Address mobilenode@sun.com]
Type = node
SPI = 257
Pool = 1

[Address Node-Default]
Type = node
SPI = 258
Pool = 1

[Address 10.68.30.36]
Type = agent
SPI = 257

```

Archivo mipagent.conf.fa-sample

En el listado siguiente se muestran las secciones, etiquetas y valores que contiene el archivo mipagent.conf.fa-sample. [“Secciones y etiquetas del archivo de configuración” en la página 734](#) describe la sintaxis, secciones, etiquetas y valores.

El archivo mipagent.conf.fa-sample muestra una configuración que ofrece únicamente funciones de agente externo. Este archivo de ejemplo no contiene una sección Pool (Agrupación) porque las agrupaciones solo las emplean los agentes internos. Por lo demás, el archivo es idéntico a mipagent.conf.sample.

```
[General]
  Version = 1.0      # version number for the configuration file. (required)

[Advertisements hme0]
  HomeAgent = no
  ForeignAgent = yes
  PrefixFlags = yes
  AdvertiseOnBcast = yes
  RegLifetime = 200
  AdvLifetime = 200
  AdvFrequency = 5
  ReverseTunnel = yes
  ReverseTunnelRequired = no

[GlobalSecurityParameters]
  MaxClockSkew = 300
  HA-FAauth = yes
  MN-FAauth = yes
  Challenge = no
  KeyDistribution = files

[SPI 257]
  ReplayMethod = none
  Key = 11111111111111111111111111111111

[SPI 258]
  ReplayMethod = none
  Key = 15111111111111111111111111111111

[Address 10.1.1.1]
  Type = node
  SPI = 258

[Address 10.68.30.36]
  Type = agent
  SPI = 257
```

Archivo mipagent.conf.ha-sample

En el listado siguiente se muestran las secciones, etiquetas y valores que contiene el archivo `mipagent.conf.ha-sample`. “[Secciones y etiquetas del archivo de configuración](#)” en la [página 734](#) describe la sintaxis, secciones, etiquetas y valores.

El archivo `mipagent.conf.ha-sample` muestra una configuración que ofrece únicamente funciones de agente interno. Por lo demás, el archivo es idéntico a `mipagent.conf-sample`.

```
[General]
  Version = 1.0      # version number for the configuration file. (required)

[Advertisements hme0]
  HomeAgent = yes
  ForeignAgent = no
  PrefixFlags = yes
  AdvertiseOnBcast = yes
  RegLifetime = 200
  AdvLifetime = 200
```

```

AdvFrequency = 5
ReverseTunnel = yes
ReverseTunnelRequired = no

[GlobalSecurityParameters]
MaxClockSkew = 300
HA-FAuth = yes
MN-FAuth = yes
Challenge = no
KeyDistribution = files

[Pool 1]
BaseAddress = 10.68.30.7
Size = 4

[SPI 257]
ReplayMethod = none
Key = 11111111111111111111111111111111

[SPI 258]
ReplayMethod = none
Key = 15111111111111111111111111111111

[Address 10.1.1.1]
Type = node
SPI = 258

[Address mobilenode@sun.com]
Type = node
SPI = 257
Pool = 1

[Address Node-Default]
Type = node
SPI = 258
Pool = 1

```

Secciones y etiquetas del archivo de configuración

El archivo de configuración de IP para móviles se compone de las secciones siguientes:

- General (obligatoria)
- Advertisements (obligatoria)
- GlobalSecurityParameters (opcional)
- Pool (opcional)
- SPI (opcional)
- Address (opcional)

Las secciones General y GlobalSecurityParameters contienen información relativa al funcionamiento del agente de IP para móviles. Estas secciones solo pueden aparecer una vez en el archivo de configuración.

Sección General

La sección General sólo contiene una etiqueta: el número de versión del archivo de configuración. La sintaxis de la sección General es la siguiente:

```
[General]
Version = 1.0
```

Sección Advertisements

La sección Advertisements contiene las etiquetas HomeAgent y ForeignAgent y otras. Se debe incluir una sección Advertisements distinta para cada interfaz del host local que ofrezca servicios de IP para móviles. La sintaxis de la sección Advertisements es la siguiente:

```
[Advertisements interface]
HomeAgent = <yes/no>
ForeignAgent = <yes/no>
.
.
```

Generalmente, un sistema tiene una única interfaz, por ejemplo eri0 o hme0, y admite operaciones de agente interno y de agente externo. Si se da esta situación para el ejemplo hme0, el valor yes se asigna a las etiquetas HomeAgent y ForeignAgent, como se indica a continuación:

```
[Advertisements hme0]
HomeAgent = yes
ForeignAgent = yes
.
.
```

Para anuncios a través de interfaces dinámicas, utilice '*' en la parte de ID de dispositivo. Por ejemplo, *nombre_interfaz* ppp* implica en realidad que se han iniciado todas las interfaces PPP configuradas después del daemon mipagent. Todos los atributos de la sección Advertisements de una interfaz dinámica permanecen iguales.

En la tabla siguiente se describen las etiquetas y los valores que se pueden utilizar en la sección Advertisements.

TABLA 29-1 Etiquetas y valores en la sección Advertisements

Etiqueta	Valor	Descripción
HomeAgent	yes o no	Determina si el daemon mipagent proporciona funcionalidad de agente interno.
ForeignAgent	yes o no	Determina si el daemon mipagent proporciona funcionalidad de agente externo.
PrefixFlags	yes o no	Especifica si los anuncios incluyen la extensión prefix-length opcional.

TABLA 29-1 Etiquetas y valores en la sección Advertisements (Continuación)

Etiqueta	Valor	Descripción
AdvertiseOnBcast	yes o no	Si es yes, los anuncios se envían por 255 . 255 . 255 . 255, en lugar de por 224 . 0 . 0 . 1.
RegLifetime	n	Valor de periodo de vida máximo aceptado en las solicitudes de registro, en segundos.
AdvLifetime	n	Periodo de tiempo máximo que el anuncio se considera válido en ausencia de otros anuncios, en segundos.
AdvFrequency	n	Tiempo entre dos anuncios consecutivos, en segundos.
ReverseTunnel	yes o noFA o HA o both	Determina si mipagent ofrece la función de túnel inverso. El valor yes implica que tanto el agente externo como el interno admiten túnel inverso. El valor no significa que la interfaz no admite túnel inverso. El valor FA significa que el agente externo admite túnel inverso. El valor HA significa que el agente interno admite túnel inverso. El valor both implica que tanto el agente externo como el interno admiten túnel inverso.
ReverseTunnelRequired	yes o no	Determina si mipagent requiere la función de túnel inverso. En consecuencia, determina si un nodo móvil debe solicitar un túnel inverso durante el registro. El valor yes implica que tanto el agente externo como el interno requieren túnel inverso. El valor no significa que la interfaz no requiere túnel inverso. El valor FA significa que el agente externo requiere un túnel inverso. El valor HA significa que el agente interno requiere un túnel inverso.
AdvInitCount	n	Determina el número inicial de anuncios no solicitados. El valor predeterminado es 1. Este valor sólo es significativo si AdvLimitUnsolicited es yes.
AdvLimitUnsolicited	yes o no	Activa o desactiva un número limitado de anuncios no solicitados a través de la interfaz de movilidad.

Sección GlobalSecurityParameters

La sección GlobalSecurityParameters contiene las etiquetas maxClockSkew, HA -FAauth, MN -FAauth, Challenge y KeyDistribution. La sintaxis de la sección es la siguiente:


```
[GlobalSecurityParameters]
  MaxClockSkew = n
  HA-FAauth = <yes/no>
  MN-FAauth = <yes/no>
  Challenge = <yes/no>
  KeyDistribution = files
```

El protocolo IP para móviles ofrece protección de repetición de mensajes por el procedimiento de permitir la presencia de marcas de tiempo en los mensajes. Si las horas difieren, el agente interno devuelve un error al nodo móvil con la hora actual y el nodo puede volver a registrarse utilizando la hora actual. La etiqueta `MaxClockSkew` se utiliza para configurar el número máximo de segundos de diferencia entre los relojes del agente interno y del agente externo. El valor predeterminado es de 300 segundos.

Las etiquetas `HA-FAauth` y `MN-FAauth` activan o desactivan el requisito de autenticación interna-externa o móvil-externa, respectivamente. El valor predeterminado es desactivado. La etiqueta `challenge` se utiliza para que el agente externo emita desafíos al nodo móvil en sus anuncios. La etiqueta se usa para protección de repetición. El valor predeterminado es también desactivado.

En la tabla siguiente se describen las etiquetas y los valores que se pueden utilizar en la sección `GlobalSecurityParameters`.

TABLA 29–2 Etiquetas y valores de la sección `GlobalSecurityParameters`

Etiqueta	Valor	Descripción
<code>MaxClockSkew</code>	<code>n</code>	Número de segundos que <code>mipagent</code> acepta como diferencia entre su propia hora local y la encontrada en las solicitudes de registro
<code>HA-FAauth</code>	<code>yes</code> o <code>no</code>	Especifica si deben estar presentes las extensiones de autenticación de agente interno-agente externo en las solicitudes y respuestas de registro
<code>MN-FAauth</code>	<code>yes</code> o <code>no</code>	Especifica si deben estar presentes las extensiones de autenticación de nodo móvil-agente externo en las solicitudes y respuestas de registro
<code>Challenge</code>	<code>yes</code> o <code>no</code>	Especifica si el agente externo incluye desafíos en sus anuncios de movilidad
<code>KeyDistribution</code>	<code>files</code>	Se le debe asignar el valor <code>files</code>

Sección `Pool`

El agente interno puede asignar a los nodos móviles direcciones dinámicas. La asignación de direcciones dinámicas se lleva a cabo mediante el daemon `mipagent` de forma independiente de DHCP. Se puede crear una agrupación de direcciones que los nodos móviles pueden utilizar mediante la solicitud de una dirección permanente. Las agrupaciones de direcciones se configuran mediante la sección `Pool` del archivo de configuración.

La sección `Pool` contiene las etiquetas `BaseAddress` y `Size`. La sintaxis de la sección `Pool` es la siguiente:

```
[Pool pool-identifier]  
  BaseAddress = IP-address  
  Size = size
```

Nota – Si utiliza un identificador `Pool`, también deberá estar en la sección `Address` del nodo móvil.

La sección `Pool` se utiliza para definir agrupaciones de direcciones que se pueden asignar a los nodos móviles. La etiqueta `BaseAddress` se utiliza para establecer la primera dirección IP de la agrupación. La etiqueta `Size` se utiliza para especificar el número de direcciones disponibles en la agrupación.

Por ejemplo, si las direcciones IP `192.168.1.1` a `192.168.1.100` están reservadas en la agrupación 10, la entrada de la sección `Pool` será la siguiente:

```
[Pool 10]  
  BaseAddress = 192.168.1.1  
  Size = 100
```

Nota – Los intervalos de direcciones no deben abarcar la dirección de difusión. Por ejemplo, no se debe asignar `BaseAddress = 192.168.1.200` y `Size = 60`, porque este rango abarca la dirección de difusión `192.168.1.255`.

En la tabla siguiente se describen las etiquetas y valores que se utilizan en la sección `Pool`.

TABLA 29–3 Etiquetas y valores de la sección `Pool`

Etiqueta	Valor	Descripción
BaseAddress	n.n.n.n	Primera dirección de la agrupación de direcciones
Size	n	Número de direcciones de la agrupación

Sección SPI

El protocolo de IP para móviles requiere autenticación de mensajes, por lo tanto se debe identificar el contexto de seguridad mediante el índice de parámetros de seguridad (SPI). El contexto de seguridad se define en la sección `SPI`. Se debe incluir una sección `SPI` distinta para cada contexto de seguridad definido. El contexto de seguridad se identifica con un código numérico. El protocolo IP para móviles reserva los primeros 256 SPI. Por lo tanto, sólo debe utilizar valores SPI superiores a 256. En la sección `SPI` se puede encontrar información relacionada con la seguridad, como secretos compartidos y protección de repetición.

La sección SPI contiene también las etiquetas `ReplayMethod` y `Key`. La sintaxis de la sección SPI es la siguiente:

```
[SPI SPI-identifier
  ReplayMethod = <none/timestamps>
  Key = key
```

Dos equivalentes que se comuniquen deben compartir el mismo identificador SPI. Es necesario configurarlos con la misma clave y método de repetición. La clave se especifica en forma de cadena de dígitos hexadecimales. La longitud máxima es de 16 bytes. Por ejemplo, si la clave tiene una longitud de 16 bytes y contiene los valores hexadecimales 0 a f, el aspecto de la cadena de la clave será similar a:

```
Key = 0102030405060708090a0b0c0d0e0f10
```

El número de dígitos de las claves debe ser par, para corresponderse con la representación de dos dígitos por byte.

En la tabla siguiente se describen las etiquetas y valores que se pueden utilizar en la sección SPI.

TABLA 29-4 Etiquetas y valores de la sección SPI

Etiqueta	Valor	Descripción
ReplayMethod	none o timestamps	Especifica el tipo de autenticación de repetición que se utiliza para el SPI
Key	x	Clave de autenticación en hexadecimal

Sección Address

La implementación de Solaris de IP para móviles permite configurar los nodos móviles con tres métodos posibles. Cada método se configura en la sección `Address`. El primer método sigue el protocolo IP para móviles tradicional, y exige que cada nodo móvil tenga una dirección permanente. El segundo método permite identificar un nodo móvil mediante su Identificador de acceso de red (NAI). El último método permite configurar un nodo móvil *predeterminado*, que puede utilizar cualquier nodo móvil que tenga el valor de SPI adecuado y el material de clave relacionado.

Nodo móvil

La sección `Address` de un nodo móvil contiene las etiquetas `Type` y `SPI`, que definen el tipo de dirección y el identificador SPI. La sintaxis de la sección `Address` es la siguiente:

```
[Address address
  Type = node
  SPI = SPI-identifier
```

Se debe incluir una sección `Address` en el archivo de configuración de un agente interno por cada nodo para móviles que se admita.

Si se exige autenticación de mensajes de IP para móviles entre el agente externo y el agente interno, se debe incluir una sección `Address` por cada equivalente con el que un agente necesita comunicarse.

El valor de SPI configurado debe representar una sección SPI que esté presente en el archivo de configuración.

También puede configurar direcciones privadas para un nodo móvil.

En la tabla siguiente se describen las etiquetas y los valores que se pueden utilizar en la sección `Address` de un nodo móvil.

TABLA 29-5 Etiquetas y valores de la sección `Address` (nodo móvil)

Etiqueta	Valor	Descripción
Type	nodo	Especifica que la entrada es para un nodo móvil
SPI	n	Especifica el valor de SPI para la entrada asociada

Agente de movilidad

La sección `Address` de un agente de movilidad contiene las etiquetas `Type` y `SPI`, que definen el tipo de dirección y el identificador SPI. La sección `Address` de un agente de movilidad presenta la siguiente sintaxis:

```
[Address address]
  Type = agent
  SPI = SPI-identifier
```

Se debe incluir una sección `Address` en el archivo de configuración de un agente interno por cada agente de movilidad que se admita.

Si se requiere autenticación de mensajes IP entre los agentes interno y externo, debe incluirse una sección `Address` para cada equivalente con el que un agente desee comunicarse.

El valor de SPI configurado debe representar una sección SPI que esté presente en el archivo de configuración.

En la tabla siguiente se describen las etiquetas y valores que se pueden utilizar en la sección `Address` de un agente de movilidad.

TABLA 29-6 Etiquetas y valores de la sección `Address` (agente de movilidad)

Etiqueta	Valor	Descripción
Type	agent	Especifica que la entrada corresponde a un agente de movilidad

TABLA 29-6 Etiquetas y valores de la sección Address (agente de movilidad) *(Continuación)*

Etiqueta	Valor	Descripción
SPI	n	Especifica el valor de SPI para la entrada asociada

Nodo móvil identificado por su NAI

La sección Address para un nodo móvil identificado mediante su NAI contiene las etiquetas Type, SPI y Pool. El parámetro NAI permite identificar nodos móviles a través de su NAI. La sintaxis de la sección Address con el parámetro NAI es la siguiente:

```
[Address NAI]
    Type = Node
    SPI = SPI-identifier
    Pool = pool-identifier
```

Para utilizar agrupaciones, los nodos móviles se deben identificar mediante su NAI. La sección Address permite configurar un NAI, en lugar de una dirección permanente. Un NAI tiene el formato usuario@dominio. La etiqueta Pool se utiliza para especificar la agrupación de direcciones que se debe utilizar para asignar la dirección permanente al nodo móvil.

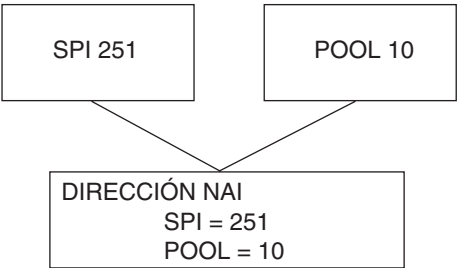
En la tabla siguiente se describen las etiquetas y los valores que se pueden utilizar en la sección Address para un nodo móvil identificado por su NAI.

TABLA 29-7 Etiquetas y valores de la sección Address (nodo móvil identificador por su NAI)

Etiqueta	Valor	Descripción
Type	nodo	Especifica que la entrada es para un nodo móvil
SPI	n	Especifica el valor de SPI para la entrada asociada
Pool	n	Asigna la agrupación desde la que se asigna una dirección a un nodo móvil

Deberá tener secciones SPI y Pool correspondientes a las etiquetas SPI y Pool definidas en una sección Address con un nodo móvil identificado por su NAI, como se muestra en la figura siguiente.

FIGURA 29-1 Secciones SPI y Pool correspondientes para la sección Address en un nodo móvil identificado por su NAI



Nodo móvil predeterminado

La sección Address para un nodo móvil predeterminado contiene las etiquetas Type, SPI y Pool. Con el parámetro Node-Default se puede dar permiso para que todos los nodos móviles obtengan servicio si tienen el SPI correcto (definido en esta sección). La sintaxis de la sección Address con el parámetro Node-Default es la siguiente:

```
[Address Node-Default]
  Type = Node
  SPI = SPI-identifier
  Pool = pool-identifier
```

El parámetro Node-Default permite reducir el tamaño del archivo de configuración. En caso contrario, cada nodo móvil necesitaría su propia sección. Sin embargo, el parámetro Node-Default implica un riesgo de seguridad. Si un nodo móvil deja de ser de confianza, es necesario actualizar la información de seguridad en todos los nodos móviles de confianza. Se trata de una tarea muy tediosa. Sin embargo, se puede utilizar el parámetro Node-Default en redes en las que los riesgos de seguridad no tienen importancia.

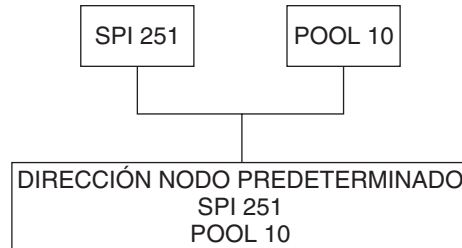
En la tabla siguiente se describen las etiquetas y valores que se pueden utilizar en la sección Address para un nodo móvil predeterminado.

TABLA 29-8 Etiquetas y valores de la sección Address (nodo móvil predeterminado)

Etiqueta	Valor	Descripción
Type	nodo	Especifica que la entrada es para un nodo móvil
SPI	n	Especifica el valor de SPI para la entrada asociada
Pool	n	Asigna la agrupación desde la que se asigna una dirección a un nodo móvil

Deberá tener secciones SPI y Pool correspondientes a las etiquetas SPI y Pool definidas en una sección Address con un nodo móvil predeterminado, como se muestra en la figura siguiente.

FIGURA 29-2 Secciones SPI y Pool correspondientes para la sección Address en un nodo móvil predeterminado



Configuración del agente de movilidad IP

El comando `mipagentconfig` es apto para configurar el agente de movilidad. Este comando permite crear o modificar cualquier parámetro del archivo de configuración `/etc/inet/mipagent.conf`. Específicamente, se puede modificar cualquier configuración. También se pueden agregar o eliminar clientes de movilidad, agrupaciones y SPI. La sintaxis del comando `mipagentconfig` es la siguiente:

```
# mipagentconfig <command> <parameter> <value>
```

En la tabla siguiente se describen todos los comandos que se pueden utilizar con `mipagentconfig` para crear o modificar parámetros en el archivo de configuración `/etc/inet/mipagent.conf`.

TABLA 29-9 Subcomandos de `mipagentconfig`

Orden	Descripción
add	Se utiliza para agregar parámetros de anuncio, de seguridad, SPI y direcciones al archivo de configuración
change	Se utiliza para modificar parámetros de anuncio, de seguridad, SPI y direcciones en el archivo de configuración
delete	Se utiliza para eliminar parámetros de anuncio, de seguridad, SPI y direcciones del archivo de configuración
get	Se utiliza para mostrar los valores actuales del archivo de configuración

Consulte la página del comando `man mipagentconfig(1M)` para ver una descripción de los parámetros de los comandos y de los valores que pueden adquirir. En [“Modificación del archivo de configuración de IP móvil” en la página 719](#) se detallan procedimientos que utilizan el comando `mipagentconfig`.

Estado de un agente de movilidad de IP para móviles

El comando `mipagentstat` se utiliza para obtener una lista de visitantes de agente externo y una tabla de enlace de agente interno. También se pueden mostrar las asociaciones de seguridad con los agentes de movilidad equivalentes de un agente. Para mostrar la lista de visitantes del agente externo se debe utilizar el comando `mipagentstat` con la opción `-f`. Para mostrar la tabla de enlace del agente interno se debe utilizar el comando `mipagentstat` con la opción `-h`. En los ejemplos siguientes se muestran pantallas de salida típicas del comando `mipagentstat` con las opciones mencionadas.

EJEMPLO 29-1 Lista de visitantes de agente externo

Mobile Node	Home Agent	Time (s) Granted	Time (s) Remaining	Flags
-----	-----	-----	-----	-----
foobar.xyz.com	ha1.xyz.com	600	125T.
10.1.5.23	10.1.5.1	1000	10T.

EJEMPLO 29-2 Tabla de enlace de agente interno

Mobile Node	Home Agent	Time (s) Granted	Time (s) Remaining	Flags
-----	-----	-----	-----	-----
foobar.xyz.com	fa1.tuv.com	600	125T.
10.1.5.23	123.2.5.12	1000	10T.

Consulte la página de comando `man mipagentstat(1M)` para obtener más información sobre las opciones del comando. En [“Presentación del estado del agente de movilidad” en la página 725](#) se detallan procedimientos que utilizan el comando `mipagentstat`.

Información de estado de IP para móviles

Al cerrarse, el daemon `mipagent` almacena la información de estado interna en `/var/inet/mipagent_state`. Esto ocurre cuando `mipagent` ofrece servicios como agente interno. Esta información de estado incluye la lista de nodos móviles a los que ofrece servicio como agente interno, sus direcciones de auxilio actuales y los tiempos de registro restantes. En esta información se incluye también la configuración de asociación de seguridad con los agentes de movilidad equivalentes. Si el daemon `mipagent` se cierra por mantenimiento y luego se reinicia, `mipagent_state` se utiliza para volver a crear el estado interno del agente de movilidad con la máxima fidelidad posible. La intención es minimizar la interrupción de servicio en los nodos móviles que pueden estar visitando otras redes. Si existe `mipagent_state`, se lee inmediatamente después de `mipagent.conf` cada vez que se inicia o reinicia `mipagent`.

Extensiones de netstat para IP para móviles

Se han agregado extensiones para IP para móviles al comando `netstat` para identificar rutas de reenvío de IP para móviles. En concreto, se puede utilizar el comando `netstat` para mostrar una nueva tabla de enrutamiento denominada "Source-Specific". Consulte la página de comando `man netstat(1M)` para obtener más información.

En el ejemplo siguiente se muestra la salida de `netstat` cuando se utilizan los indicadores `-nr`.

EJEMPLO 29-3 Salida de IP para móviles del comando `netstat`

Routing Table:	IPv4	Source-Specific				
Destination	In If	Source	Gateway	Flags	Use	Out If
-----	-----	-----	-----	-----	-----	-----
10.6.32.11	ip.tun1	--	10.6.32.97	UH	0	hme1
--	hme1	10.6.32.11	--	U	0	ip.tun1

En el ejemplo se muestran las rutas para un agente externo que utiliza un túnel inverso. La primera línea indica que la dirección IP de destino `10.6.32.11` y la interfaz entrante `ip.tun1` seleccionan `hme1` como interfaz de reenvío de los paquetes. La siguiente línea indica que todos los paquetes con origen en la interfaz `hme1` y la dirección de origen `10.6.32.11` deben reenviarse a `ip.tun1`.

Extensiones snoop de IP para móviles

Se han agregado extensiones para IP para móviles al comando `snoop` para identificar el tráfico de IP para móviles en el enlace. Consulte la página de comando `man snoop(1M)` para obtener más información.

En el ejemplo siguiente se muestra la salida de `snoop` que se ejecuta en el nodo móvil `mip-mn2`.

EJEMPLO 29-4 Salida de IP para móviles del comando `snoop`

```
mip-mn2# snoop
Using device /dev/hme (promiscuous mode)
mip-fa2 -> 224.0.0.1 ICMP Router advertisement (Lifetime 200s [1]:
{mip-fa2-80 2147483648}), (Mobility Agent Extension), (Prefix Lengths),
(padding)
mip-mn2 -> mip-fa2 Mobile IP reg rqst
mip-fa2 -> mip-mn2 Mobile IP reg reply (OK code 0)
```

En este ejemplo se muestra que el nodo móvil ha recibido uno de los anuncios de agente de movilidad enviados periódicamente desde el agente externo, `mip-fa2`. A continuación, `mip-mn2` ha enviado una solicitud de registro a `mip-fa2` y, a cambio, ha recibido una respuesta de registro. En la respuesta se indica que el nodo móvil se ha registrado satisfactoriamente con su agente interno.

P A R T E V I

IPMP

Esta parte introduce las múltiples rutas de redes IP (IPMP) y contiene las tareas necesarias para administrar IPMP. IPMP proporciona funciones de detección de fallos y conmutación por error para las interfaces de un sistema que están conectadas al mismo vínculo.

Introducción a IPMP (descripción general)

Las múltiples rutas de redes IP (IPMP) detectan los fallos en la interfaz física y conmutan por error el acceso a la red de forma transparente para un sistema con varias interfaces en el mismo vínculo IP. IPMP también permite repartir la carga de los paquetes para los sistemas con varias interfaces.

Este capítulo contiene la información siguiente:

- “Por qué debe utilizar IPMP” en la página 749
- “Requisitos básicos de IPMP” en la página 753
- “Direcciones IPMP” en la página 754
- “Componentes IPMP de Oracle Solaris” en la página 750
- “Configuraciones de interfaces IPMP” en la página 757
- “Funciones de detección de fallos IPMP y recuperación” en la página 758
- “IPMP y reconfiguración dinámica” en la página 763

Para conocer las tareas de configuración de IPMP, consulte el [Capítulo 31, “Administración de IPMP \(tareas\)”](#).

Por qué debe utilizar IPMP

IPMP ofrece una mayor fiabilidad, disponibilidad y rendimiento de la red para los sistemas con múltiples interfaces físicas. Ocasionalmente, una interfaz física o el hardware de red conectado a la interfaz podrían fallar o requerir mantenimiento. Por norma general, en ese punto, ya no es posible contactar con el sistema mediante cualquiera de las direcciones IP que están asociadas con la interfaz fallida. Asimismo, se interrumpe cualquier conexión con el sistema que utilice dichas direcciones IP.

Gracias a IPMP, puede configurar una o más interfaces físicas en un grupo de múltiples rutas IP o *grupo IPMP*. Después de configurar IPMP, el sistema supervisa automáticamente las interfaces del grupo IPMP para detectar posibles errores. Si falla una interfaz del grupo o se elimina para fines de mantenimiento, IPMP migra automáticamente o *hace que fallen* las

direcciones IP de la interfaz fallida. El destinatario de estas direcciones es una interfaz en funcionamiento del grupo IPMP de la interfaz fallida. La función de conmutación tras error de IPMP mantiene la conectividad e impide la interrupción de cualquier conexión. Asimismo, IPMP mejora el rendimiento global de la red al expandir automáticamente el tráfico de la red por un conjunto de interfaces del grupo IPMP. Este proceso se denomina *expansión de carga*.

Componentes IPMP de Oracle Solaris

IPMP de Oracle Solaris implica el siguiente software:

- El daemon `in.mpathd`, que se describe detalladamente en la página del comando `man in.mpathd(1M)`.
- El archivo de configuración `/etc/default/mpathd`, que también se describe en la página del comando `man in.mpathd(1M)`.
- Opciones `ifconfig` para la configuración de IPMP, tal como se describe en la página del comando `man ifconfig(1M)`.

Daemon de múltiples rutas, `in.mpathd`

El daemon `in.mpathd` detecta los fallos de la interfaz y, a continuación, implementa varios procedimientos para la conmutación y recuperación tras error. Si `in.mpathd` detecta un fallo o una reparación, el daemon envía un comando `ioctl` para llevar a cabo la conmutación o recuperación tras error. El módulo de núcleo `ip`, que implementa `ioctl`, lleva a cabo la conmutación por error de acceso de red de modo transparente y automático.

Nota – No utilice las rutas alternativas si utiliza IPMP en el mismo conjunto de tarjetas de interfaz de red. Tampoco debe utilizar IPMP mientras utiliza las rutas alternativas. Puede utilizar las rutas alternativas e IPMP de forma simultánea en diferentes conjuntos de interfaces. Para obtener más información sobre las rutas alternativas, consulte *Sun Enterprise Server Alternate Pathing 2.3.1 User Guide*.

El daemon `in.mpathd` detecta fallos y reparaciones enviando sondeos a todas las interfaces que forman parte de un grupo IPMP. El daemon `in.mpathd` también detecta fallos y reparaciones supervisando el indicador `RUNNING` en cada interfaz del grupo. Consulte la página del comando `man in.mpathd(1M)` para obtener más información.

Nota – No se admite DHCP para administrar direcciones de datos IPMP. Si intenta utilizar DHCP en estas direcciones, DHCP finalmente abandonará el control de dichas direcciones. No utilice DHCP en las direcciones de datos.

Terminología y conceptos de IPMP

En esta sección se introducen los términos y conceptos que se utilizan en los capítulos sobre IPMP de esta guía.

Vínculo IP

En terminología IPMP, un *vínculo IP* es una utilidad de comunicación o medio a través del cual los nodos se pueden comunicar en la capa del vínculo de datos del conjunto de protocolos de Internet. Los tipos de vínculos IP podrían incluir redes Ethernet simples, Ethernet con puente, concentradores o redes de modalidad de transferencia asíncrona (ATM). Un vínculo IP puede tener uno o más números de subred IPv4 y, si es preciso, uno o más prefijos de subred IPv6. No se puede asignar el mismo número o prefijo de subred a más de un vínculo IP. En ATM LANE, un vínculo IP es una sola red de área local (LAN) emulada. Con el protocolo de resolución de direcciones (ARP), el alcance del protocolo ARP es un único vínculo IP.

Nota – Otros documentos relacionados con IP, como RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, utilizan el término *vínculo* en lugar de *vínculo IP*. La parte VI utiliza el término *vínculo IP* para evitar la confusión con IEEE 802. En IEEE 802, *vínculo* hace referencia a una única conexión entre una tarjeta de interfaz de red Ethernet (NIC) y un conmutador Ethernet.

Interfaz física

La *interfaz física* proporciona una conexión del sistema con un vínculo IP. Esta conexión se suele implementar como un controlador de dispositivos y una NIC. Si un sistema tiene varias interfaces conectadas al mismo vínculo, puede configurar IPMP para que lleve a cabo la conmutación por error si falla una de las interfaces. Para obtener más información sobre las interfaces físicas, consulte “[Configuraciones de interfaces IPMP](#)” en la [página 757](#).

Tarjeta de interfaz de red

Una *tarjeta de interfaz de red* es un adaptador de red que se puede integrar en el sistema. Una NIC también puede ser una tarjeta independiente que actúe como interfaz de un sistema a un vínculo IP. Algunas NIC pueden tener varias interfaces físicas. Por ejemplo, una NIC que puede tener cuatro interfaces, de qfe0 a qfe3, etc.

Grupo IPMP

Un grupo de múltiples rutas IP, o grupo *IPMP*, se compone de una o más interfaces físicas en el mismo sistema configuradas con el mismo nombre de grupo IPMP. Todas las interfaces del grupo IPMP deben estar conectadas al mismo vínculo IP. El mismo nombre de grupo IPMP de cadena de caracteres (no nula) identifica a todas las interfaces del grupo. Puede colocar interfaces de NIC de diferentes velocidades en el mismo grupo IPMP, siempre que las NIC sean

del mismo tipo. Por ejemplo, en el mismo grupo puede configurar las interfaces de NIC Ethernet de 100 megabits y las interfaces de NIC Ethernet de 1 gigabit. A modo de ejemplo, supongamos que tiene dos tarjetas NIC Ethernet de 100 megabits. Puede configurar una de las interfaces con 10 megabits y seguir colocando las dos interfaces en el mismo grupo IPMP.

No es posible colocar dos interfaces de distintos tipos de medios en un grupo IPMP. Por ejemplo, no puede colocar una interfaz ATM en el mismo grupo que una interfaz Ethernet.

Detección de fallos y conmutación por error

La *detección de fallos* es el proceso de detectar si una interfaz o su ruta a un dispositivo de capa de Internet han dejado de funcionar. IPMP ofrece a los sistemas la posibilidad de detectar si una interfaz ha fallado. IPMP detecta los siguientes tipos de fallos de comunicación:

- La ruta de transmisión o recepción de la interfaz han fallado.
- La conexión de la interfaz al vínculo IP está inactiva.
- El puerto del conmutador no transmite ni recibe paquetes.
- La interfaz física de un grupo IPMP no está presente en el inicio del sistema.

Tras detectar un fallo, IPMP inicia la conmutación por error. La *conmutación por error* es el proceso automático de conmutar el acceso de red de una interfaz fallida a una interfaz física que funcione del mismo grupo. El acceso a red incluye unidifusión, multidifusión y tráfico de emisión IPv4, así como unidifusión, multidifusión y tráfico de emisión IPv6. La conmutación por error sólo se produce si se ha configurado más de una interfaz en el grupo IPMP. El proceso de conmutación por error garantiza un acceso ininterrumpido a la red.

Detección de reparaciones y recuperación tras los errores

La *detección de reparaciones* es el proceso de detectar si una tarjeta NIC o la ruta de una NIC a un dispositivo de capa de Internet empieza a funcionar correctamente tras un error. Tras detectar si una NIC se ha reparado, IPMP lleva a cabo la *recuperación tras los errores*, el proceso de restablecer el acceso a la red para la interfaz reparada. La detección de reparaciones da por sentado que se ha activado la función de recuperación tras los errores. Consulte [“Detección de reparaciones de interfaces físicas” en la página 761](#) para obtener más información.

Sistemas de destino

La detección de errores basada en sondeos utiliza los *sistemas de destino* para determinar la condición de una interfaz. Cada sistema de destino debe estar conectado al mismo vínculo IP que los miembros del grupo IPMP. El daemon `in.mpathd` del sistema local envía mensajes de sondeo de ICMP a cada sistema de destino. Los mensajes de sondeo ayudan a determinar el estado de cada interfaz del grupo IPMP.

Para obtener más información sobre el uso del sistema de destino en la detección de fallos basada en sondeos, consulte [“Detección de fallos basada en sondeos” en la página 759](#).

Expansión de la carga saliente

Con IPMP configurado, los paquetes de red salientes se reparten en varias NIC sin que ello afecte al orden de los paquetes. Este proceso se conoce como *expansión de carga*. Como consecuencia de la expansión de carga, se obtiene un mayor rendimiento. La expansión de carga sólo se produce cuando el tráfico de red fluye hacia varios destinos que utilizan múltiples conexiones.

Reconfiguración dinámica

La *reconfiguración dinámica* (DR) es la capacidad de volver a configurar un sistema mientras se ejecuta, prácticamente con ningún impacto o con ninguno en absoluto en las operaciones en curso. No todas las plataformas de Sun admiten DR. Es posible que algunas plataformas de Sun sólo admitan DR de determinados tipos de hardware. En las plataformas que admiten DR de NIC, se puede utilizar IPMP para conmutar por error de modo transparente el acceso de red y proporcionar acceso de red ininterrumpido al sistema.

Para obtener más información sobre cómo IPMP admite DR, consulte [“IPMP y reconfiguración dinámica” en la página 763](#).

Requisitos básicos de IPMP

IPMP se integra en Oracle Solaris y no requiere hardware especial. Cualquier interfaz que admita Oracle Solaris se puede utilizar con IPMP. Sin embargo, IPMP impone los siguientes requisitos de topología y configuración de la red:

- Todas las interfaces de un grupo IPMP deben tener direcciones MAC únicas.
De modo predeterminado, todas las interfaces de red de sistemas basados en SPARC comparten una única dirección MAC. De este modo, debe cambiar explícitamente la configuración predeterminada para poder utilizar IPMP en sistemas basados en SPARC. Para obtener más información, consulte [“Cómo planificar un grupo IPMP” en la página 769](#).
- Todas las interfaces de un grupo IPMP deben tener el mismo tipo de medio. Si desea más información, consulte [“Grupo IPMP” en la página 751](#).
- Todas las interfaces de un grupo IPMP deben estar conectadas al mismo vínculo IP. Si desea más información, consulte [“Grupo IPMP” en la página 751](#).

Nota – No se admiten varios grupos IPMP en el mismo dominio de emisión de capa de vínculo (L2 o capa 2). Normalmente, un dominio de emisión L2 se asigna a una subred específica. Por lo tanto, debe configurar sólo un grupo IPMP por subred.

- En función de los requisitos de detección de fallos, es posible que deba utilizar tipos específicos de interfaces de red o configurar direcciones IP adicionales en cada interfaz de red. Consulte [“Detección de fallos basada en vínculos” en la página 759](#) y [“Detección de fallos basada en sondeos” en la página 759](#).

Direcciones IPMP

Puede configurar la detección de fallos IPMP en redes IPv4 y de pila doble, y redes IPv4 e IPv6. Las interfaces que se configuran con IPMP admiten dos tipos de direcciones: direcciones de datos y direcciones de prueba.

Direcciones de datos

Las *direcciones de datos* son direcciones IPv4 e IPv6 convencionales que se asignan a una interfaz de NIC durante el inicio o manualmente mediante el comando `ifconfig`. El tráfico de paquetes IPv4 estándar y, si es aplicable, el tráfico de paquetes IPv6 mediante una interfaz se considera *tráfico de datos*.

Direcciones de prueba

Las *direcciones de prueba* son direcciones específicas IPMP que utiliza el daemon `in.mpathd`. Para que una interfaz utilice la detección de fallos basada en sondeos y la reparación, debe estar configurada como mínimo con una dirección de prueba.

Nota – Sólo es necesario configurar direcciones de prueba si se va a utilizar la detección de fallos basada en sondeos.

El daemon `in.mpathd` utiliza las direcciones de prueba para el intercambio de sondeos ICMP (denominado también *tráfico de sondeos*) con otros destinos del vínculo IP. El tráfico de sondeos ayuda a determinar el estado de la interfaz y su NIC, incluida la información sobre si una interfaz ha fallado. Los sondeos verifican que la ruta de envío y recepción de la interfaz esté funcionando correctamente.

Cada interfaz puede configurarse con una dirección de prueba IP. Para una interfaz de una red de doble pila, puede configurar una dirección de prueba IPv4, una dirección de prueba IPv6 o tanto la dirección de prueba IPv4 como la IPv6.

Tras el fallo de una interfaz, las direcciones de prueba permanecen en la interfaz fallida de modo que `in.mpathd` puede seguir enviando sondeos para comprobar las posteriores reparaciones. Debe configurar de modo específico las direcciones de prueba para que las aplicaciones no las utilicen por accidente. Para más información, consulte [“Cómo evitar que las aplicaciones utilicen direcciones de prueba” en la página 756](#).

Para más información sobre la detección de fallos basada en sondeos, consulte [“Detección de fallos basada en sondeos” en la página 759](#).

Direcciones de prueba IPv4

En general, puede utilizar cualquier dirección IPv4 de la subred como dirección de prueba. Las direcciones de prueba IPv4 no necesitan ser enrutables. Dado que las direcciones IPv4 son un recurso limitado para muchos sitios, puede utilizar direcciones privadas RFC 1918 no enrutables como direcciones de prueba. Observe que el daemon `in.mpathd` intercambia sólo sondeos ICMP con otros hosts que se encuentran en la misma subred que la dirección de prueba. Si utiliza las direcciones de prueba RFC 1918, debe configurar otros sistemas, preferiblemente enrutadores, en el vínculo IP con direcciones en la subred RFC 1918 pertinente. De este modo, el daemon `in.mpathd` podrá intercambiar correctamente los sondeos con los sistemas de destino.

Los ejemplos IPMP utilizan direcciones RFC 1918 de la red `192.168.0/24` como direcciones de prueba IPv4. Para obtener más información acerca de direcciones privadas de RFC 1918, consulte [RFC 1918, Address Allocation for Private Internets](#). (<http://www.ietf.org/rfc/rfc1918.txt?number=1918>)

Para configurar direcciones de prueba IPv4, consulte la tarea [“Cómo configurar un grupo IPMP con múltiples interfaces” en la página 771](#).

Direcciones de prueba IPv6

La única dirección de prueba IPv6 válida es la dirección local de vínculo de una interfaz física. No necesita una dirección IPv6 aparte para hacer la función de dirección de prueba IPMP. La dirección local de vínculo IPv6 se basa en la dirección de control de acceso de soportes (MAC) de la interfaz. Las direcciones locales de vínculo se configuran automáticamente cuando la interfaz se activa para IPv6 durante el inicio o cuando se configura manualmente mediante `ifconfig`.

Para identificar la dirección local de vínculo de una interfaz, ejecute el comando `ifconfig interfaz` de un nodo habilitado para IPv6. Compruebe el resultado de la dirección que comienza con el prefijo `fe80`, el prefijo local de vínculo. El indicador `NOFAILOVER` del siguiente resultado de `ifconfig` indica que la dirección local de vínculo `fe80::a00:20ff:feb9:17fa/10` de la interfaz `hme0` se utiliza como dirección de prueba.

```
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:17fa/10
```

Para obtener más información sobre las direcciones locales de vínculo, consulte [Dirección unidifusión local de vínculo](#).

Cuando un grupo IPMP tiene conectadas direcciones tanto IPv4 como IPv6 en todas las interfaces del grupo, no es necesario configurar direcciones de IPv4 aparte. El daemon `in.mpathd` puede utilizar las direcciones locales de vínculo IPv6 como direcciones de prueba.

Para crear una dirección de prueba IPv6, consulte la tarea [“Cómo configurar un grupo IPMP con múltiples interfaces”](#) en la página 771.

Cómo evitar que las aplicaciones utilicen direcciones de prueba

Una vez configurada una dirección de prueba, debe asegurarse de que las aplicaciones no la utilicen. De lo contrario, si falla la interfaz, no se podrá acceder a la aplicación porque las direcciones de prueba no se conmutarán por error durante la operación de conmutación por error. Para asegurarse de que la IP no elija las direcciones de prueba para las aplicaciones normales, marque las direcciones de prueba como deprecated.

IPv4 no utiliza una dirección descartada como dirección de origen para las comunicaciones, a menos que una aplicación se vincule explícitamente con la dirección. El daemon `in.mpathd` se vincula explícitamente con dicha dirección para enviar y recibir tráfico de sondeos. Sin embargo, si una aplicación no se vincula explícitamente con una dirección, y la única dirección que está marcada como UP en la interfaz también está marcada como deprecated; después, como última instancia, esa dirección se utiliza como dirección de origen.

Nota – En los casos de conmutación por error y recuperación tras los errores, mientras la detección de direcciones duplicadas todavía se está ejecutando, puede que las aplicaciones reciban los paquetes que utilizan direcciones descartadas como direcciones de origen. Éste es el comportamiento esperado. Normalmente, una vez que DAD se ha completado, las direcciones descartadas ya no se procesan con las aplicaciones. Sin embargo, puede producirse una excepción inusual con paquetes TCP. Después de que una conexión TCP selecciona una determinada dirección de origen, el uso de dicha dirección no puede cambiarse durante esa conexión. Esa duración puede ampliarse durante un largo período. En casos extremos como éste, existe la posibilidad de que las aplicaciones continúen utilizando direcciones descartadas, incluso después de que DAD finaliza.

Dado que las direcciones locales de vínculo IPv6 normalmente no están presentes en un servicio de nombres, las aplicaciones DNS y NIS no utilizan direcciones locales de vínculo para la comunicación. Por tanto, no debe marcar las direcciones locales de vínculo IPv6 como deprecated.

Las direcciones de prueba IPv4 no deben colocarse en las tablas de servicios de nombres DNS ni NIS. En IPv6, las direcciones locales de vínculo no se colocan normalmente en las tablas de servicios de nombres.

Configuraciones de interfaces IPMP

Una configuración IPMP se compone normalmente de dos o más interfaces físicas en el mismo sistema que están conectadas al mismo vínculo IP. Estas interfaces físicas pueden estar en la misma NIC o no estarlo. Las interfaces se configuran como miembros del mismo grupo IPMP. Si el sistema cuenta con interfaces adicionales en un segundo vínculo IP, debe configurar dichas interfaces como otro grupo IPMP.

Una única interfaz se puede configurar en su propio grupo IPMP. El grupo IPMP de interfaz única tiene el mismo comportamiento que un grupo IPMP con múltiples interfaces. No obstante, la recuperación tras los errores y la conmutación por error no pueden tener lugar para un grupo IPMP que sólo tenga una interfaz.

Asimismo, puede configurar redes VLAN en un grupo IPMP siguiendo los mismos pasos que se deben seguir para configurar un grupo a partir de interfaces IP. Para ver los procedimientos, consulte [“Configuración de grupos IPMP” en la página 771](#). Los mismos requisitos que se enumeran en [“Requisitos básicos de IPMP” en la página 753](#) se aplican para configurar redes VLAN en un grupo IPMP.



Precaución – La convención que se utiliza para denominar redes VLAN puede conducir a errores al configurar redes VLAN como grupo IPMP. Para obtener más detalles acerca de nombres de VLAN, consulte [“Etiquetas VLAN y puntos de conexión físicos” en la página 155](#) de *System Administration Guide: IP Services*. Considere el ejemplo de cuatro redes VLAN bge1000, bge1001, bge2000 y bge2001. La implementación de IPMP precisa que estas VLAN se agrupen del siguiente modo: bge1000 y bge1001 pertenecen a un grupo de la misma VLAN 1, mientras bge2000 y bge2001 pertenecen a otro grupo de la misma VLAN 2. Debido a los nombres de VLAN, pueden darse con frecuencia errores como mezclar VLAN que pertenecen a varios vínculos en un grupo IPMP, por ejemplo, bge1000 y bge2000.

Interfaces de reserva en un grupo IPMP

La *interfaz de reserva* de un grupo IPMP no se utiliza para el tráfico de datos a menos que falle otra interfaz del grupo. Cuando se produce un fallo, las direcciones de datos de la interfaz fallida se migran a la interfaz de reserva. La interfaz de reserva recibe el mismo tratamiento que las demás interfaces activas hasta que se repara la interfaz fallida. Es posible que algunas conmutaciones por error no elijan una interfaz de reserva. En lugar de ello, estas conmutaciones por error podrían elegir una interfaz activa con menos direcciones de datos configurados como UP que la interfaz de reserva.

En una interfaz de reserva debe configurar únicamente las direcciones de prueba. IPMP no permite agregar una dirección de datos a una interfaz configurada con el comando `ifconfig` como `standby`. Cualquier intento de crear este tipo de configuración será fallido. De modo similar, si configura como `standby` una interfaz que ya cuenta con direcciones de datos, estas

direcciones conmutarán por error automáticamente a otra interfaz del grupo IPMP. Debido a estas restricciones, debe utilizar el comando `ifconfig` para marcar cualquier dirección de prueba como `deprecated` y `- failover` antes de configurar la interfaz como `standby`. Para configurar interfaces de reserva, consulte [“Cómo configurar una interfaz de reserva para un grupo IPMP” en la página 777](#)

Configuraciones comunes de interfaces IPMP

Como se menciona en [“Direcciones IPMP” en la página 754](#), las interfaces de un grupo IPMP controlan el tráfico de sondeos y de datos regulares, según la configuración de las interfaces. Las opciones IPMP del comando `ifconfig` se utilizan para establecer la configuración.

Una *interfaz activa* es una interfaz física que transmite tanto tráfico de datos como tráfico de sondeos. La interfaz se configura como "activa" llevando a cabo los procedimientos de [“Cómo configurar un grupo IPMP con múltiples interfaces” en la página 771](#) o [“Cómo configurar un grupo IPMP de interfaz única” en la página 780](#).

A continuación se describen los dos tipos comunes de configuraciones IPMP:

Configuración activa-activa	Un grupo IPMP de dos interfaces en el que ambas interfaces están "activas", es decir, que pueden transmitir tanto tráfico de datos como tráfico de sondeos en cualquier momento
Configuración activa-reserva	Grupo IPMP de dos interfaces en el que una interfaz se configura como "reserva".

Comprobación del estado de una interfaz

Puede comprobar el estado de una interfaz escribiendo el comando `ifconfig interfaz`. Para obtener información general sobre los informes de estado `ifconfig`, consulte [Cómo obtener información sobre una interfaz específica](#).

Por ejemplo, puede utilizar el comando `ifconfig` para obtener el estado de una interfaz de reserva. Cuando la interfaz de reserva no aloja ninguna dirección de datos, tiene el indicador de estado `INACTIVE`. Este observador se encuentra en las líneas de estado de la interfaz en el resultado de `ifconfig`.

Funciones de detección de fallos IPMP y recuperación

El daemon `in.mpathd` controla los siguientes tipos de detección de fallos:

- Detección de fallos basada en vínculos, si la admite el controlador de la NIC
- Detección de fallos basada en sondeos, cuando se configuran las direcciones de prueba
- Detección de interfaces que no estaban presentes durante el inicio

La página del comando `man in.mpathd(1M)` describe detalladamente el modo en que el daemon `in.mpathd` controla la detección de fallos de la interfaz.

Detección de fallos basada en vínculos

La detección de fallos basada en vínculos siempre está activada, cuando la interfaz admite este tipo de detección de fallos. En la versión actual de Oracle Solaris se admiten los siguientes controladores de red de Sun:

- hme
- eri
- ce
- ge
- bge
- qfe
- dmfe
- e1000g
- ixgb
- nge
- nxge
- rge
- xge

Para determinar si la interfaz de otro proveedor admite la detección de fallos basada en vínculos, consulte la documentación del fabricante.

Estos controladores de interfaces de red supervisan el estado del vínculo de la interfaz y notifican al subsistema de red si dicho estado cambia. Cuando se notifica un cambio, el subsistema de red establece o borra el indicador `RUNNING` para dicha interfaz, según sea preciso. Si el daemon detecta que el indicador `RUNNING` de la interfaz se ha borrado, el daemon rechaza inmediatamente la interfaz.

Detección de fallos basada en sondeos

El daemon `in.mpathd` lleva a cabo la detección de fallos basada en sondeos en cada interfaz del grupo IPMP que cuente con una dirección de prueba. La detección de fallos basada en sondeos implica enviar y recibir los mensajes de sondeo de ICMP que utilizan direcciones de prueba. Estos mensajes pasan por la interfaz y se dirigen a uno o más sistemas de destino del mismo vínculo IP. Para ver una introducción a las direcciones de prueba, consulte [“Direcciones de prueba” en la página 754](#). Si desea información sobre cómo configurar las direcciones de prueba, consulte [“Cómo configurar un grupo IPMP con múltiples interfaces” en la página 771](#).

El daemon `in.mpathd` determina qué sistemas de destino se sondean dinámicamente. Los enrutadores conectados al vínculo IP se seleccionan automáticamente como destinos para el sondeo. Si no hay enrutadores en el vínculo, `in.mpathd` envía sondeos a los hosts vecinos del vínculo. Un paquete multidifusión que se envía a la dirección multidifusión de todos los hosts, `224.0.0.1` en IPv4 y `ff02::1` en IPv6, determina qué hosts se utilizarán como sistemas de destino. Los primeros hosts que responden a los paquetes echo se eligen como destinos para los sondeos. Si `in.mpathd` no encuentra enrutadores ni hosts que respondan a los paquetes echo ICMP, `in.mpathd` no puede detectar los fallos basados en sondeos.

Puede utilizar las rutas host para configurar explícitamente una lista de sistemas de destino para utilizar con el comando `in.mpathd`. Para obtener más información, consulte [“Configuración de sistemas de destino” en la página 775](#).

Para asegurarse de que cada interfaz del grupo IPMP funcione correctamente, `in.mpathd` sondea todos los destinos por separado mediante todas las interfaces del grupo IPMP. Si no hay ninguna respuesta a cinco sondeos consecutivos, `in.mpathd` considera que la interfaz ha fallado. La velocidad de sondeo depende del *tiempo de detección de fallos* (FDT). El valor predeterminado del tiempo de detección de fallos es de 10 segundos. Puede ajustar el tiempo de detección de fallos en el archivo `/etc/default/mpathd`. Para obtener instrucciones, consulte [“Cómo configurar el archivo /etc/default/mpathd” en la página 789](#).

Para un tiempo de detección de reparaciones de 10 segundos, la velocidad de sondeo es de aproximadamente un sondeo cada dos segundos. El tiempo mínimo de detección de reparaciones predeterminado es el doble del tiempo de detección de fallos, es decir, 20 segundos, ya que debe recibirse la respuesta de 10 sondeos consecutivos. Los tiempos de detección de fallos y reparaciones sólo se aplican a la detección de fallos basada en sondeos.

Nota – En un grupo IPMP compuesto por redes VLAN, la detección de fallos basada en vínculos se implementa por vínculos físicos y, por lo tanto, afecta a todas las redes VLAN del vínculo en cuestión. La detección de fallos basada en sondeos se realiza por vínculos VLAN. Por ejemplo, `bge0/bge1` y `bge1000/bge1001` se configuran en un mismo grupo. Si el cable para `bge0` está desconectado, la detección de fallos basada en vínculos no indicará que `bge0` y `bge1000` hayan fallado de manera inmediata. Sin embargo, si no se puede alcanzar ningún destino de sondeo de `bge0`, sólo se indicará que ha fallado `bge0`, porque `bge1000` tiene sus propios destinos de sondeo en su red VLAN.

Fallos de grupo

Un *fallo de grupo* tiene lugar cuando todas las interfaces de un grupo IPMP fallan al mismo tiempo. El daemon `in.mpathd` no lleva a cabo conmutaciones por error para un fallo de grupo.

Asimismo, no se puede realizar ninguna conmutación por error si todos los sistemas de destino fallan de forma simultánea. En este caso, `in.mpathd` vacía todos los sistemas de destino actuales y descubre nuevos sistemas de destino.

Detección de reparaciones de interfaces físicas

Para que el daemon `in.mpathd` considere que se ha reparado una interfaz, el indicador `RUNNING` debe estar configurado para la interfaz. Si se utiliza la detección de fallos basada en sondeos, el daemon `in.mpathd` debe recibir respuestas a 10 paquetes de sondeos consecutivos de la interfaz antes de que ésta se considere como reparada. Cuando una interfaz se considera reparada, cualquier dirección que conmutaba por error a otra interfaz, se recuperará tras el error a la interfaz reparada. Si la interfaz estaba configurada como "activa" antes de que fallara, tras la reparación podrá seguir enviando y recibiendo tráfico.

Qué ocurre durante la conmutación por error de la interfaz

Los dos ejemplos siguientes muestran una configuración típica y cómo dicha configuración cambia automáticamente cuando falla una interfaz. Cuando falla la interfaz `hme0`, observe que todas las direcciones de datos pasan de `hme0` a `hme1`.

EJEMPLO 30-1 Configuración de la interfaz antes de un fallo

```
hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
      mtu 1500 index 2
      inet 192.168.85.19 netmask fffffff0 broadcast 192.168.85.255
      groupname test
hme0:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
      mtu 1500
      index 2 inet 192.168.85.21 netmask fffffff0 broadcast 192.168.85.255
hme1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
8      inet 192.168.85.20 netmask fffffff0 broadcast 192.168.85.255
      groupname test
hme1:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
      mtu 1500
      index 2 inet 192.168.85.22 netmask fffffff0 broadcast 192.168.85.255
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:19fa/10
      groupname test
hme1: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:1bfc/10
      groupname test
```

EJEMPLO 30-2 Configuración de la interfaz después de un fallo

```
hme0: flags=19000842<BROADCAST,RUNNING,MULTICAST,IPv4,
      NOFAILOVER,FAILED> mtu 0 index 2
```

EJEMPLO 30-2 Configuración de la interfaz después de un fallo *(Continuación)*

```

    inet 0.0.0.0 netmask 0
    groupname test
hme0:1: flags=19040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,
    NOFAILOVER,FAILED> mtu 1500 index 2
    inet 192.168.85.21 netmask fffffff0 broadcast 10.0.0.255
hme1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.85.20 netmask fffffff0 broadcast 192.168.85.255
    groupname test
hme1:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,
    NOFAILOVER> mtu 1500
    index 2 inet 192.168.85.22 netmask fffffff0 broadcast 10.0.0.255
hme1:2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 6
    inet 192.168.85.19 netmask fffffff0 broadcast 192.168.18.255
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER,FAILED> mtu 1500 index 2
    inet6 fe80::a00:20ff:feb9:19fa/10
    groupname test
hme1: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
    inet6 fe80::a00:20ff:feb9:1bfc/10
    groupname test

```

Puede ver que el indicador FAILED aparece en hme0 para indicar que la interfaz ha fallado. Observe también que se ha creado hme1:2. hme1:2 era originalmente hme0. La dirección 192.168.85.19 se convierte en accesible mediante hme1.

Los miembros multidifusión asociados con 192.168.85.19 pueden seguir recibiendo paquetes, pero ahora los reciben mediante hme1. Cuando se produce el fallo de la dirección 192.168.85.19 de hme0 a hme1, se crea la dirección ficticia 0.0.0.0 en hme0. La dirección ficticia se crea para que se pueda seguir accediendo a hme0. hme0:1 no puede existir sin hme0. La dirección de prueba se elimina cuando tiene lugar una recuperación tras los errores.

De modo similar, se produce la conmutación por error de la dirección IPv6 de hme0 a hme1. En IPv6, los miembros de multidifusión se asocian con índices de interfaz. Los miembros de multidifusión también se conmutan por error de hme0 a hme1. También se mueven todas las direcciones configuradas por `in.ndpd`. Esta acción no se muestra en los ejemplos.

El daemon `in.mpathd` sigue realizando el sondeo a través de la interfaz fallida hme0. Cuando el daemon recibe 10 respuestas consecutivas para un tiempo de detección de reparaciones predeterminado de 20 segundos, determina que la interfaz se ha reparado. Dado que el indicador RUNNING también se establece en hme0, el daemon invoca la recuperación tras los errores. Después de la recuperación tras los errores, se restablece la configuración original.

Para ver una descripción de todos los mensajes de error registrados en la consola durante los fallos y las reparaciones, consulte la página del comando `man in.mpathd(1M)`.

IPMP y reconfiguración dinámica

La función de reconfiguración dinámica (DR) permite volver a configurar el hardware del sistema, como las interfaces, mientras el sistema está en ejecución. En esta sección se explica cómo DR interopera con IPMP.

En un sistema que admite la DR de NIC, IPMP se puede utilizar para mantener la conectividad y evitar la interrupción de las conexiones existentes. Puede conectar, desconectar o volver a conectar tarjetas NIC de forma segura en un sistema que admita DR y utilice IPMP. Esto es posible porque IPMP se integra en la estructura del Gestor de coordinación de reconfiguración (RCM). RCM administra la reconfiguración dinámica de los componentes del sistema.

Normalmente se utiliza el comando `cfgadm` para llevar a cabo las operaciones de DR. Sin embargo, algunas plataformas proporcionan otros métodos. Consulte la documentación de su plataforma para obtener más información. Encontrará información específica sobre DR en los siguientes recursos.

TABLA 30-1 Recursos de documentación para la reconfiguración dinámica

Descripción	Para obtener información
Información detallada sobre el comando <code>cfgadm</code>	Página del comando man <code>cfgadm(1M)</code>
Información específica sobre DR en el entorno de Sun Cluster	<i>Sun Cluster 3.1 System Administration Guide</i>
Información específica sobre DR en el entorno de Sun Fire	<i>Sun Fire 880 Dynamic Reconfiguration Guide</i>
Información introductoria sobre DR y el comando <code>cfgadm</code>	Capítulo 6, “Dynamically Configuring Devices (Tasks)” de <i>System Administration Guide: Devices and File Systems</i>
Tareas para administrar grupos IPMP en un sistema que admite DR	“Sustitución de una interfaz física fallida en sistemas que admiten reconfiguración dinámica” en la página 784

Conexión de NIC

Puede agregar interfaces a un grupo IPMP en cualquier momento utilizando el comando `ifconfig`, tal como se describe en [“Cómo configurar un grupo IPMP con múltiples interfaces” en la página 771](#). De este modo, cualquier interfaz de los componentes del sistema que conecte tras el inicio del sistema se podrá sondear y agregar a un grupo IPMP existente. Si es preciso, puede configurar las interfaces que acaba de agregar en su propio grupo IPMP.

Estas interfaces y las direcciones de datos que se configuran en ellas están inmediatamente disponibles para el grupo IPMP. Sin embargo, para que el sistema configure y utilice las

interfaces automáticamente tras un reinicio, debe crear un archivo `/etc/hostname.interfaz` para cada interfaz nueva. Para obtener más información, consulte [Cómo configurar una interfaz física tras la instalación del sistema](#).

Si ya existe un archivo `/etc/hostname.interfaz` cuando se conecta la interfaz, RCM configura automáticamente la interfaz de acuerdo con el contenido de este archivo. De este modo, la interfaz recibe la misma configuración que habría recibido tras el inicio del sistema.

Desconexión de NIC

Todas las solicitudes para desconectar los componentes del sistema que contengan NIC se comprueban antes para garantizar el mantenimiento de la conectividad. Por ejemplo, de modo predeterminado no puede desconectar una NIC que no se encuentre en un grupo IPMP. Tampoco puede desconectar una NIC que contenga las únicas interfaces en funcionamiento de un grupo IPMP. Sin embargo, si debe eliminar el componente del sistema, puede modificar este comportamiento con la opción `-f` de `cfgadm`, tal como se explica en la página del comando `man cfgadm(1M)`.

Si las comprobaciones son correctas, las direcciones de datos asociadas con la NIC desconectada conmutarán por error a una NIC en funcionamiento del mismo grupo, como si la NIC que se desconecta hubiera fallado. Cuando se desconecta la NIC, todas las direcciones de prueba de las interfaces NIC se desconfiguran. A continuación, la NIC se desconecta del sistema. Si falla alguno de estos pasos, o falla la DR de otro hardware del mismo componente del sistema, se restablece el estado original de la configuración anterior. Recibirá un mensaje de estado sobre este evento. De lo contrario, la solicitud de desconexión se completará correctamente. Ya podrá eliminar el componente del sistema. Las conexiones existentes no se interrumpen.

Reconexión de NIC

RCM registra la información de configuración asociada con cualquier NIC que se desconecte de un sistema en ejecución. Como consecuencia, RCM trata la reconexión de una NIC que se ha desconectado previamente del mismo modo que lo haría con la conexión de una nueva NIC. Por tanto, RCM sólo realiza conexiones.

Sin embargo, las NIC reconectadas cuentan con un archivo `/etc/hostname.interfaz`. En ese caso, RCM configura automáticamente la interfaz de acuerdo con el contenido del archivo `/etc/hostname.interfaz`. Asimismo, RCM informa al daemon `in.mpathd` de cada dirección de datos que se alojó originalmente en la interfaz reconectada. Cuando la interfaz reconectada funciona correctamente, todas sus direcciones de datos se recuperan tras los errores en la interfaz reconectada como si se hubiera reparado.

Si la NIC que se reconecta no tiene ningún archivo `/etc/hostname.interfaz`, no hay ninguna información de configuración disponible. RCM no tiene información sobre cómo configurar la interfaz. Una consecuencia de esta situación es que las direcciones que se habían conmutado por error a otra interfaz no se recuperarán tras los errores.

NIC que no estaban presentes durante el inicio del sistema

Las tarjetas NIC que no están presentes durante el inicio del sistema representan un caso especial de detección de fallos. Durante el inicio, las secuencias de inicio supervisan las interfaces con archivos `/etc/hostname.interfaz` que no se pueden sondear. Todas las direcciones de datos que haya en dicho archivo `/etc/hostname.interfaz` se alojan de manera automática en otra interfaz del grupo IPMP.

En tal caso, recibirá mensajes de error similares a los siguientes:

```
moving addresses from failed IPv4 interfaces: hme0 (moved to hme1)
moving addresses from failed IPv6 interfaces: hme0 (moved to hme1)
```

Si no existe ninguna dirección alternativa, recibirá mensajes de error similares a los siguientes:

```
moving addresses from failed IPv4 interfaces: hme0 (couldn't move;
no alternative interface)
moving addresses from failed IPv6 interfaces: hme0 (couldn't move;
no alternative interface)
```

Nota – En este caso de detección de fallos, sólo se mueven a una interfaz alternativa las direcciones de datos que se especifican en el archivo `/etc/hostname.interfaz` de la interfaz que falta. Cualquier dirección que se obtenga por otros medios, como RARP o DHCP, no se obtendrá ni se moverá.

Si se reconecta con DR una interfaz con el mismo nombre que otra interfaz que no estaba presente durante el inicio del sistema, RCM sondea la interfaz automáticamente. A continuación, RCM configura la interfaz de acuerdo con el contenido del archivo `/etc/hostname.interfaz` de la interfaz. Finalmente, RCM recupera tras los errores las direcciones de datos, como si la interfaz se hubiera reparado. Por tanto, la configuración de red final es idéntica a la configuración que se habría realizado si el sistema se hubiera iniciado con la interfaz presente.

Administración de IPMP (tareas)

En este capítulo se describen las tareas para administrar grupos de interfaces con múltiples rutas de redes IP (IPMP). Se abordan los siguientes temas principales:

- “Configuración de IPMP (mapas de tareas)” en la [página 767](#)
- “Configuración de grupos IPMP” en la [página 769](#)
- “Mantenimiento de grupos IPMP” en la [página 781](#)
- “Sustitución de una interfaz física fallida en sistemas que admiten reconfiguración dinámica” en la [página 784](#)
- “Recuperación de una interfaz física que no estaba presente durante el inicio del sistema” en la [página 786](#)
- “Modificación de configuraciones IPMP” en la [página 788](#)

Para obtener una descripción general de los conceptos de IPMP, consulte el [Capítulo 30, “Introducción a IPMP \(descripción general\)”](#).

Configuración de IPMP (mapas de tareas)

Esta sección contiene los vínculos a las tareas que se describen en este capítulo.

Configuración y administración de grupos IPMP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Planificar un grupo IPMP.	Enumera toda la información auxiliar y las tareas necesarias para poder configurar un grupo IPMP.	“Cómo planificar un grupo IPMP” en la página 769

Tarea	Descripción	Para obtener instrucciones
Configurar un grupo de interfaces IPMP con múltiples interfaces.	Configura varias interfaces como miembros de un grupo IPMP.	“Cómo configurar un grupo IPMP con múltiples interfaces” en la página 771
Configurar un grupo IPMP en el que una de las interfaces es una interfaz de reserva.	Configura una de las interfaces de un grupo de interfaces IPMP como interfaz de reserva.	“Cómo configurar una interfaz de reserva para un grupo IPMP” en la página 777
Configurar un grupo IPMP compuesto por una única interfaz.	Crea un único grupo de interfaces IPMP.	“Cómo configurar un grupo IPMP de interfaz única” en la página 780
Mostrar el grupo IPMP al que pertenece una interfaz física.	Explica cómo obtener el nombre de un grupo IPMP de la interfaz a partir del resultado del comando <code>ifconfig</code> .	“Cómo mostrar la pertenencia de una interfaz a un grupo IPMP” en la página 781
Agregar una interfaz a un grupo IPMP.	Configura una nueva interfaz como miembro de un grupo IPMP existente.	“Cómo agregar una interfaz a un grupo IPMP” en la página 782
Eliminar una interfaz de un grupo IPMP.	Explica cómo eliminar una interfaz de un grupo IPMP.	“Cómo eliminar una interfaz de un grupo IPMP” en la página 782
Mover una interfaz de un grupo IPMP existente a otro grupo distinto.	Mueve las interfaces entre los grupos IPMP.	“Cómo mover una interfaz de un grupo IPMP a otro grupo” en la página 783
Cambiar tres parámetros predeterminados para el daemon <code>in.mpathd</code> .	Personaliza el tiempo de detección de fallos y otros parámetros del daemon <code>in.mpathd</code> .	“Cómo configurar el archivo <code>/etc/default/mpathd</code>” en la página 789

Administración de IPMP en interfaces que admiten reconfiguración dinámica (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Eliminar una interfaz que ha fallado.	Elimina una interfaz fallida de un sistema.	“Cómo eliminar una interfaz física que ha fallado (desconexión en DR)” en la página 784
Reemplazar una interfaz que ha fallado.	Reemplaza una interfaz fallida.	“Como sustituir una interfaz física que ha fallado (conexión en DR)” en la página 785
Recuperar una interfaz que no se ha configurado durante el inicio.	Recupera una interfaz fallida.	“Cómo recuperar una interfaz física que no está presente al iniciar el sistema” en la página 786

Configuración de grupos IPMP

Esta sección describe los procedimientos para configurar los grupos IPMP. También explica cómo configurar una interfaz como interfaz de reserva.

Planificación de un grupo IPMP

Antes de configurar las interfaces de un sistema como parte de un grupo IPMP, debe realizar una planificación previa.

▼ Cómo planificar un grupo IPMP

El procedimiento siguiente incluye las tareas de planificación de la información que se debe obtener antes de configurar el grupo IPMP. No es necesario realizar las tareas por orden.

1 Decida qué interfaces del sistema formarán parte del grupo IPMP.

Un grupo IPMP se compone normalmente de, como mínimo, dos interfaces físicas conectadas al mismo vínculo IP. No obstante, si lo desea, puede configurar un grupo IPMP de interfaz única. Para ver una introducción a los grupos IPMP, consulte [“Configuraciones de interfaces IPMP” en la página 757](#). Por ejemplo, puede configurar el mismo conmutador Ethernet o la misma subred IP en el mismo grupo IPMP. Puede configurar la cantidad de interfaces que desee en el mismo grupo IPMP.

No puede utilizar el parámetro `group` del comando `ifconfig` con interfaces lógicas. Por ejemplo, puede utilizar el parámetro `group` con `hme0`, pero no con `hme0:1`.

2 Compruebe que cada interfaz del grupo tenga una dirección MAC exclusiva.

Para ver instrucciones, consulte [“SPARC: Cómo asegurarse de que la dirección MAC de una interfaz sea única” en la página 152](#).

3 Elija un nombre para el grupo IPMP.

Cualquier nombre que no sea nulo será válido. También puede utilizar un nombre que identifique el vínculo IP al que están vinculadas las interfaces.

4 Asegúrese de que se inserte y configure el mismo conjunto de módulos STREAMS en todas las interfaces del grupo IPMP.

Todas las interfaces del mismo grupo deben tener configurados los mismos módulos STREAMS y en el mismo orden.

a. Compruebe el orden de los módulos STREAMS en todas las interfaces del grupo IPMP eventual.

Puede imprimir una lista de los módulos STREAMS utilizando el comando `ifconfig interfaz modlist`. Por ejemplo, éste es el resultado de `ifconfig` para una interfaz `hme0`:

```
# ifconfig hme0 modlist
0 arp
1 ip
2 hme
```

Las interfaces existen normalmente como controladores de red justo debajo del módulo IP, tal como se muestra en el resultado de `ifconfig hme0 modlist`. No requieren ninguna configuración adicional.

Sin embargo, determinadas tecnologías, como NCA o el Filtro IP, se insertan como módulos STREAMS entre el módulo IP y el controlador de red. Es posible que se originen problemas en el comportamiento de las interfaces del mismo grupo IPMP.

Si un módulo STREAMS tiene estado, puede producirse un comportamiento inesperado en la conmutación por error, aunque se inserte el mismo módulo en todas las interfaces de un grupo. Sin embargo, puede utilizar módulos STREAMS sin estado, siempre y cuando los inserte en el mismo orden en todas las interfaces del grupo IPMP.

b. Inserte los módulos de una interfaz en el orden estándar para el grupo IPMP.

```
ifconfig interface modinsert module-name
```

```
ifconfig hme0 modinsert ip
```

5 Utilice el mismo formato de direcciones IP en todas las interfaces del grupo IPMP.

Si una interfaz está configurada para IPv4, todas las interfaces del grupo deben estar configuradas para IPv4. Supongamos que tiene un grupo IPMP compuesto por interfaces de varias NIC. Si añade direcciones IPv6 a las interfaces de una tarjeta NIC, todas las interfaces del grupo IPMP se deben configurar para que admitan IPv6.

6 Compruebe que todas las interfaces del grupo IPMP estén conectadas al mismo vínculo IP.

7 Compruebe que el grupo IPMP no contenga interfaces con diferentes tipos de medios de red.

Las interfaces que están agrupadas deben tener el mismo tipo de interfaz, de acuerdo con lo que se define en `/usr/include/net/if_types.h`. Por ejemplo, no puede combinar interfaces Ethernet y Token Ring en un grupo IPMP. Tampoco puede combinar una interfaz de bus Token con las interfaces de modalidad de transferencia asíncrona (ATM) del mismo grupo IPMP.

- 8 En el caso de IPMP con interfaces ATM, configure dichas interfaces en modo de emulación de LAN.**

IPMP no se admite para las interfaces que utilicen IP clásica sobre ATM.

Configuración de grupos IPMP

Esta sección contiene las tareas de configuración para un grupo IPMP típico con un mínimo de dos interfaces físicas.

- Para ver una introducción a los grupos IPMP de interfaces múltiples, consulte [“Grupo IPMP” en la página 751](#).
- Para conocer las tareas de planificación, consulte [“Planificación de un grupo IPMP” en la página 769](#).
- Para configurar un grupo IPMP con una sola interfaz física, consulte [“Configuración de grupos IPMP con una única interfaz física” en la página 779](#).

▼ Cómo configurar un grupo IPMP con múltiples interfaces

Los siguientes pasos para configurar un grupo IPMP también se aplican al configurar redes VLAN en un grupo IPMP.

Antes de empezar

Es preciso que ya haya configurado las direcciones IPv4, y, si es necesario, las direcciones IPv6 de todas las interfaces del grupo IPMP eventual.



Precaución – Debe configurar sólo un grupo IPMP para cada subred o dominio de emisión L2. Para obtener más información, consulte [“Requisitos básicos de IPMP” en la página 753](#)

- 1 En el sistema cuyas interfaces se deben configurar, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

- 2 Coloque cada interfaz física en un grupo IPMP.**

```
# ifconfig interface group group-name
```

Por ejemplo, para colocar hme0 y hme1 en el grupo testgroup1, debe escribir los siguientes comandos:

```
# ifconfig hme0 group testgroup1
# ifconfig hme1 group testgroup1
```

Evite utilizar espacios en los nombres de grupo. La pantalla de estado de `ifconfig` no muestra espacios. Por tanto, no cree dos nombres de grupo similares que sólo se diferencien en un espacio. Si uno de los nombres de grupo contiene un espacio, aparecerán iguales en la pantalla de estado.

En un entorno de doble pila, si se coloca una instancia IPv4 de una interfaz en un grupo específico, automáticamente se coloca la instancia IPv6 en el mismo grupo.

3 (Opcional) Configure una dirección de prueba IPv4 en una o más interfaces físicas.

Sólo debe configurar una dirección de prueba si desea utilizar la detección de fallos basada en sondeos en una interfaz específica. Las direcciones de prueba se configuran como interfaces lógicas de la interfaz física que especifica para el comando `ifconfig`.

Si una interfaz del grupo va a convertirse en la interfaz de reserva, no configure ninguna dirección de prueba para la interfaz en este momento. Configure una dirección de prueba para la interfaz de reserva como parte de la tarea “[Cómo configurar una interfaz de reserva para un grupo IPMP](#)” en la [página 777](#).

Utilice la siguiente sintaxis del comando `ifconfig` para configurar una dirección de prueba:

```
# ifconfig interface addif ip-address parameters -failover deprecated up
```

Por ejemplo, para la interfaz de red principal `hme0` debe crear la siguiente dirección de prueba:

```
# ifconfig hme0 addif 192.168.85.21 netmask + broadcast + -failover deprecated up
```

Este comando configura los siguientes parámetros para la interfaz de red principal `hme0`:

- La dirección se establece en `192.168.85.21`.
- La dirección de emisión y la máscara de red se configuran con el valor predeterminado.
- Se establecen las opciones `-failover` y `deprecated`.

Nota – Debe marcar una dirección de prueba IPv4 como `deprecated` para evitar que las aplicaciones utilicen la dirección de prueba.

4 Compruebe la configuración de IPv4 para una interfaz específica.

Puede ver el estado de una interfaz en cualquier momento escribiendo `ifconfig interfaz`. Para obtener mas información sobre cómo ver el estado de una interfaz, consulte [Cómo obtener información sobre una interfaz específica](#).

Puede obtener información sobre la configuración de la dirección de prueba para una interfaz física especificando la interfaz lógica que está asignada a la dirección de prueba.

```
# ifconfig hme0:1
hme0:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
mtu 1500 index 2
inet 192.168.85.21 netmask ffffffff broadcast 192.168.85.255
```

5 (Opcional) Si procede, configure una dirección de prueba IPv6.

```
# ifconfig interface inet6 -failover
```

Las interfaces físicas con direcciones IPv6 se colocan en el mismo grupo IPMP que las direcciones IPv4 de las interfaces. Esto sucede al configurar la interfaz física con direcciones IPv4 en un grupo IPMP. Si coloca primero las interfaces físicas con direcciones IPv6 en un grupo IPMP, las interfaces físicas con direcciones IPv4 también se colocan implícitamente en el mismo grupo IPMP.

Por ejemplo, para configurar hme0 con una dirección de prueba IPv6, debe escribir lo siguiente:

```
# ifconfig hme0 inet6 -failover
```

No es necesario marcar una dirección de prueba IPv6 como descartada para impedir que las aplicaciones utilicen la dirección de prueba.

6 Compruebe la configuración de IPv6.

```
# ifconfig hme0 inet6
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
    inet6 fe80::a00:20ff:feb9:17fa/10
    groupname test
```

La dirección de prueba IPv6 es la dirección local de vínculo de la interfaz.

7 (Opcional) Conserve la configuración del grupo IPMP tras los reinicios.

- Para IPv4, agregue la línea siguiente al archivo `/etc/hostname.interface`:

```
interface-address <parameters> group group-name up \
    addif logical-interface -failover deprecated <parameters> up
```

En esta instancia, la dirección IPv4 de prueba se configura sólo después de reiniciar. Si desea invocar la configuración en la sesión actual, lleve a cabo los pasos 1, 2, y, opcionalmente, 3.

- Para IPv6, agregue la línea siguiente al archivo `/etc/hostname6.interface`:

```
-failover group group-name up
```

Esta dirección IPv6 de prueba se configura sólo después del reinicio. Si desea invocar la configuración en la sesión actual, lleve a cabo los pasos 1, 2, y, opcionalmente, 5.

8 (Opcional) Agregue más interfaces al grupo IPMP repitiendo los pasos del 1 al 6.

Puede agregar nuevas interfaces a un grupo existente en un sistema en funcionamiento. No obstante, los cambios se perderán al reiniciar.

Ejemplo 31-1 Configuración de un grupo IPMP con dos interfaces

Supongamos que desea hacer lo siguiente:

- Configurar la dirección de emisión y la máscara de red con el valor predeterminado.
- Configurar la interfaz con una dirección de prueba 192.168.85.21.

Debe escribir el comando siguiente:

```
# ifconfig hme0 addif 192.168.85.21 netmask + broadcast + -failover deprecated up
```

Debe marcar una dirección de prueba IPv4 como deprecated para evitar que las aplicaciones utilicen la dirección de prueba. Consulte [“Cómo configurar un grupo IPMP con múltiples interfaces” en la página 771](#).

Para activar el atributo de conmutación por error de la dirección, debe utilizar la opción `failover` sin el guión.

Todas las direcciones IP de prueba de un grupo IPMP deben utilizar el mismo prefijo de red. Las direcciones IP de prueba deben pertenecer a una única subred IP.

Ejemplo 31–2 Conservación de la configuración de un grupo IPMP IPv4 tras el reinicio

Supongamos que desea crear un grupo IPMP denominado `testgroup1` con la siguiente configuración:

- La interfaz física `hme0` con la dirección de datos `192.168.85.19`.
- Una interfaz lógica con la dirección de prueba `192.168.85.21`.

Nota – En este ejemplo, la interfaz física y la dirección de datos están emparejadas. La interfaz lógica y la dirección de prueba. No obstante, no existen relaciones inherentes entre un "tipo" de interfaz y el tipo de dirección.

- Las opciones `deprecated` y `-failover` configuradas.
- La dirección de emisión y la máscara de red se configuran con el valor predeterminado.

Debe agregar la siguiente línea al archivo `/etc/hostname.hme0`:

```
192.168.85.19 netmask + broadcast + group testgroup1 up \  
    addif 192.168.85.21 deprecated -failover netmask + broadcast + up
```

De modo similar, para colocar la segunda interfaz `hme1` bajo el mismo grupo `testgroup1` y configurar una dirección de prueba, debe agregar la línea siguiente:

```
192.168.85.20 netmask + broadcast + group testgroup1 up \  
    addif 192.168.85.22 deprecated -failover netmask + broadcast + up
```

Ejemplo 31–3 Conservación de la configuración de un grupo IPMP IPv6 tras el reinicio

Para crear un grupo de prueba para la interfaz `hme0` con una dirección IPv6, debe agregar la línea siguiente al archivo `/etc/hostname6.hme0`:

```
-failover group testgroup1 up
```

De modo similar, para colocar la segunda interfaz `hme1` en el grupo `testgroup1` y configurar una dirección de prueba, debe agregar la línea siguiente al archivo `/etc/hostname6.hme1`:

```
-failover group testgroup1 up
```

Errores más frecuentes

Durante la configuración del grupo IPMP, `in.mpathd` genera una serie de mensajes para la consola del sistema o el archivo `syslog`. Estos mensajes son informativos e indican que la configuración de IPMP funciona correctamente.

- Este mensaje indica que la interfaz `hme0` se ha agregado al grupo IPMP `testgroup1`. Sin embargo, `hme0` no tiene configurada una dirección de prueba. Para permitir la detección de fallos basada en sondeos, debe asignar una dirección de prueba a la interfaz.

```
May 24 14:09:57 host1 in.mpathd[101180]:
No test address configured on interface hme0;
disabling probe-based failure detection on it.
testgroup1
```

- Este mensaje aparece para todas las interfaces que sólo tengan direcciones IPv4 agregadas a un grupo IPMP.

```
May 24 14:10:42 host4 in.mpathd[101180]:
NIC qfe0 of group testgroup1 is not
plumbed for IPv6 and may affect failover capability
```

- Este mensaje aparece al configurar una dirección de prueba para una interfaz.

```
Created new logical interface hme0:1
May 24 14:16:53 host1 in.mpathd[101180]:
Test address now configured on interface hme0;
enabling probe-based failure detection on it
```

Véase también

Si desea que el grupo IPMP tenga una configuración de reserva activa, vaya a [“Cómo configurar una interfaz de reserva para un grupo IPMP” en la página 777](#).

Configuración de sistemas de destino

La detección de fallos basada en sondeos implica el uso de sistemas de destino, tal como se explica en [“Detección de fallos basada en sondeos” en la página 759](#). Para algunos grupos IPMP, los destinos predeterminados que utiliza `in.mpathd` son suficientes. Sin embargo, para algunos grupos IPMP, quizá desee configurar destinos específicos para la detección de fallos basada en sondeos. La detección de fallos basada en sondeos se lleva a cabo configurando las rutas host en la tabla de enrutamiento como destinos de sondeo. Cualquier ruta host configurada en la tabla de enrutamiento aparece enumerada antes del enrutador predeterminado. Por tanto, IPMP utiliza rutas host definidas explícitamente para la selección de destino. Puede utilizar cualquiera de estos dos métodos para especificar destinos directamente: configurar manualmente las rutas host o crear una secuencia shell que se pueda convertir en una secuencia de inicio.

Considere los siguientes criterios cuando evalúe qué hosts de su red podrían constituir destinos correctos.

- Asegúrese de que los posibles destinos estén disponibles y ejecutándose. Cree una lista de sus direcciones IP.
- Asegúrese de que las interfaces de destino se encuentren en la misma red que el grupo IPMP que está configurando.
- La máscara de red y la dirección de emisión de los sistemas de destino deben ser las mismas que las direcciones del grupo IPMP.
- El host de destino debe poder responder a las solicitudes de ICMP desde la interfaz que utiliza la detección de fallos basada en sondeos.

▼ **Cómo especificar manualmente los sistemas de destino para la detección de fallos basada en sondeos**

- 1 Inicie sesión con su cuenta de usuario en el sistema en el que va a configurar la detección de fallos basada en sondeos.
- 2 Agregue una ruta a un host particular para utilizar como destino en la detección de fallos basada en sondeos.

```
$ route add -host destination-IP gateway-IP -static
```

Sustituya los valores de *IP_destino* e *IP_portal* por la dirección IPv4 del host que se utilizará como destino. Por ejemplo, escriba lo siguiente para especificar el sistema de destino 192.168.85.137, que se encuentra en la misma subred que las interfaces del grupo IPMP testgroup1.

```
$ route add -host 192.168.85.137 192.168.85.137 -static
```

- 3 Agregue rutas a los host adicionales de la red para utilizar como sistemas de destino.

▼ **Cómo especificar sistemas de destino en una secuencia de shell**

- 1 En el sistema en el que ha configurado un grupo IPMP, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 Cree una secuencia de shell que configure rutas estáticas para los destinos propuestos.

Por ejemplo, puede crear una secuencia de shell denominada `ipmp.targets` con el siguiente contenido:

```
TARGETS="192.168.85.117 192.168.85.127 192.168.85.137"

case "$1" in
    'start')
```



```

        /usr/bin/echo "Adding static routes for use as IPMP targets"
        for target in $TARGETS; do
        /usr/sbin/route add -host $target $target
        done
        ;;
    'stop')
        /usr/bin/echo "Removing static routes for use as IPMP targets"
        for target in $TARGETS; do
        /usr/sbin/route delete -host $target $target
        done
        ;;
esac

```

3 Copie la secuencia de shell en el directorio de la secuencia de inicio.

```
# cp ipmp.targets /etc/init.d
```

4 Cambie los permisos de la nueva secuencia de inicio.

```
# chmod 744 /etc/init.d/ipmp.targets
```

5 Cambie la propiedad de la nueva secuencia de inicio.

```
# chown root:sys /etc/init.d/ipmp.targets
```

6 Cree un vínculo para la secuencia de inicio en el directorio `/etc/init.d`.

```
# ln /etc/init.d/ipmp.targets /etc/rc2.d/S70ipmp.targets
```

El prefijo S70 del nombre de archivo S70ipmp.targets ordena la nueva secuencia correctamente con respecto a las demás secuencias de inicio.

Configuración de interfaces de reserva

Siga este procedimiento para que el grupo IPMP tenga una configuración de reserva activa. Para obtener más información sobre este tipo de configuración, consulte [“Configuraciones de interfaces IPMP” en la página 757](#).

▼ Cómo configurar una interfaz de reserva para un grupo IPMP

Antes de empezar

- Debe tener todas las interfaces configuradas como miembros del grupo IPMP.
- No debe configurar ninguna dirección de prueba en la interfaz que se convertirá en la interfaz de reserva.

Para obtener información sobre cómo configurar un grupo IPMP y asignar direcciones de prueba, consulte [“Cómo configurar un grupo IPMP con múltiples interfaces” en la página 771](#).

1 En el sistema cuyas interfaces de reserva se deben configurar, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Configure una interfaz como reserva y asigne la dirección de prueba.

```
# ifconfig interface plumb \  
ip-address other-parameters deprecated -failover standby up
```

Una interfaz de reserva sólo puede tener una dirección IP (la dirección de prueba). Debe configurar la opción `-failover` antes de configurar la opción `standby up`. Para `<other-parameters>`, utilice los parámetros que requiera su configuración, según lo descrito en la página del comando `man ifconfig(1M)`.

- Por ejemplo, para crear una dirección de prueba IPv4, debe escribir el siguiente comando:

```
# ifconfig hme1 plumb 192.168.85.22 netmask + broadcast + deprecated -failover standby up
```

hme1	Define hme1 como interfaz típica para configurar como interfaz de reserva.
192.168.85.22	Asigna esta dirección de prueba a la interfaz de reserva.
deprecated	Indica que la dirección de prueba no se utiliza para los paquetes salientes.
-failover	Indica que la dirección de prueba no conmuta por error si falla la interfaz.
standby	Marca la interfaz como interfaz de reserva.

- Por ejemplo, para crear una dirección de prueba IPv6, debe escribir el siguiente comando:

```
# ifconfig hme1 plumb -failover standby up
```

3 Compruebe los resultados de la configuración de la interfaz de reserva.

```
# ifconfig hme1  
hme1: flags=69040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER,  
STANDBY,INACTIVE mtu 1500  
index 4 inet 192.168.85.22 netmask ffffffff broadcast 19.16.85.255  
groupname test
```

El indicador `INACTIVE` significa que esta interfaz no se utiliza para ningún paquete saliente. Cuando se produce una conmutación por error en esta interfaz de reserva, se borra el indicador `INACTIVE`.

Nota – Puede ver el estado de una interfaz en cualquier momento escribiendo el comando `ifconfig interfaz`. Para más información sobre cómo ver el estado de la interfaz, consulte [“Cómo obtener información sobre una interfaz específica” en la página 205](#).

4 (Opcional) Mantenga la interfaz de reserva IPv4 después de reiniciar.

Asigne la interfaz de reserva al mismo grupo IPMP, y configure una dirección de prueba para la interfaz de reserva.

Por ejemplo, para configurar hme1 como interfaz de reserva, debe agregar la siguiente línea al archivo `/etc/hostname.hme1`:

```
192.168.85.22 netmask + broadcast + deprecated group test -failover standby up
```

5 (Opcional) Conserve la interfaz de reserva IPv6 tras los reinicios.

Asigne la interfaz de reserva al mismo grupo IPMP, y configure una dirección de prueba para la interfaz de reserva.

Por ejemplo, para configurar hme1 como interfaz de reserva, agregue la línea siguiente al archivo `/etc/hostname6.hme1`:

```
-failover group test standby up
```

Ejemplo 31–4 Configuración de una interfaz de reserva para un grupo IPMP

Supongamos que desea crear una dirección de prueba con la siguiente configuración:

- La interfaz física hme2 como interfaz de reserva.
- La dirección de prueba 192.168.85.22.
- Las opciones `deprecated` y `-failover` configuradas.
- La dirección de emisión y la máscara de red se configuran con el valor predeterminado.

Debe escribir lo siguiente:

```
# ifconfig hme2 plumb 192.168.85.22 netmask + broadcast + \
deprecated -failover standby up
```

La interfaz se marca como interfaz de reserva sólo después de que la dirección se marque como dirección `NOFAILOVER`.

Debe eliminar el estado de reserva de una interfaz escribiendo lo siguiente:

```
# ifconfig interface -standby
```

Configuración de grupos IPMP con una única interfaz física

Cuando sólo tiene una interfaz en un grupo IPMP, no es posible conmutar tras un fallo. Sin embargo, puede activar la función de detección de fallos en dicha interfaz asignándola a un grupo IPMP. No es necesario que configure una dirección IP de prueba dedicada para establecer la detección de fallos para un grupo IPMP de interfaz única. Puede utilizar una sola dirección IP para enviar datos y detectar los fallos.

▼ **Cómo configurar un grupo IPMP de interfaz única**

- 1 En el sistema con el eventual grupo IPMP de interfaz única, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 Para IPv4, cree el grupo IPMP de interfaz única.**

Utilice la siguiente sintaxis para asignar la interfaz única a un grupo IPMP.

```
# ifconfig interface group group-name
```

El ejemplo siguiente asigna la interfaz hme0 al grupo IPMP v4test:

```
# ifconfig hme0 group v4test
```

Tras realizar este paso, IPMP permite la detección de fallos basada en vínculos en la interfaz.

Además, puede utilizar el subcomando `-failover` del comando `ifconfig` para habilitar la detección de fallos basada en sonda. En el ejemplo siguiente se muestra la detección de fallos basada en sonda de hme0 mediante la dirección IP asignada actualmente a hme0:

```
# ifconfig hme0 -failover
```

A diferencia de los grupos de interfaz múltiple, la misma dirección IP puede ser de datos y de prueba. Para que las aplicaciones puedan utilizar la dirección de prueba como dirección de datos, las direcciones de prueba nunca se deben marcar como deprecated en los grupos IPMP de interfaz única.

- 3 Para IPv6, cree el grupo IPMP de interfaz única.**

Utilice la siguiente sintaxis para asignar la interfaz única a un grupo IPMP:

```
# ifconfig interface inet6 group group-name
```

Por ejemplo, para agregar la interfaz única hme0 en el grupo IPMP v6test, escriba lo siguiente:

```
# ifconfig hme0 inet6 group v6test
```

Tras realizar este paso, IPMP permite la detección de fallos basada en vínculos en la interfaz.

Además, puede utilizar el subcomando `-failover` del comando `ifconfig` para habilitar la detección de fallos basada en sonda. En el ejemplo siguiente se muestra la detección de fallos basada en sonda de hme0 mediante la dirección IP asignada actualmente a hme0:

```
# ifconfig hme0 inet6 -failover
```

A diferencia de los grupos de interfaz múltiple, la misma dirección IP puede ser de datos y de prueba. Para que las aplicaciones puedan utilizar la dirección de prueba como dirección de datos, las direcciones de prueba nunca se deben marcar como deprecated en los grupos IPMP de interfaz única.

En una configuración de interfaz física única, no puede comprobar si ha fallado el sistema de destino que se está sondeando o la interfaz. El sistema de destino se puede sondear mediante una única interfaz física. Si sólo hay un enrutador predeterminado en la subred, desactive IPMP si hay una única interfaz física en el grupo. Si existe un enrutador distinto para IPv4 e IPv6, o hay varios enrutadores predeterminados, debe sondearse más de un sistema de destino. De este modo, podrá activar IPMP de un modo seguro.

Mantenimiento de grupos IPMP

Esta sección contiene las tareas para mantener los grupos IPMP existentes y las interfaces que los componen. Las tareas presuponen que ya se ha configurado un grupo IPMP, tal como se explica en [“Configuración de grupos IPMP” en la página 769](#).

▼ Cómo mostrar la pertenencia de una interfaz a un grupo IPMP

- 1 **En el sistema con la configuración de grupo IPMP, conviértase en superusuario o asuma un rol equivalente.**
Las funciones incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre las funciones, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 **Visualice la información sobre la interfaz, incluido el grupo al que pertenece la interfaz.**
`# ifconfig interface`
- 3 **Si es preciso, visualice la información de IPv6 para la interfaz.**
`# ifconfig interface inet6`

Ejemplo 31–5 Visualización de grupos de interfaces físicas

Para mostrar el nombre de grupo para hme0, debe escribir lo siguiente:

```
# ifconfig hme0
hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2 inet 192.168.85.19 netmask ffffffff broadcast 192.168.85.255
groupname testgroup1
```

Para mostrar el nombre de grupo sólo para la información de IPv6, debe escribir:

```
# ifconfig hme0 inet6
   hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
       inet6 fe80::a00:20ff:feb9:19fa/10
       groupname testgroup1
```

▼ Cómo agregar una interfaz a un grupo IPMP

- 1 En el sistema con la configuración de grupo IPMP, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 Agregue la interfaz al grupo IPMP.

```
# ifconfig interface group group-name
```

La interfaz especificada en *interfaz* se convierte en miembro del grupo IPMP *nombre_grupo*.

Ejemplo 31–6 Adición de una interfaz a un grupo IPMP

Para agregar hme0 al grupo IPMP testgroup2, escriba el comando siguiente:

```
# ifconfig hme0 group testgroup2
   hme0: flags=9000843<UP ,BROADCAST,RUNNING,MULTICAST,IPv4,NOFAILOVER> mtu 1500 index 2
       inet 192.168.85.19 netmask ff000000 broadcast 10.255.255.255
       groupname testgroup2
       ether 8:0:20:c1:8b:c3
```

▼ Cómo eliminar una interfaz de un grupo IPMP

Al ejecutar el parámetro group del comando ifconfig con una cadena nula, la interfaz se elimina de su grupo IPMP actual. Tenga cuidado al eliminar interfaces de un grupo. Si ha fallado otra interfaz del grupo IPMP, es posible que se haya producido una conmutación por error anteriormente. Por ejemplo, si hme0 ha fallado previamente, todas las direcciones serán fallidas para hme1, si hme1 forma parte del mismo grupo. La eliminación de hme1 del grupo hace que el daemon in.mpathd devuelva todas las direcciones de conmutación por error a otra interfaz del grupo. Si no hay otras interfaces en funcionamiento en el grupo, es posible que la conmutación por error no restaure todos los accesos de la red.

De un modo similar, cuando se debe desconectar una interfaz de un grupo, primero es preciso eliminar la interfaz del grupo. A continuación, asegúrese de que la interfaz tiene configuradas

todas las direcciones IP originales. El daemon `in.mpathd` trata de restaurar la configuración original de una interfaz que se elimina del grupo. Debe asegurarse de que se restaure la configuración antes de desconectar la interfaz. Consulte [“Qué ocurre durante la conmutación por error de la interfaz” en la página 761](#) para ver el aspecto de las interfaces antes y después de una conmutación por error.

1 En el sistema con la configuración de grupo IPMP, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Elimine la interfaz del grupo IPMP.

```
# ifconfig interface group ""
```

Las comillas indican una cadena nula.

Ejemplo 31–7 Eliminación de una interfaz de un grupo

Para eliminar `hme0` del grupo IPMP `test`, escriba el comando siguiente:

```
# ifconfig hme0 group ""
# ifconfig hme0
hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2 inet 192.168.85.19 netmask fffffff0 broadcast 192.168.85.255
# ifconfig hme0 inet6
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
inet6 fe80::a00:20ff:feb9:19fa/10
```

▼ Cómo mover una interfaz de un grupo IPMP a otro grupo

Puede colocar una interfaz en un nuevo grupo IPMP cuando la interfaz pertenece a un grupo IPMP existente. No es necesario eliminar la interfaz del grupo IPMP actual. Cuando coloca la interfaz en un nuevo grupo, se elimina automáticamente de cualquier grupo IPMP existente.

1 En el sistema con la configuración de grupo IPMP, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Mueva la interfaz a un nuevo grupo IPMP.

```
# ifconfig interface group group-name
```

Al colocar la interfaz en un nuevo grupo se elimina automáticamente la interfaz de cualquier grupo existente.

Ejemplo 31-8 Cómo mover una interfaz a otro grupo IPMP

Para cambiar el grupo IPMP de la interfaz hme0, escriba:

```
# ifconfig hme0 group cs-link
```

Con este comando se elimina la interfaz hme0 del grupo IPMP test y se coloca en el grupo cs-link.

Sustitución de una interfaz física fallida en sistemas que admiten reconfiguración dinámica

Esta sección contiene los procedimientos relativos a la administración de sistemas que admiten reconfiguración dinámica (DR).

Nota – Las tareas sólo se aplican a las capas IP configuradas con el comando `ifconfig`. Las capas que hay delante o detrás de la capa IP, como ATM u otros servicios, requieren pasos manuales específicos si las capas no están automatizadas. Los pasos de los procedimientos siguientes permiten desconfigurar interfaces durante la desconexión previa y configurarlas tras la conexión posterior.

▼ Cómo eliminar una interfaz física que ha fallado (desconexión en DR)

Este procedimiento muestra cómo eliminar una interfaz física de un sistema que admite DR. El procedimiento presupone la existencia de las siguientes condiciones:

- Las interfaces físicas hme0 y hme1 son las interfaces de ejemplo.
- Ambas interfaces se encuentran en el mismo grupo IPMP.
- hme0 ha fallado.
- La interfaz lógica hme0:1 tiene la dirección de prueba.
- Se está sustituyendo la interfaz fallida por el mismo nombre de interfaz física, por ejemplo hme0 por hme0.

Nota – Puede omitir el paso 2 si la dirección de prueba se conecta utilizando el archivo `/etc/hostname.hme0`.

- 1 **En el sistema con la configuración de grupo IPMP, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Visualice la configuración de la dirección de prueba.**

```
# ifconfig hme0:1
```

```
hme0:1:
flags=9040842<BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
mtu 1500 index 3
inet 192.168.233.250 netmask ffffffff broadcast 192.168.233.255
```

Esta información es necesaria para volver a sondear la dirección de prueba cuando se reemplaza la interfaz física.

- 3 **Elimine la interfaz física.**

Consulte las siguientes fuentes para obtener una descripción completa sobre cómo eliminar la interfaz física:

- Página del comando `man cfgadm(1M)`
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*
- *Sun Enterprise 10000 DR Configuration Guide*

▼ Como sustituir una interfaz física que ha fallado (conexión en DR)

Este procedimiento muestra cómo reemplazar una interfaz física en un sistema que admite DR.

- 1 **En el sistema con la configuración de grupo IPMP, asuma el rol de administrador principal o conviértase en superusuario.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Reemplace la interfaz física.**

Consulte las instrucciones que se incluyen en las siguientes fuentes:

- Página del comando `man cfgadm(1M)`
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*
- *Sun Enterprise 10000 DR Configuration Guide* o *Sun Fire 880 Dynamic Reconfiguration User's Guide*

Recuperación de una interfaz física que no estaba presente durante el inicio del sistema

Nota – El siguiente procedimiento sólo se aplica a las capas IP configuradas con el comando `ifconfig`. Las capas que hay delante o detrás de la capa IP, como ATM u otros servicios, requieren pasos manuales específicos si las capas no están automatizadas. Los pasos específicos del siguiente procedimiento permiten desconfigurar interfaces durante la desconexión previa y configurarlas tras la conexión posterior.

La recuperación tras la reconfiguración dinámica es automática para una interfaz que forma parte de la placa de E/S de una plataforma Sun Fire™. Si la tarjeta NIC es una Sun Crypto Accelerator I - cPCI, la recuperación también es automática. Como resultado, no es necesario realizar los pasos siguientes para una interfaz que se recupera como parte de una operación de DR. Para obtener más información sobre los sistemas Sun Fire x800 y Sun Fire 15000, consulte la página del comando `man cfgadm_sbd(1M)`. La interfaz física vuelve a la configuración especificada en el archivo `/etc/hostname.interface`. Consulte “Configuración de grupos IPMP” en la página 769 para obtener más detalles sobre cómo configurar las interfaces para que conserven la configuración tras un reinicio.

Nota – En los sistemas Sun Fire (Exx00) antiguos, la desconexión DR sigue estando sujeta a los procedimientos manuales. Sin embargo, las conexiones en DR están automatizadas.

▼ Cómo recuperar una interfaz física que no está presente al iniciar el sistema

Debe completar el procedimiento siguiente para recuperar una interfaz física que no estaba presente al iniciar el sistema. El ejemplo de este procedimiento está configurado del modo siguiente:

- Las interfaces físicas son `hme0` y `hme1`.
- Ambas interfaces se encuentran en el mismo grupo IPMP.
- `hme0` no estaba instalada durante el inicio del sistema.

Nota – La recuperación tras error de direcciones IP durante la recuperación de una interfaz física fallida puede tardar hasta tres minutos. Este tiempo puede variar en función del tráfico de la red. El tiempo también depende de la estabilidad de la interfaz entrante para recuperar las interfaces fallidas mediante el daemon `in.mpathd`.

1 En el sistema con la configuración de grupo IPMP, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Recupere la información de red fallida del mensaje de error del registro de la consola.

Consulte la página del comando `man syslog(3C)`. El mensaje de error podría ser similar al siguiente:

```
moving addresses from failed IPv4 interfaces:
hme1 (moved to hme0)
```

Este mensaje indica que las direcciones IPv4 de la interfaz fallida hme1 han fallado para la interfaz hme0.

También podría recibir un mensaje como el siguiente:

```
moving addresses from failed IPv4 interfaces:
hme1 (couldn't move, no alternative interface)
```

Este mensaje indica que no se ha podido encontrar ninguna interfaz activa en el mismo grupo que la interfaz fallida hme1. Por tanto, las direcciones IPv4 de hme1 no se han podido conmutar por error.

3 Conecte la interfaz física al sistema.

Consulte las siguientes instrucciones para reemplazar la interfaz física:

- Página del comando `man cfgadm(1M)`
- *Sun Enterprise 10000 DR Configuration Guide*
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*

4 Consulte el contenido del paso 2. Si no se pueden mover las direcciones, vaya al paso 6. Si se han podido mover las direcciones, continúe con el paso 5.

5 Desconecte las interfaces lógicas que se configuraron como parte del proceso de conmutación por error.

a. Revise el contenido del archivo `/etc/hostname.movido_de_interfaz` para determinar qué interfaces lógicas se han configurado como parte del proceso de conmutación por error.

b. Desconecte cada dirección IP de conmutación por error.

```
# ifconfig moved-to-interface removeif moved-ip-address
```

Nota – Las direcciones de conmutación por error se marcan con el parámetro `failover`, o no se marcan con el parámetro `-failover`. No es necesario desconectar las direcciones IP marcadas con `-failover`.

Por ejemplo, supongamos que el contenido del archivo `/etc/hostname.hme0` contiene las líneas siguientes:

```
inet 10.0.0.4 -failover up group one
addif 10.0.0.5 failover up
addif 10.0.0.6 failover up
```

Para desconectar cada dirección IP de conmutación tras error, escriba los comandos siguientes:

```
# ifconfig hme0 removeif 10.0.0.5
# ifconfig hme0 removeif 10.0.0.6
```

6 Reconfigure la información de IPv4 para la interfaz física reemplazada escribiendo el comando siguiente para cada interfaz eliminada:

```
# ifconfig removed-from-NIC <parameters>
```

Por ejemplo, escriba:

```
# ifconfig hme1 inet plumb
# ifconfig hme1 inet 10.0.0.4 -failover up group one
# ifconfig hme1 addif 10.0.0.5 failover up
# ifconfig hme1 addif 10.0.0.6 failover up
```

Modificación de configuraciones IPMP

Utilice el archivo de configuración IPMP `/etc/default/mpathd` para configurar los siguientes parámetros del sistema para los grupos IPMP.

- `FAILURE_DETECTION_TIME`
- `TRACK_INTERFACES_ONLY_WITH_GROUPS`
- `FAILBACK`

▼ Cómo configurar el archivo `/etc/default/mpathd`

- 1 En el sistema con la configuración de grupo IPMP, asuma el rol de administrador principal o conviértase en superusuario.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 Edite el archivo `/etc/default/mpathd`.

Cambie el valor predeterminado de uno o más de los tres parámetros.

- a. Escriba el nuevo valor para el parámetro `FAILURE_DETECTION_TIME`.

```
FAILURE_DETECTION_TIME=n
```

donde *n* es el tiempo en segundos para que los sondeos ICMP detecten si se ha producido un fallo de la interfaz. El valor predeterminado es de 10 segundos.

- b. Escriba el nuevo valor para el parámetro `FAILBACK`.

```
FAILBACK=[yes | no]
```

- *yes*: El valor *yes* es el comportamiento de recuperación tras fallo predeterminado de IPMP. Cuando se detecta la reparación de una interfaz fallida, el acceso de red recupera la interfaz reparada, tal como se describe en [“Funciones de detección de fallos IPMP y recuperación”](#) en la página 758.

- *no*: El valor *no* indica que el tráfico de datos no se devuelve a una interfaz reparada. Cuando se detecta la reparación de una interfaz fallida, se configura el indicador *INACTIVE* para dicha interfaz. Este indicador significa que la interfaz no se va a utilizar para el tráfico de datos. La interfaz se puede seguir utilizando para el tráfico de sondeos.

Por ejemplo, supongamos que un grupo IPMP se compone de dos interfaces, `ce0` y `ce1`. A continuación, supongamos que se configura el valor `FAILBACK=no` en `/etc/default/mpathd`. Si falla `ce0`, su tráfico fallará para `ce1`, de acuerdo con el comportamiento de IPMP. No obstante, cuando IPMP detecta que se ha reparado `ce0`, el tráfico no se recupera de `ce1`, debido al parámetro `FAILBACK=no` de `/etc/default/mpathd`. La interfaz `ce0` conserva su estado *INACTIVE* y no se utiliza para tráfico a menos que falle la interfaz `ce1`. Si falla la interfaz `ce1`, las direcciones de `ce1` se migran de nuevo a `ce0`, cuyo indicador *INACTIVE* se borra. Esta migración tiene lugar siempre y cuando `ce0` sea la única interfaz *INACTIVE* del grupo. Si hay otras interfaces *INACTIVE* en el grupo, las direcciones podrían migrarse a una interfaz *INACTIVE* que no sea `ce0`.

- c. Escriba el nuevo valor para el parámetro `TRACK_INTERFACES_ONLY_WITH_GROUPS`.

```
TRACK_INTERFACES_ONLY_WITH_GROUPS=[yes | no]
```

- *yes*: El valor *yes* es el comportamiento predeterminado de IPMP. Este parámetro hace que IPMP omita las interfaces de red que no están configuradas en un grupo IPMP.
- *no*: El valor *no* define la detección de fallos y la reparación para *todas* las interfaces de red, independientemente de si están configuradas en un grupo IPMP. Sin embargo, cuando se detecta un fallo o reparación en una interfaz que no está configurada en un grupo IPMP, no tiene lugar ninguna recuperación tras error o conmutación por error. Por tanto, el valor *no* sólo resulta útil para comunicar errores y no mejora directamente la disponibilidad de la red.

3 Reinicie el daemon `in.mpathd`.

```
# kill -HUP in.mpathd
```

P A R T E V I I

Calidad de servicio IP (IPQoS)

Esta sección contiene tareas e información sobre Calidad de servicio IP (IPQoS), la implementación de servicios diferenciados de Oracle Solaris.

Introducción a IPQoS (Descripción general)

IP Quality of Service (IPQoS) permite priorizar, controlar y realizar un seguimiento de las estadísticas de control. Utilizando IPQoS, puede ofrecer un nivel de servicio estable a los usuarios de la red. También puede administrar el tráfico para evitar que se congestione la red.

A continuación puede ver una lista de temas de este capítulo:

- “Conceptos básicos de IPQoS” en la página 793
- “Proporcionar calidad de servicio con IPQoS” en la página 796
- “Mejorar la eficacia de la red con IPQoS” en la página 797
- “Modelo de servicios diferenciados” en la página 799
- “Reenvío del tráfico en una red con IPQoS” en la página 804

Conceptos básicos de IPQoS

IPQoS posibilita la arquitectura de servicios diferenciados (Diffserv) definida por el grupo de trabajo de servicios diferenciados de IETF (Internet Engineering Task Force). En Oracle Solaris, IPQoS se implementa en el nivel de IP de la pila de protocolo TCP/IP.

¿Qué son los servicios diferenciados?

Utilizando IPQoS, puede proporcionar diferentes niveles de servicio de red para clientes seleccionados y aplicaciones específicas. Los diferentes niveles de servicios se denominan *servicios diferenciados*. Los servicios diferenciados que se proporcionan a los clientes pueden estar basados en una estructura de niveles de servicio que su compañía ofrezca a los clientes. También puede ofrecer servicios diferenciados según las prioridades definidas para aplicaciones o usuarios de la red.

Para proporcionar calidad de servicio se deben llevar a cabo las siguientes actividades:

- Delegar los niveles de servicio a diferentes grupos, como clientes o departamentos de una empresa

- Priorizar los servicios de red que se ofrecen a grupos o aplicaciones específicos
- Descubrir y eliminar áreas de cuello de botella de la red y otros tipos de congestión
- Supervisar el rendimiento de la red y proporcionar estadísticas de rendimiento
- Regular el ancho de banda hasta y desde recursos de red

Funciones de IPQoS

IPQoS proporciona las siguientes funciones:

- `ipqosconf` Herramienta de línea de comandos para configurar la directiva QoS
- Clasificador que selecciona acciones basadas en filtros que configuran la directiva QoS de la organización
- Módulo de medición para medir el tráfico de red que cumple el modelo Diffserv
- Diferenciación del servicio basada en la posibilidad de marcar el encabezado IP de un paquete con información de redirección
- Módulo de control de flujo que realiza un seguimiento de las estadísticas de flujo de tráfico
- Seguimiento de las estadísticas de clases de tráfico mediante el uso del comando UNIX® `kstat`
- Compatibilidad con la arquitectura SPARC® y x86
- Compatibilidad con direcciones IPv4 e IPv6
- Interoperatividad con la arquitectura de seguridad IPsec
- Compatibilidad con marcados de prioridad de usuario 802.1D para redes de área local virtuales (VLAN)

Dónde obtener más información sobre la teoría y práctica de la calidad del servicio

Puede obtener información sobre servicios diferenciados y calidad del servicio de diferentes fuentes impresas y en línea.

Libros sobre la calidad del servicio

Si necesita más información sobre la teoría y la práctica de la calidad del servicio, consulte los siguientes libros:

- Ferguson, Paul y Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Kilkki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.

Petición de comentarios (RFC) sobre la calidad de servicio

IPQoS cumple las especificaciones descritas en las siguientes RFC y borradores de Internet:

- [RFC 2474, Definición del campo de servicios diferenciados \(DS\) en los encabezados IPv4 e IPv6](http://www.ietf.org/rfc/rfc2474.txt?number=2474) (<http://www.ietf.org/rfc/rfc2474.txt?number=2474>): describe una mejora del campo de tipo de servicio (ToS) o campos DS de los encabezados de paquetes IPv4 e IPv6 para admitir servicios diferenciados.
- [RFC 2475, An Architecture for Differentiated Services](http://www.ietf.org/rfc/rfc2475.txt?number=2475) (<http://www.ietf.org/rfc/rfc2475.txt?number=2475>): proporciona una descripción detallada de la organización y de los módulos de la arquitectura Diffserv.
- [RFC 2597, Assured Forwarding PHB Group](http://www.ietf.org/rfc/rfc2597.txt?number=2597) (<http://www.ietf.org/rfc/rfc2597.txt?number=2597>): describe cómo funciona el comportamiento por salto del reenvío asegurado (AF).
- [RFC 2598, An Expedited Forwarding PHB](http://www.ietf.org/rfc/rfc2598.txt?number=2598) (<http://www.ietf.org/rfc/rfc2598.txt?number=2598>): describe cómo funciona el comportamiento por salto de reenvío acelerado (EF).
- Borrador de Internet, *Un modelo de administración informal para enrutadores Diffserv*: presenta un modelo para implementar la arquitectura Diffserv en enrutadores.

Sitios web con información sobre calidad del servicio

El grupo de trabajo sobre servicios diferenciados del IETF mantiene un sitio web con vínculos a borradores de Internet sobre Diffserv:

<http://www.ietf.org/html.charters/diffserv-charter.html>.

Los fabricantes de enrutadores, como Cisco Systems y Juniper Networks, proporcionan información en sus sitios web corporativos sobre cómo implementar servicios diferenciados en sus productos.

Páginas de comando man de IPQoS

La documentación de IPQoS incluye las siguientes páginas man:

- [ipqosconf\(1M\)](#) - Describe el comando para definir el archivo de configuración IPQoS
- [ipqos\(7ipp\)](#) - Describe la implementación IPQoS del modelo de arquitectura Diffserv
- [ipgpc\(7ipp\)](#) - Describe la implementación IPQoS de un clasificador Diffserv
- [tokenmt\(7ipp\)](#) - Describe el medidor IPQoS tokenmt
- [tswtclmt\(7ipp\)](#) - Describe el medidor IPQoS tswtclmt
- [dscpmk\(7ipp\)](#) - Describe el módulo marcador DSCP
- [dlcosmk\(7ipp\)](#) - Describe el módulo marcador de prioridad de usuario IPQoS 802.1D
- [flowacct\(7ipp\)](#) - Describe el módulo de control de flujo IPQoS

- `acctadm(1M)`: describe el comando de configuración de funciones de contabilidad ampliada de Oracle Solaris. El comando `acctadm` incluye extensiones IPQoS.

Proporcionar calidad de servicio con IPQoS

Las funciones IPQoS permiten a los proveedores de Internet (ISP) y proveedores de aplicaciones (ASP) ofrecer diferentes niveles de servicio de red a los clientes. Estas funciones permiten a las empresas e instituciones educativas priorizar servicios para organizaciones internas o aplicaciones principales.

Utilización de acuerdos de nivel de servicio

Si su organización es un ISP o ASP, puede basar la configuración IPQoS en el *acuerdo de nivel de servicio* (SLA) que la empresa ofrezca a sus clientes. En un acuerdo SLA, un proveedor garantiza a un cliente un nivel de servicio de red específico según categorías de precios. Por ejemplo, un acuerdo SLA de máxima calidad garantiza que el cliente reciba la prioridad máxima para todos los tipos de tráfico de red 24 horas al día. Del mismo modo, un acuerdo SLA de calidad media garantiza que el cliente reciba prioridad máxima para el correo electrónico durante el horario de negocios. Y el resto de tráfico puede recibir prioridad media 24 horas al día.

Garantizar la calidad de servicio para una organización específica

Si su organización es una empresa o una institución, también puede proporcionar funciones de calidad de servicio para la red. Puede garantizar que el tráfico de un grupo específico o de una aplicación determinada reciba un grado de servicio mayor o menor.

Introducción a la directiva de calidad de servicio

Para utilizar la calidad de servicio es necesario definir una *directiva de calidad de servicio* (QoS). La política QoS define varios atributos de red, como prioridades de clientes o aplicaciones, y acciones para tratar diferentes categorías de tráfico. La directiva QoS de la organización se define en un archivo de configuración IPQoS. Este archivo configura los módulos IPQoS que residen en el núcleo de Oracle Solaris. Un host con una directiva IPQoS se considera un *sistema con IPQoS*.

Normalmente, la directiva QoS define lo siguiente:

- Grupos independientes de tráfico de red denominados *clases de servicio*.
- Sistemas de medición para regular la cantidad de tráfico de red de cada clase. Estas medidas controlan el proceso de control del tráfico denominado *medición*.

- Una acción que un sistema IPQoS y un enrutador Diffserv deben aplicar al flujo de un paquete. Este tipo de acción se denomina *comportamiento por salto* (PHB).
- Cualquier seguimiento de estadísticas que necesite su organización para una clase de servicio. Un ejemplo es el tráfico generado por un cliente o aplicación específicos.

Cuando los paquetes se transfieren a la red, el sistema con IPQoS evalúa los encabezados de los paquetes. La acción que realiza el sistema IPQoS la determina la directiva QoS.

Las tareas para diseñar la directiva QoS se describen en la sección [“Planificación de la directiva de calidad de servicio” en la página 813](#).

Mejorar la eficacia de la red con IPQoS

IPQoS incluye funciones que facilitan la mejora del rendimiento de la red al utilizar la calidad de servicio. Con la expansión de las redes informáticas, también aumenta la necesidad de administrar el tráfico de red generado por el número creciente de usuarios y los procesadores más potentes. Algunos de los síntomas de una red saturada son la pérdida de datos y la congestión del tráfico. Ambos síntomas dan como resultado tiempos de respuesta lentos.

En el pasado, los administradores de sistemas solucionaban los problemas de tráfico de red añadiendo más ancho de banda. A menudo, el nivel de tráfico de los vínculos variaba de manera notable. Con IPQoS, puede administrar el tráfico de la red y determinar con facilidad si es necesario realizar una expansión, y dónde.

Por ejemplo, para una compañía o institución, es necesario mantener una red efectiva para evitar los cuellos de botella. También es necesario garantizar que un grupo o aplicación no consume más ancho de banda del asignado. Para un proveedor ISP o ASP, es necesario administrar el rendimiento de la red para garantizar que los clientes reciben el servicio de red por el que pagan.

Cómo afecta el ancho de banda al tráfico de red

Puede usar IPQoS para regular el *ancho de banda* de la red, es decir, la cantidad máxima de datos que un vínculo de red o dispositivo puede transferir como límite máximo. La directiva QoS debe priorizar el uso del ancho de banda para proporcionar calidad de servicio a los clientes o usuarios. Los módulos de medición de IPQoS permiten medir y controlar la asignación de ancho de banda entre las diferentes clases de tráfico en un host con IPQoS.

Antes de poder administrar de manera efectiva el tráfico de la red, debe responder a estas preguntas sobre el uso del ancho de banda:

- ¿Cuáles son las áreas de problemas de tráfico de su red local?
- ¿Qué debe hacer para conseguir la utilización óptima del ancho de banda disponible?

- ¿Cuáles son las aplicaciones de mayor importancia de su organización que deben tener la prioridad máxima?
- ¿Qué aplicaciones pueden congestionarse?
- ¿Cuáles son las aplicaciones de menor importancia, que pueden tener la prioridad más baja?

Utilización de clases de servicio para priorizar el tráfico

Para utilizar la calidad de servicio, debe analizar el tráfico de la red para determinar los grandes grupos en los que se puede dividir el tráfico. Después, debe organizar los grupos en clases de servicio con características y prioridades individuales. Estas clases forman las categorías básicas en las que se basa la directiva QoS de la organización. Las clases de servicio representan los grupos de tráfico que se desea controlar.

Por ejemplo, un proveedor puede ofrecer niveles de servicio platino, oro, plata y bronce, con una escala de diferentes precios. Un acuerdo SLA platino puede garantizar una prioridad máxima para el tráfico entrante destinado a un sitio web que el ISP aloja para el cliente. Por lo tanto, el tráfico entrante del sitio web del cliente podría ser una clase de tráfico.

Para una empresa, se pueden crear clases de servicio basadas en los requisitos de los departamentos. También se pueden crear clases basadas en el nivel de utilización de una aplicación específica en el tráfico de red. A continuación puede ver algunos ejemplos de clases de tráfico de una empresa:

- Aplicaciones muy utilizadas, como correo electrónico y FTP saliente a un servidor específico, cada una podría ser una clase. Debido a que los empleados utilizan estas aplicaciones constantemente, su directiva QoS puede garantizar una pequeña cantidad de ancho de banda y una prioridad más baja al correo electrónico y FTP.
- Una base de datos de entrada que debe estar activa las 24 horas del día. Según la importancia de la aplicación de base de datos para la empresa, puede asignarle una gran cantidad de ancho de banda y una prioridad alta.
- Un departamento que realiza un trabajo de vital importancia o que debe tratarse con cuidado, como el departamento de salarios y nóminas. La importancia del departamento para la organización determina la prioridad y la cantidad de ancho de banda que se le asignará.
- Llamadas entrantes al sitio web externo de una compañía. A esta clase se le puede asignar una pequeña cantidad de ancho de banda con prioridad baja.

Modelo de servicios diferenciados

IPQoS incluye los siguientes módulos, que forman parte de la arquitectura *Diffserv* (*servicios diferenciados*) definida en RFC 2475:

- Clasificador
- Medidor
- Marcador

IPQoS añade las siguientes mejoras al modelo Diffserv:

- Módulo de control de flujo
- Marcador de datagrama 802.1D

En esta sección se explican los módulos Diffserv tal y como se utilizan en IPQoS. Es necesario conocer estos módulos, sus nombres y su utilización para configurar la directiva QoS. Si necesita información detallada sobre cada módulo, consulte la sección “[Arquitectura IPQoS y el modelo Diffserv](#)” en la página 871.

Descripción general del clasificador (ipgpc)

En el modelo Diffserv, el *clasificador* selecciona paquetes del flujo de tráfico de una red. Un *flujo de tráfico* consiste en un grupo de paquetes con información idéntica en los siguientes campos de encabezado de IP:

- Dirección de origen
- Dirección de destino
- Puerto de origen
- Puerto de destino
- Número de protocolo

En IPQoS, estos campos se conocen como *5-tuple*.

El módulo clasificador de IPQoS se llama *ipgpc*. El clasificador *ipgpc* organiza los flujos de tráfico en clases basada en características definidas en el archivo de configuración IPQoS.

Si necesita información detallada sobre *ipgpc*, consulte la sección “[Módulo Classifier](#)” en la página 871.

Clases IPQoS

Una *clase* es un grupo de flujos de red que comparten características similares. Por ejemplo, un ISP puede definir clases que representen los diferentes niveles de servicio ofrecidos a los clientes. Un ASP puede definir acuerdos SLA que asignen diferentes niveles de servicio a distintas aplicaciones. En la política QoS de un ASP, una clase puede incluir tráfico FTP saliente destinado a una dirección IP de destino específica. El tráfico saliente del sitio web externo de una empresa también puede definirse como una clase.

Agrupar el tráfico en clases es una parte importante de la planificación de la directiva QoS. Al crear clases utilizando la herramienta `ipqosconf`, se está configurando el clasificador `ipgpc`.

Si necesita información sobre cómo definir clases, consulte la sección [“Cómo definir las clases de la directiva QoS” en la página 816](#).

Filtros IPQoS

Los *filtros* son conjuntos de reglas que contienen parámetros denominados *selectores*. Cada filtro debe hacer referencia a una clase. IPQoS compara los paquetes con los selectores de cada filtro para determinar si el paquete pertenece a la clase del filtro. Se puede filtrar un paquete utilizando diferentes selectores, por ejemplo, 5-tuple de IPQoS y otros parámetros comunes:

- Dirección de origen y dirección de destino
- Puerto de origen y puerto de destino
- Números de protocolo
- ID de usuario
- ID de proyecto
- Punto de código de servicios diferenciados (DSCP)
- Índice de interfaz

Por ejemplo, un filtro sencillo puede incluir el puerto de destino con un valor de 80. A continuación, el clasificador `ipgpc` selecciona todos los paquetes que están vinculados con el puerto de destino 80 (HTTP) y gestiona los paquetes según lo estipulado en la directiva QoS.

Si necesita información sobre cómo crear filtros, consulte la sección [“Cómo definir filtros en la directiva QoS” en la página 819](#).

Descripción general de medidor (`tokenmt` y `tswtclmt`)

En el modelo Diffserv, el *medidor* controla la tasa de transmisión de los flujos de tráfico por clase. El medidor evalúa la medida en que la tasa actual del flujo se ajusta a las tasas configuradas para determinar el resultado apropiado. Según el resultado de los flujos de tráfico, el medidor selecciona una acción subsiguiente. Las acciones subsiguientes pueden incluir enviar el paquete a otra acción o devolver el paquete a la red sin más procesamiento.

Los medidores IPQoS determinan si un flujo de red cumple la tasa de transmisión definida para su clase en la directiva QoS. IPQoS incluye dos módulos de medición:

- `tokenmt` – Utiliza un esquema de medición con conjunto de dos tokens
- `tswtclmt` – Utiliza un esquema de medición de ventana de lapso de tiempo

Ambos módulos de medición reconocen tres resultados: rojo, amarillo y verde. Las acciones que deben tomarse para cada resultado se definen en los parámetros `red_action_name`, `yellow_action_name` y `green_action_name`.

También puede configurar `tokenmt` para que tenga presente el color. Una instancia de medición que tenga presente el color utiliza el tamaño del paquete, DSCP, tasa de tráfico y parámetros configurados para determinar el resultado. El medidor utiliza el DSCP para asignar el resultado del paquete al color verde, amarillo o rojo.

Si necesita información sobre cómo definir parámetros para los medidores IPQoS, consulte la sección [“Cómo planificar el control de flujo” en la página 820](#).

Descripción general de marcadores (`dscpmk` y `dlsosmk`)

En el modelo Diffserv, el *marcador* marca un paquete con un valor que refleja un comportamiento de redirección. El *marcado* es el proceso de colocar un valor en el encabezado del paquete para indicar cómo se debe reenviar el paquete a la red. IPQoS contiene dos módulos de marcado:

- `dscpmk`: marca el campo DS del encabezado de un paquete IP con un valor numérico denominado *punto de código de servicios diferenciados* o DSCP. Un enrutador que admita Diffserv puede utilizar el punto de código DS para aplicar el comportamiento de reenvío correspondiente al paquete.
- `dlsosmk` – Marca la etiqueta de red de área local virtual (VLAN) del encabezado de un frame Ethernet con un valor numérico denominado *prioridad de usuario*. La prioridad de usuario indica la *clase de servicio* (CoS), que define el comportamiento de reenvío que debe aplicarse al datagrama.

`dlsosmk` es una adición de IPQoS que no forma parte del modelo Diffserv designado por IETF.

Si necesita información sobre cómo utilizar un sistema de marcadores para la directiva QoS, consulte [“Cómo planificar el comportamiento de reenvío” en la página 823](#).

Descripción general del control de flujo (`flowacct`)

IPQoS añade el módulo de control `flowacct` al modelo Diffserv. El módulo `flowacct` puede usarse para recopilar estadísticas sobre el flujo de tráfico y cobrar a los clientes según su acuerdo SLA. El control de flujo también es útil para la planificación de la capacidad y la supervisión de sistemas.

El módulo `flowacct` puede usarse con el comando `acctadm` para crear un archivo de registro de control. Un registro básico incluye IPQoS 5-tuple y dos atributos adicionales, como se muestra en la siguiente lista:

- Dirección de origen
- Puerto de origen
- Dirección de destino

- Puerto de destino
- Número de protocolo
- Número de paquetes
- Número de bytes

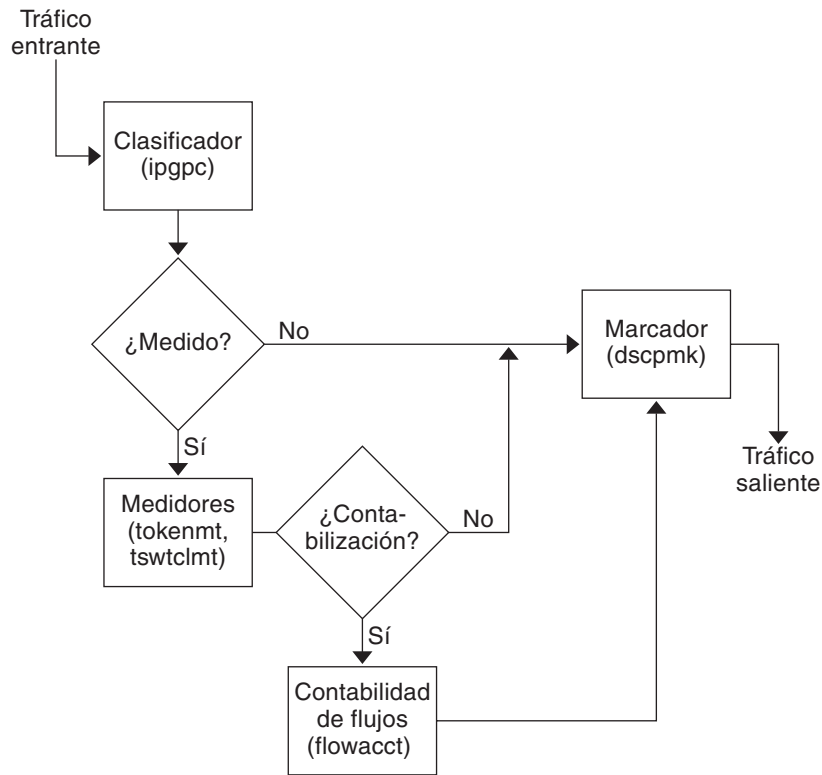
También puede recopilar estadísticas de otros atributos, como se describe en la sección [“Registro de información sobre flujos de tráfico” en la página 866](#), y en las páginas de comando `man flowacct(7ipp)` y `acctadm(1M)`.

Si necesita más información sobre cómo planificar una estrategia de control de flujo, consulte la sección [“Cómo planificar la recopilación de datos de flujo” en la página 825](#).

Cómo fluye el tráfico a través de los módulos IPQoS

En la siguiente figura se muestra una ruta que puede tomar el tráfico entrante a través de algunos de los módulos IPQoS.

FIGURA 32-1 Flujo de tráfico a través de la implementación IPQoS del modelo Diffserv



Esta figura ilustra una secuencia de flujo de tráfico común en un sistema con IPQoS:

1. El clasificador selecciona todos los paquetes del flujo que cumplen los criterios de filtrado de la directiva QoS del sistema.
2. A continuación, se evalúan los paquetes para determinar la acción que se debe ejecutar.
3. El clasificador envía al marcador cualquier tráfico que no requiera control de flujo.
4. El tráfico que requiere control de flujo se envía al medidor.
5. El medidor fuerza la tasa configurada. A continuación, el medidor asigna un valor de cumplimiento de tráfico a los paquetes de flujo controlado.
6. Se evalúan los paquetes de flujo controlado para determinar si necesitan control.
7. El medidor envía al marcador el tráfico que no requiere control de flujo.
8. El módulo de control de flujo recopila estadísticas sobre los paquetes recibidos. A continuación, el módulo envía los paquetes al marcador.
9. El marcador asigna un punto de código DS al encabezado del paquete. Este DSCP indica el comportamiento por salto que un sistema con Diffserv debe aplicar al paquete.

Reenvío del tráfico en una red con IPQoS

En esta sección se explican los elementos relacionados con el reenvío de paquetes en una red con IPQoS. Un sistema con IPQoS gestiona cualquier paquete del flujo de la red con la dirección IP del sistema como destino. A continuación, aplica la directiva QoS al paquete para establecer servicios diferenciados.

Punto de código DS

El punto de código DS (DSCP) define en el encabezado del paquete la acción que cualquier sistema con Diffserv debe ejecutar en un paquete marcado. La arquitectura diffserv define un conjunto de puntos de código DS que utilizarán los sistemas con IPQoS y enrutadores diffserv. La arquitectura Diffserv también define un conjunto de acciones denominadas *comportamientos de reenvío*, que corresponden a los DSCP. El sistema IPQoS marca los bits precedentes del campo DS del encabezado del paquete con el DSCP. Cuando un enrutador recibe un paquete con un valor DSCP, aplica el comportamiento de reenvío asociado a dicho DSCP. Después, el paquete se envía a la red.

Nota – El marcador `d\cosmk` no utiliza el DSCP. En su lugar, `d\cosmk` marca los encabezados de frame Ethernet con un valor CoS. Si quiere configurar IPQoS en una red que utiliza dispositivos VLAN, consulte la sección “[Módulo marcador](#)” en la [página 876](#).

Comportamientos por salto

En la terminología Diffserv, el comportamiento de reenvío asignado a un DSCP se denomina *comportamiento por salto (PHB)*. El PHB define la precedencia de reenvío que un paquete marcado recibe en relación con otro tráfico del sistema con Diffserv. Esta precedencia determina si el sistema con IPQoS o enrutador Diffserv reenvía o descarta el paquete marcado. Para un paquete reenviado, cada enrutador Diffserv que el paquete encuentra en la ruta hasta su destino aplica el mismo PHB. La excepción ocurre si otro sistema Diffserv cambia el DSCP. Si necesita más información sobre PHB, consulte la sección “[Utilización del marcador `dscpmk` para reenviar paquetes](#)” en la [página 877](#).

El objetivo de PHB es proporcionar una cantidad específica de recursos de red a una clase de tráfico en la red contigua. Puede conseguir este objetivo en la directiva QoS. Defina los puntos DSCP que indican los niveles de precedencia para las clases de tráfico cuando los flujos de tráfico abandonan el sistema con IPQoS. Las precedencias pueden alternar entre alta precedencia/baja probabilidad de descarte y baja precedencia/alta probabilidad de descarte.

Por ejemplo, la directiva QoS puede asignar a una clase de tráfico un DSCP que garantice un PHB de baja probabilidad de descarte. Esta clase de tráfico recibirá un PHB de precedencia de baja probabilidad de descarte de cualquier enrutador con Diffserv, lo que garantiza el ancho de

banda para paquetes de esta clase. Puede añadir a la directiva QoS otros puntos DSCP que asignen diferentes niveles de precedencia a las clases de tráfico. Los sistemas Diffserv asignan ancho de banda a los paquetes de baja precedencia según las prioridades indicadas en los puntos DSCP de los paquetes.

IPQoS admite dos tipos de comportamientos de reenvío, definidos en la arquitectura Diffserv, reenvío acelerado y reenvío asegurado.

Reenvío acelerado

el comportamiento por salto de *reenvío acelerado (EF)* asegura que cualquier clase de tráfico con reenvíos EF relacionados con DSCP tiene la máxima prioridad. El tráfico con DSCP EF no se pone en cola. EF proporciona una pérdida de datos, latencia y demora mínimas. El DSCP recomendado para EF es 101110. Un paquete que esté marcado con 101110 recibe una precedencia de baja probabilidad de descarte asegurada al atravesar redes Diffserv hacia su destino. Utilice DSCP EF al asignar prioridad a clientes o aplicaciones con un acuerdo SLA de nivel alto.

Reenvío asegurado

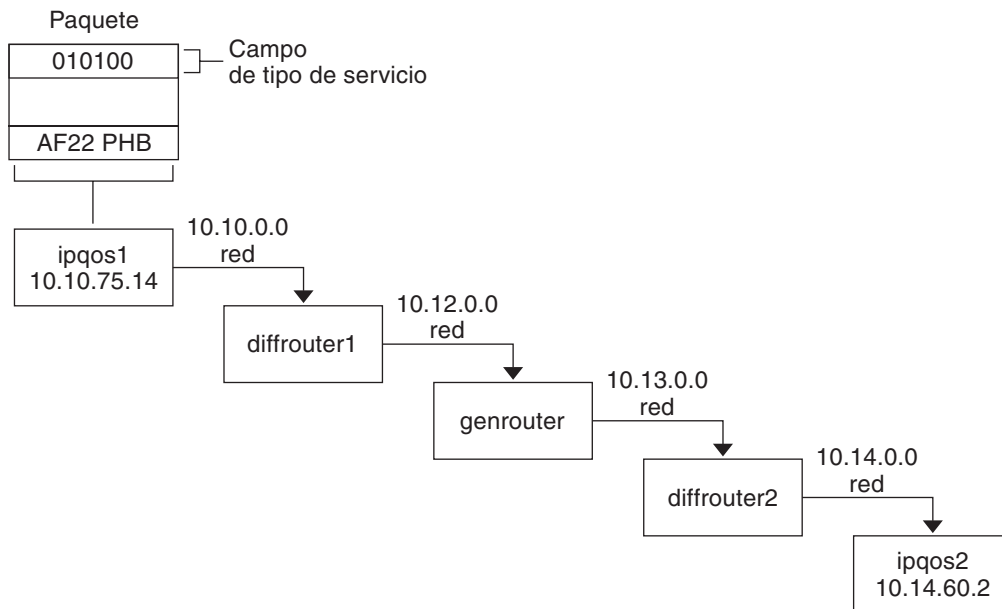
El comportamiento por salto de *reenvío asegurado (AF)* proporciona cuatro clases de reenvío diferentes que se pueden asignar a un paquete. Cada clase de reenvío proporciona tres precedencias de descarte, tal y como se muestra en la [Tabla 37-2](#).

Los diferentes puntos de código AF permiten asignar distintos niveles de servicio a clientes y aplicaciones. Puede priorizar tráfico y servicios de la red al planificar la directiva QoS. Después, puede asignar diferentes niveles AF para priorizar el tráfico.

Reenvío de paquetes en un entorno Diffserv

La siguiente figura muestra parte de una intranet de una empresa con un entorno que utiliza Diffserv parcialmente. En este escenario, todos los hosts de las redes 10.10.0.0 y 10.14.0.0 utilizan IPQoS y los enrutadores locales de ambas redes tienen Diffserv. Aunque las redes intermedias no están configuradas para utilizar Diffserv.

FIGURA 32-2 Reenvío de paquetes en saltos de red con Diffserv



Los siguientes pasos muestran el flujo del paquete mostrado en la figura. Los pasos comienzan con el progreso de un paquete originado en el host ipqos1. Los pasos continúan con varios saltos hasta el host ipqos2.

1. El usuario de ipqos1 ejecuta el comando ftp para acceder al host ipqos2, que está tres saltos más allá.
2. ipqos1 aplica su directiva QoS al flujo de paquetes resultante. Después, ipqos1 clasifica el tráfico ftp.

El administrador del sistema ha creado una clase para todo el tráfico ftp saliente con origen en la red local 10.10.0.0. Se asigna el comportamiento por salto AF22 al tráfico de la clase ftp: clase dos, precedencia de descarte media. Se ha asignado una tasa de flujo de tráfico de 2 Mb/seg a la clase ftp.

3. ipqos-1 mide el flujo ftp para determinar si excede la tasa asignada de 2 Mbit/seg.
4. El marcador de ipqos1 marca los campos DS de los paquetes ftp salientes con el DSCP 010100, que corresponde a AF22 PHB.
5. El enrutador diffrouter1 recibe los paquetes ftp. A continuación, diffrouter1 comprueba el DSCP. Si diffrouter1 está congestionado, los paquetes marcados con AF22 se descartan.
6. El tráfico ftp se reenvía al siguiente salto de acuerdo con el comportamiento por salto configurado para AF22 en los archivos de diffrouter1.

7. El tráfico `ftp` atraviesa la red `10.12.0.0` hasta `genrouter`, que no utiliza Diffserv. Como resultado, el tráfico recibe el comportamiento de reenvío "mejor posible".
8. `genrouter` pasa el tráfico `ftp` a la red `10.13.0.0`, donde lo recibe `diffrouter2`.
9. `diffrouter2` utiliza Diffserv. Por lo tanto, el enrutador reenvía los paquetes `ftp` a la red de acuerdo con el PHB definido en la directiva del enrutador para paquetes AF22.
10. `ipqos2` recibe el tráfico `ftp`. `ipqos2` solicita al usuario de `ipqos1` un nombre de usuario y contraseña.

Planificación para una red con IPQoS (Tareas)

Puede configurar IPQoS en cualquier sistema que ejecute Oracle Solaris. El sistema IPQoS funciona con enrutadores con Diffserv para proporcionar servicios diferenciados y administración del tráfico en una intranet.

Este capítulo contiene tareas de planificación para añadir sistemas con IPQoS a una red con Diffserv. Se tratan los temas siguientes.

- “Planificación de configuración IPQoS general (Mapa de tareas)” en la página 809
- “Planificación de la distribución de la red Diffserv” en la página 810
- “Planificación de la directiva de calidad de servicio” en la página 813
- “Planificación de la directiva QoS (Mapa de tareas)” en la página 814
- “Introducción al ejemplo de configuración IPQoS” en la página 826

Planificación de configuración IPQoS general (Mapa de tareas)

Utilizar servicios diferenciados, como IPQoS, en una red requiere una planificación exhaustiva. Debe considerarse no sólo la posición y función de cada sistema con IPQoS, sino también la relación de cada sistema con el enrutador de la red local. El mapa de tareas siguiente muestra las principales tareas de planificación para implementar IPQoS en la red, y contiene vínculos a procedimientos para realizar las tareas.

Tarea	Descripción	Para obtener instrucciones
1. Planificar una distribución de red Diffserv que incorpore los sistemas con IPQoS.	Adquirir conocimientos sobre las diferentes distribuciones de red Diffserv para determinar cuál es la mejor solución en su caso.	“Planificación de la distribución de la red Diffserv” en la página 810.

Tarea	Descripción	Para obtener instrucciones
2. Planificar los diferentes tipos de servicios que ofrecerán los sistemas IPQoS.	Organizar los tipos de servicios que proporciona la red en acuerdos de nivel de servicio (SLA).	“Planificación de la directiva de calidad de servicio” en la página 813.
3. Planificar la directiva QoS para cada sistema IPQoS.	Decidir cuáles son las funciones de clases, medición y recopilación de datos necesarias para cada acuerdo SLA.	“Planificación de la directiva de calidad de servicio” en la página 813.
4. Si procede, planificar la directiva del enrutador Diffserv.	Establecer las directivas de planificación y espera en cola del enrutador Diffserv utilizado con los sistemas IPQoS.	Consulte la documentación del enrutador si necesita información sobre las directivas de espera en cola y planificación.

Planificación de la distribución de la red Diffserv

Para proporcionar servicios diferenciados en la red, necesita al menos un sistema con IPQoS y un enrutador con Diffserv. Puede expandir esta configuración básica de diferentes modos, como se explica en esta sección.

Estrategias de hardware para la red Diffserv

Normalmente, los clientes utilizan IPQoS en servidores y consolidaciones de servidores, como Sun Enterprise™ 0000. También puede utilizar IPQoS en sistemas de sobremesa, como UltraSPARC®, según las necesidades de la red. La siguiente lista contiene posibles sistemas para una configuración IPQoS:

- Sistemas Oracle Solaris que ofrecen varios servicios, como servidores web o de base de datos
- Servidores de aplicaciones que ofrecen servicios de correo electrónico, FTP y otras aplicaciones de red comunes
- Servidores de caché web o proxy
- Redes de conjuntos de servidores con IPQoS administradas por equilibradores de carga con Diffserv
- Cortafuegos que administran el tráfico de una red heterogénea
- Sistemas IPQoS que forman parte de una red de área local (LAN) virtual

Puede integrar sistemas IPQoS en una distribución de red que ya tenga enrutadores con Diffserv en funcionamiento. Si el enrutador que utiliza no admite Diffserv, considere las soluciones Diffserv que ofrecen Cisco Systems, Juniper Networks y otros fabricantes de enrutadores. Si el enrutador local no utiliza Diffserv, se limita a transferir los paquetes marcados al siguiente salto sin evaluar las marcas.

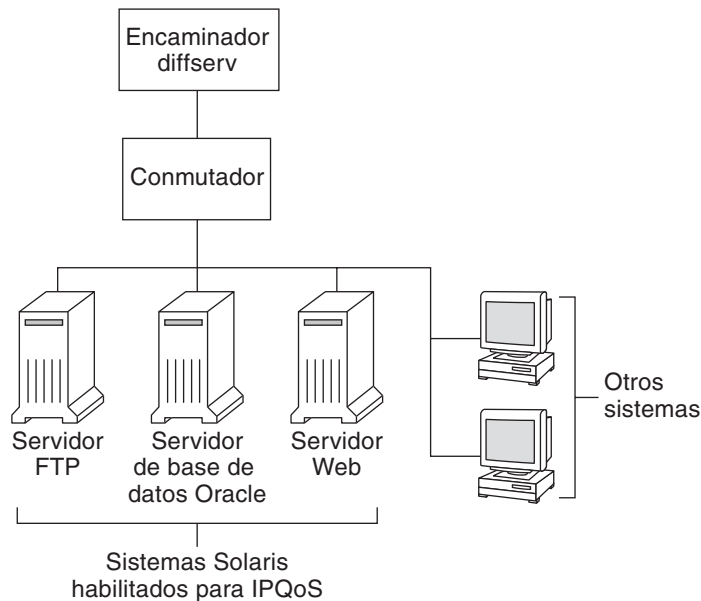
Distribuciones de red IPQoS

En esta sección se ilustran estrategias IPQoS para redes con diferentes requisitos.

IPQoS en hosts individuales

La siguiente figura ilustra una red de sistemas con IPQoS.

FIGURA 33-1 Sistemas IPQoS en un segmento de red

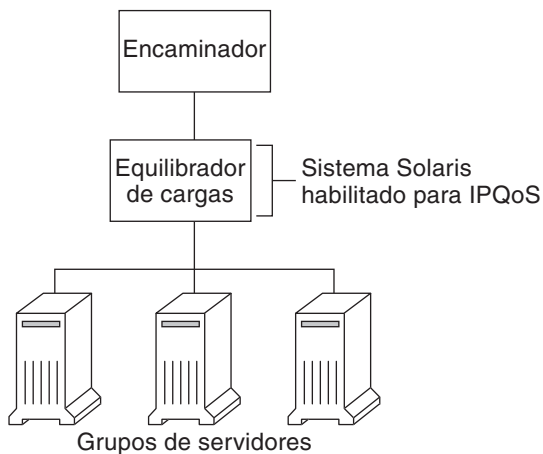


Esta red es sólo un segmento de una intranet empresarial. Activando IPQoS en los servidores de aplicaciones y servidores web, puede controlar la tasa a la que cada sistema IPQoS envía el tráfico saliente. Si configura el enrutador para utilizar Diffserv, puede obtener un mayor grado de control del tráfico entrante y saliente.

El ejemplo de esta guía utiliza una configuración con IPQoS en un único host. Para ver la distribución de ejemplo que se utiliza en esta guía, consulte la [Figura 33-4](#).

IPQoS en una red de conjuntos de servidores

La siguiente figura muestra una red con varios conjuntos de servidores heterogéneos.

FIGURA 33-2 Red de conjuntos de servidores con IPQoS

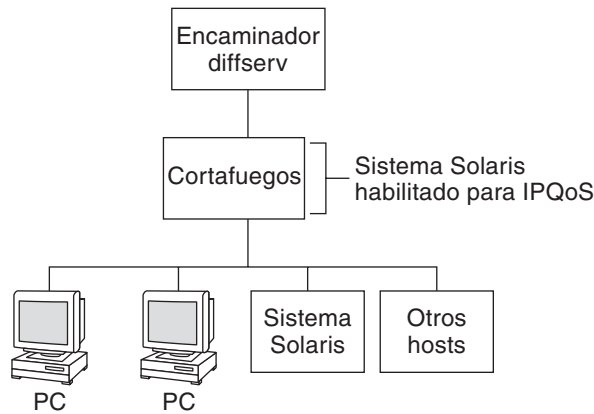
En esta distribución, el enrutador utiliza Diffserv y, por lo tanto, puede poner en cola y tasar el tráfico entrante y saliente. El equilibrador de carga también utiliza Diffserv y los conjuntos de servidores usan IPQoS. El equilibrador de carga permite realizar un filtrado adicional al del enrutador utilizando selectores como el ID de usuario o de proyecto. Estos selectores están incluidos en los datos de aplicación.

Esta configuración permite controlar el flujo y reenviar el tráfico para administrar la congestión en la red local. También evita que el tráfico saliente de los conjuntos de servidores sobrecargue otros sectores de la intranet.

IPQoS en un cortafuegos

La siguiente figura muestra un segmento de una red corporativa protegido de otros segmentos mediante un cortafuegos.

FIGURA 33-3 Red protegida por un cortafuegos con IPQoS



En esta configuración, el tráfico fluye hasta un enrutador con Diffserv que filtra y pone en cola los paquetes. Todo el tráfico entrante reenviado por el enrutador se transfiere al cortafuegos con IPQoS. Para utilizar IPQoS, el cortafuegos no debe omitir la pila de reenvío de IP.

La directiva de seguridad del cortafuegos determina si el tráfico entrante puede entrar o salir de la red interna. La directiva QoS controla los niveles de servicio para el tráfico entrante que ha pasado el cortafuegos. Según la directiva QoS, el tráfico saliente también puede marcarse con un comportamiento de reenvío.

Planificación de la directiva de calidad de servicio

Al planificar la directiva de calidad de servicio (QoS) debe revisar, clasificar y después priorizar los servicios que proporciona la red. También debe evaluar la cantidad de ancho de banda disponible para determinar la tasa a la que cada clase de tráfico se transfiere en la red.

Ayudas para planificar la directiva QoS

Recopile información para planificar la directiva QoS en un formato que incluya los datos necesarios para el archivo de configuración IPQoS. Por ejemplo, puede usar la siguiente plantilla para realizar una lista de las categorías de información principales que se utilizarán en el archivo de configuración IPQoS.

TABLA 33–1 Plantilla de planificación QoS

Clase	Prioridad	Filtro	Selector	Tasa	¿Reenvío?	¿Recopilación de datos?
Clase 1	1	Filtro 1	Selector 1	Tasas de medidor, según tipo de medidor	Precedencia de descarte de marcador	Requiere estadísticas de recopilación de datos de flujo
		Filtro 3	Selector 2			
Clase 1	1	Filtro 2	Selector 1	N/D	N/D	N/D
			Selector 2			
Clase 2	2	Filtro 1	Selector 1	Tasas de medidor, según tipo de medidor	Precedencia de descarte de marcador	Requiere estadísticas de recopilación de datos de flujo
			Selector 2			
Clase 2	2	Filtro 2	Selector 1	N/D	N/D	N/D
			Selector 2			

Puede dividir cada categoría principal para definir más la directiva QoS. En las siguientes secciones se explica cómo obtener información sobre las categorías mostradas en la plantilla.

Planificación de la directiva QoS (Mapa de tareas)

Este mapa de tareas enumera las tareas principales para planificar una directiva QoS.

Tarea	Descripción	Para obtener instrucciones
1. Diseñar la distribución de red para que sea compatible con IPQoS.	Identificar los hosts y enrutadores de la red para proporcionar servicios diferenciados.	“Cómo preparar una red para IPQoS” en la página 815
2. Definir las clases en las que los servicios de la red deben dividirse.	Examinar los tipos de servicios y acuerdos SLA que ofrece su organización y determinar las clases de tráfico independientes a las que pertenece cada servicio.	“Cómo definir las clases de la directiva QoS” en la página 816
3. Definir filtros para las clases.	Determinar el mejor modo de separar el tráfico de una clase específica del flujo de tráfico de la red.	“Cómo definir filtros en la directiva QoS” en la página 819

Tarea	Descripción	Para obtener instrucciones
4. Definir tasas de control de flujo para medir el tráfico cuando los paquetes salen del sistema IPQoS.	Determinar tasas de flujo aceptables para cada clase de tráfico.	“Cómo planificar el control de flujo” en la página 820
5. Definir los puntos DSCP o valores de prioridad de usuario que se deben utilizar en la directiva QoS.	Planificar un esquema para determinar el comportamiento de reenvío asignado a un flujo de tráfico cuando lo controla el enrutador o nodo.	“Cómo planificar el comportamiento de reenvío” en la página 823
6. Si procede, definir un plan de supervisión de estadísticas para los flujos de tráfico de la red.	Evaluar las clases de tráfico para determinar qué flujos de tráfico deben supervisarse por cuestiones de recopilación de datos o estadísticas.	“Cómo planificar la recopilación de datos de flujo” en la página 825

Nota – En el resto de esta sección se explica cómo planificar la directiva QoS de un sistema con IPQoS. Para planificar la directiva QoS del enrutador Diffserv, consulte la documentación y el sitio web del fabricante del enrutador.

▼ Cómo preparar una red para IPQoS

El siguiente procedimiento contiene tareas generales que llevar a cabo antes de crear la directiva QoS.

1 Revisar la distribución de la red. Después, planificar una estrategia que utilice sistemas IPQoS y enrutadores Diffserv.

Para ver ejemplos de distribución de la red, consulte la sección [“Planificación de la distribución de la red Diffserv” en la página 810](#).

2 Identificar los hosts de la distribución de red que requieren IPQoS o que pueden ser buenos candidatos para el servicio IPQoS.

3 Determinar qué sistemas con IPQoS pueden usar la misma directiva QoS.

Por ejemplo, si piensa activar IPQoS en todos los hosts de la red, identifique los hosts que pueden usar la misma directiva QoS. Cada sistema con IPQoS debe tener una directiva QoS local, que se implementa en el archivo de configuración IPQoS correspondiente. Aunque puede crear un archivo de configuración IPQoS que utilicen varios sistemas. Después puede copiar el archivo de configuración en los sistemas que tengan los mismos requisitos de directiva QoS.

4 Revisar y realizar cualquier tarea de planificación requerida por el enrutador Diffserv de la red.

Consulte la documentación y el sitio web del fabricante del enrutador si necesita más información.

▼ Cómo definir las clases de la directiva QoS

El primer paso para definir la directiva QoS es organizar los flujos de tráfico en clases. No es necesario crear una clase para cada tipo de tráfico en una red Diffserv. Según la distribución de la red, puede que necesite crear una directiva QoS diferente para cada sistema con IPQoS.

Nota – Para ver una descripción general de las clases, consulte la sección “[Clases IPQoS](#)” en la [página 799](#).

En el siguiente procedimiento se asume que ya ha determinado qué sistemas de la red utilizarán IPQoS, como se explica en la sección “[Cómo preparar una red para IPQoS](#)” en la [página 815](#).

1 Crear una tabla de planificación QoS para organizar la información de directiva QoS.

Para ver sugerencias, consulte la [Tabla 33–1](#).

2 Realizar el resto de los pasos para cada directiva QoS de la red.

3 Definir las clases que utilizar en la directiva QoS.

Las siguientes preguntas son una guía para analizar el tráfico de red para posibles definiciones de clases.

■ ¿Su empresa ofrece acuerdos de nivel de servicio a los clientes?

En caso afirmativo, evalúe los niveles de prioridad relativa de los acuerdos SLA que su empresa ofrece a los clientes. Las mismas aplicaciones pueden ofrecerse a clientes con niveles de prioridad diferentes garantizados.

Por ejemplo, su empresa puede ofrecer alojamiento de sitios web a cada cliente, lo que indica que necesita definir una clase para cada sitio web de cliente. Un acuerdo SLA puede ofrecer un sitio web de nivel alto como un nivel de servicio. Otro acuerdo SLA puede ofrecer un sitio web personal "best-effort" a clientes con descuento. Este factor no sólo implica diferentes clases de sitio web sino también diferentes comportamientos por salto que se asignan a las clases de sitio web.

■ ¿El sistema IPQoS ofrece aplicaciones comunes que necesitan control de flujo?

Puede mejorar el rendimiento de la red activando IPQoS en servidores que ofrecen aplicaciones comunes que generan mucho tráfico. Algunos ejemplos son el correo electrónico, noticias de red y FTP. Considere la posibilidad de crear clases independientes para el tráfico entrante y saliente para cada tipo de servicio, si corresponde. Por ejemplo, puede crear una clase mail-in y una clase mail-out para la directiva QoS de un servidor de correo.

■ ¿La red contiene aplicaciones que requieren comportamientos de reenvío de máxima prioridad?

Cualquier aplicación importante que requiera comportamientos de reenvío de máxima prioridad debe recibir la máxima prioridad en la cola del enrutador. Los ejemplos más típicos son el streaming de vídeo y audio.

Definir clases de entrada y clases de salida para estas aplicaciones de alta prioridad. Después, añadir las clases a las directivas QoS del sistema con IPQoS que proporciona las aplicaciones y del enrutador Diffserv.

■ **¿La red tiene flujos de tráfico que deben controlarse porque consumen grandes cantidades de ancho de banda?**

Utilizar netstat, snoop y otras herramientas de supervisión de la red para descubrir los tipos de tráfico que causan problemas en la red. Revisar las clases creadas hasta ahora y crear clases para cualquier categoría de tráfico con problemas no definidos. Si ya ha definido clases para una categoría de tráfico problemático, defina tasas para que el medidor controle el tráfico.

Crear clases para el tráfico problemático en cada sistema con IPQoS de la red. Después, cada sistema IPQoS puede gestionar el tráfico problemático limitando la tasa a la que el flujo de tráfico se envía en la red. Asegúrese de definir estas clases de problemas en la directiva QoS del enrutador Diffserv. Después, el enrutador puede poner en cola y planificar los flujos problemáticos de acuerdo con la configuración de la directiva QoS.

■ **¿Necesita estadísticas sobre determinados tipos de tráfico?**

Una revisión rápida del acuerdo SLA permite determinar qué tipos de tráfico del cliente requieren recopilación de datos. Si su empresa ofrece acuerdos SLA, es probable que ya haya creado clases para el tráfico que requiere recopilación de datos. También puede definir clases para activar la recopilación de estadísticas en flujos de tráfico que esté supervisando. También es posible crear clases para tráfico al que se restringe el acceso por motivos de seguridad.

4 Enumerar las clases definidas en la tabla de planificación QoS creada en el paso 1.

5 Asignar un nivel de prioridad a cada clase.

Por ejemplo, el nivel de prioridad 1 representa la clase de prioridad máxima y se asignan prioridades de nivel descendente al resto de clases. El nivel de prioridad que se asigna sólo tiene propósito organizativo. Los niveles de prioridad definidos en la plantilla de directiva QoS no se utilizan en IPQoS. De hecho, puede asignar la misma prioridad a varias clases, si es apropiado para la directiva QoS.

6 Cuando haya terminado de definir las clases, puede definir filtros para cada clase, como se explica en ["Cómo definir filtros en la directiva QoS" en la página 819](#).

Más información Priorizar las clases

Al crear clases, resulta fácil ver cuáles tiene la prioridad máxima, la prioridad media y la prioridad "best-effort". Un buen esquema para priorizar clases resulta especialmente

importante si se asignan comportamientos por salto al tráfico saliente, como se explica en la sección [“Cómo planificar el comportamiento de reenvío” en la página 823](#).

Además de asignar un PHB a una clase, también puede definir un selector de prioridad en un filtro para la clase. El selector de prioridad está activo sólo en el host con IPQoS. Imagine que varias clases con tasas iguales y puntos DSCP idénticos en ocasiones compiten por el ancho de banda al salir del sistema IPQoS. El selector de prioridad de cada clase puede ordenar el nivel de servicio que se asigna a dos clases con valores que de otro modo serían idénticos.

Definir filtros

Puede crear filtros para identificar flujos de paquetes como miembros de una clase específica. Cada filtro contiene selectores, que definen los criterios para evaluar un flujo de paquetes. El sistema con IPQoS utiliza los criterios de los selectores para extraer paquetes de un flujo de tráfico. Después, el sistema IPQoS asocia los paquetes con una clase. Para ver una introducción a los filtros, consulte la sección [“Filtros IPQoS” en la página 800](#).

En la siguiente tabla se enumeran los selectores más usados. Los cinco selectores representan el 5-tuple IPQoS, que el sistema IPQoS utiliza para identificar paquetes como miembros de un flujo. Para ver una lista completa de selectores, consulte la [Tabla 37–1](#).

TABLA 33–2 Selectores IPQoS comunes

Nombre	Definición
saddr	Dirección de origen.
daddr	Dirección de destino.
sport	Número de puerto de origen. Puede usar un número de puerto conocido, definido en <code>/etc/services</code> o un número de puerto definido por el usuario.
dport	Número de puerto de destino.
protocol	Número de protocolo IP o nombre de protocolo asignado al tipo de flujo de tráfico en <code>/etc/protocols</code> .
ip_version	Estilo de direcciones que usar. Se utiliza IPv4 o IPv6. IPv4 es el predeterminado.
dsfield	Contenido del campo DS, es decir, el punto DSCP. Utilice este selector para extraer paquetes entrantes que ya están marcados con un DSCP específico.
priority	Nivel de prioridad asignado a la clase. Si necesita más información, consulte “Cómo definir las clases de la directiva QoS” en la página 816 .
user	El ID de usuario de UNIX o nombre de usuario que se utiliza cuando se ejecuta la aplicación de nivel superior.
projid	ID de proyecto que se utiliza cuando se ejecuta la aplicación de nivel superior.

TABLA 33-2 Selectores IPQoS comunes (Continuación)

Nombre	Definición
direction	Dirección del flujo de tráfico. El valor es LOCAL_IN, LOCAL_OUT, FWD_IN o FWD_OUT.

Nota – Elija los selectores con detenimiento. Utilice sólo los selectores necesarios para extraer paquetes de una clase. Cuantos más selectores defina, más se verá afectado el rendimiento IPQoS.

▼ Cómo definir filtros en la directiva QoS

Antes de empezar Antes de llevar a cabo los siguientes pasos, debe haber completado el procedimiento “[Cómo definir las clases de la directiva QoS](#)” en la página 816.

- 1 Cree al menos un filtro para cada clase de la tabla de planificación QoS creada en la sección “[Cómo definir las clases de la directiva QoS](#)” en la página 816.**
Consideres la posibilidad de crear filtros independientes para el tráfico entrante y saliente de cada clase, si procede. Por ejemplo, añada un filtro ftp-in y un filtro ftp-out a la directiva QoS de un servidor con IPQoS. Después puede definir un selector direction apropiado además de los selectores básicos.
- 2 Defina al menos un selector para cada filtro de una clase.**
Utilice la tabla de planificación QoS que se ha introducido en la [Tabla 33-1](#) para rellenar los filtros de las clases definidas.

Ejemplo 33-1 Definir filtros para el tráfico FTP

La tabla siguiente es un ejemplo de cómo definir un filtro para el tráfico FTP saliente.

Clase	Prioridad	Filtros	Selectores
ftp-traffic	4	ftp-out	saddr 10.190.17.44 daddr 10.100.10.53 sport 21 direction LOCAL_OUT

Véase también ■ Para definir un esquema de control de flujo, consulte la sección “[Cómo planificar el control de flujo](#)” en la página 820.

- Para definir comportamientos de reenvío para flujos que vuelven al flujo de red, consulte [“Cómo planificar el comportamiento de reenvío” en la página 823](#).
- Para planificar la recopilación de datos de flujo de determinados tipos de tráfico, consulte la sección [“Cómo planificar la recopilación de datos de flujo” en la página 825](#).
- Para añadir más clases a la directiva QoS, consulte la sección [“Cómo definir las clases de la directiva QoS” en la página 816](#).
- Para añadir más filtros a la directiva QoS, consulte la sección [“Cómo definir filtros en la directiva QoS” en la página 819](#).

▼ Cómo planificar el control de flujo

El control de flujo implica medir el flujo de tráfico de una clase y transferir los paquetes en la red a una tasa definida. Al planificar el control de flujo, se definen los parámetros que utilizarán los módulos de medición IPQoS. Los medidores determinan la tasa a la que se transfiere el tráfico en la red. Para ver una introducción a los módulos de medición, consulte la sección [“Descripción general de medidor \(tokenmt y tswtclmt\)” en la página 800](#).

En el siguiente procedimiento se asume que ha definido filtros y selectores, como se describe en la sección [“Cómo definir filtros en la directiva QoS” en la página 819](#).

- 1 Determine el ancho de banda máximo de la red.**
- 2 Revise cualquier acuerdo SLA que ofrezca su red. Identifique los clientes y los tipos de servicio garantizados a cada cliente.**

Para garantizar un nivel de servicio determinado, es posible que necesite medir ciertas clases de tráfico generadas por el cliente.

- 3 Revise la lista de clases creadas en la sección [“Cómo definir las clases de la directiva QoS” en la página 816](#).**

Determine si hay alguna otra clase, a parte de las asociadas con acuerdos SLA, que deba medirse.

Suponga que el sistema IPQoS incluye una aplicación que genera mucho tráfico. Después de clasificar el tráfico de la aplicación, mida los flujos para controlar la tasa a la que los paquetes del flujo vuelven a la red.

Nota – No es necesario medir todas las clases. Tenga en mente estas directrices al revisar la lista de clases.

4 Determine qué filtros de cada clase seleccionan el tráfico que necesita control de flujo. Después, refine la lista de clases que necesitan medición.

Las clases que tengan varios filtros pueden necesitar medición sólo para un filtro. Suponga que define filtros para el tráfico entrante y saliente de una clase específica. Puede llegar a la conclusión de que sólo el tráfico en una dirección requiere control de flujo.

5 Elija un módulo de medición para cada clase con control de flujo.

Añada el nombre de módulo a la columna de medición de la tabla de planificación QoS.

6 Añada las tasas de cada clase que se medirá a la tabla de organización.

Si utiliza el módulo `tokenmt`, deberá definir las siguientes tasas en bits por segundo:

- Tasa asignada
- Tasa máxima

Si estas tasas son suficientes para medir una clase específica, puede definir solamente la tasa asignada y ráfaga asignada para `tokenmt`.

Si es necesario, puede definir también las siguientes tasas:

- Ráfaga asignada
- Ráfaga máxima

Para ver una definición completa de las tasas de `tokenmt`, consulte la sección [“Configuración de tokenmt como medidor de doble tasa” en la página 875](#). También puede encontrar información detallada en la página de comando `man tokenmt (7ipp)`.

Si utiliza el módulo `tswtclmt`, debe definir las siguientes tasas en bits por segundo.

- Tasa asignada
- Tasa máxima

También puede definir el tamaño de la ventana en milisegundos. Estas tasas están definidas en la sección [“Módulo de medición tswtclmt” en la página 876](#) y en la página de comando `man twstclmt (7ipp)`.

7 Añada resultados de cumplimiento del tráfico al metro medido.

Los resultados de ambos módulos de medición son verde, rojo y amarillo. Añada a la tabla de organización QoS los resultados de cumplimiento del tráfico aplicables a las tasas definidas. Los resultados de los medidores están explicados en la sección [“Módulo Meter” en la página 874](#).

Debe determinar qué acciones deben realizarse con el tráfico que cumple, o no cumple, la tasa asignada. Normalmente, pero no siempre, la acción consiste en marcar el encabezado del paquete con un comportamiento por salto. Una acción aceptable para el tráfico de nivel verde es continuar el procesamiento mientras los flujos de tráfico no excedan la tasa asignada. Otra acción sería descartar los paquetes de la clase si los flujos exceden la tasa máxima.

Ejemplo 33-2 Definir medidores

La tabla siguiente muestra entradas de medidor para una clase de tráfico de correo electrónico. La red en la que se encuentra el sistema IPQoS tiene un ancho de banda total de 100 Mbits/seg, o 10000000 bits por segundo. La directiva QoS asigna una prioridad baja a la clase de correo electrónico. Esta clase también recibe un comportamiento de reenvío "best-effort".

Clase	Prioridad	Filtro	Selector	Tasa
email	8	mail_in	daddr10.50.50.5	
			dport imap	
			direction LOCAL_IN	
email	8	mail_out	saddr10.50.50.5	medidor=tokenmt
			sport imap	tasa asignada=5000000
			direction LOCAL_OUT	ráfaga asignada =5000000
				tasa máxima =10000000
				ráfaga máxima=1000000
				precedencia verde=continuar procesando
				precedencia amarilla=marcar PHB amarillo
				precedencia roja=descartar

- Véase también**
- Para definir los comportamientos de reenvío para flujos cuando los paquetes vuelven al flujo de red, consulte la sección [“Cómo planificar el comportamiento de reenvío” en la página 823.](#)
 - Para planificar la recopilación de datos de flujo de determinados tipos de tráfico, consulte la sección [“Cómo planificar la recopilación de datos de flujo” en la página 825.](#)
 - Para añadir más clases a la directiva QoS, consulte la sección [“Cómo definir las clases de la directiva QoS” en la página 816.](#)
 - Para añadir más filtros a la directiva QoS, consulte la sección [“Cómo definir filtros en la directiva QoS” en la página 819.](#)
 - Para definir otro esquema de control de flujo, consulte la sección [“Cómo planificar el control de flujo” en la página 820.](#)
 - Para crear un archivo de configuración IPQoS, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834.](#)

▼ Cómo planificar el comportamiento de reenvío

El comportamiento de reenvío determina la prioridad y precedencia de descarte de los flujos de tráfico que se van a reenviar a la red. Puede elegir dos comportamientos de reenvío principales: priorizar los flujos de una clase en relación con otras clases de tráfico o descartar los flujos por completo.

El modelo Diffserv utiliza el marcador para asignar el comportamiento de reenvío elegido a los flujos de tráfico. IPQoS ofrece los siguiente módulos de marcador.

- `dscpmk` – Se utiliza para marcar el campo DS de un paquete IP con un DSCP
- `dlsosmk` – Se utiliza para marcar la etiqueta VLAN de un datagrama con un valor de clase de servicio (CoS)

Nota – Las sugerencias de esta sección hacen referencia específicamente a paquetes IP. Si el sistema IPQoS incluye un dispositivo VLAN, puede usar el marcador `dlsosmk` para marcar comportamientos de reenvío para datagramas. Si necesita más información, consulte la sección [“Uso del marcador `dlsosmk` con dispositivos VLAN” en la página 879](#).

Para priorizar el tráfico IP, debe asignar un punto DSCP a cada paquete. El marcador `dscpmk` marca el campo DS del paquete con el DSCP. El DSCP de una clase se elige de un grupo de puntos de código conocidos asociados con el tipo de comportamiento de reenvío. Estos puntos de código conocidos son 46 (101110) para el comportamiento PHB EF y un conjunto de puntos de código para el comportamiento PHB AF. Para ver una descripción general de los puntos DSCP y el reenvío, consulte la sección [“Reenvío del tráfico en una red con IPQoS” en la página 804](#).

Antes de empezar

En los siguientes pasos se asume que ha definido clases y filtros para la directiva QoS. Aunque normalmente se usa el medidor con el marcador para controlar el tráfico, puede usarse solamente el marcador para definir un comportamiento de reenvío.

1 Revise las clases creadas hasta ahora y las prioridades asignadas a cada clase.

No es necesario que se marquen todas las clases de tráfico.

2 Asigne el comportamiento por salto EF a la clase con la prioridad más alta.

El comportamiento PHB EF garantiza que los paquetes con el punto DSCP EF 46 (101110) se transfieren a la red antes que los paquetes con cualquier comportamiento PHB AF. Utilice el comportamiento PHB EF para el tráfico de mayor prioridad. Si necesita más información sobre EF, consulte la sección [“Reenvío acelerado \(EF\) PHB” en la página 877](#).

3 Asigne comportamientos de reenvío a clases cuyo tráfico se va a medir.

4 Asigne puntos de código DS al resto de clases, de acuerdo con las prioridades asignadas a las clases.

Ejemplo 33-3 Directiva QoS para una aplicación de juegos

El tráfico se suele medir según los siguientes criterios:

- Un acuerdo SLA garantiza a los paquetes de esta clase un servicio de nivel alto o de nivel bajo cuando la red tiene mucho tráfico.
- Una clase con una prioridad más baja puede colapsar la red.

Se utiliza el marcador con el medidor para proporcionar servicios diferenciados y administración del ancho de banda a estas clases. Por ejemplo, la siguiente tabla muestra una parte de una directiva QoS. Esta directiva define una clase para una aplicación de juegos muy utilizada que genera un alto volumen de tráfico.

Clase	Prioridad	Filtro	Selector	Tasa	¿Reenvío?
games_app	9	games_in	sport 6080	N/D	N/D
games_app	9	games_out	dport 6081	medidor=tokenmt tasa asignada=5000000 ráfaga asignada=5000000 tasa máxima=10000000 ráfaga máxima=15000000 precedencia verde=continuar procesando precedencia amarilla=marcar PHB amarillo precedencia roja=descartar	verde=AF31 amarillo=AF42 rojo=descartar

Los comportamientos de reenvío asignan puntos DSCP de baja prioridad al tráfico games_app que cumple su tasa asignada o está por debajo de la tasa máxima. Cuando el tráfico games_app excede la tasa máxima, la directiva QoS indica que los paquetes de games_app deben descartarse. Todos los puntos de código AF se enumeran en la [Tabla 37-2](#).

- Véase también**
- Para planificar la recopilación de datos de flujo de determinados tipos de tráfico, consulte la sección [“Cómo planificar la recopilación de datos de flujo” en la página 825](#).
 - Para añadir más clases a la directiva QoS, consulte la sección [“Cómo definir las clases de la directiva QoS” en la página 816](#).
 - Para añadir más filtros a la directiva QoS, consulte la sección [“Cómo definir filtros en la directiva QoS” en la página 819](#).
 - Para definir un esquema de control de flujo, consulte la sección [“Cómo planificar el control de flujo” en la página 820](#).
 - Para definir comportamientos de reenvío adicionales para flujos cuando los paquetes vuelven al flujo de red, consulte la sección [“Cómo planificar el comportamiento de reenvío” en la página 823](#).
 - Para crear un archivo de configuración IPQoS, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834](#).

▼ Cómo planificar la recopilación de datos de flujo

El módulo IPQoS `flowacct` se utiliza para supervisar los flujos de tráfico por motivos de facturación o de administración de la red. Utilice el siguiente procedimiento para determinar si su directiva QoS debe incluir recopilación de datos sobre flujo.

- 1 **¿Su empresa ofrece acuerdos SLA a los clientes?**
Si la respuesta es "sí", debe recopilar datos sobre el flujo. Revise los acuerdos SLA para determinar qué tipos de tráfico de red desea ofrecer su empresa a los clientes. A continuación, revise la directiva QoS para determinar qué clases seleccionan el tráfico que se facturará.
- 2 **¿Hay aplicaciones que deben supervisarse o comprobarse para evitar problemas de red?**
Si la respuesta es "sí", considere la posibilidad de recopilar datos sobre el flujo para observar el comportamiento de estas aplicaciones. Revise la directiva QoS para determinar qué clases ha asignado al tráfico que requiere supervisión.
- 3 **En la tabla de planificación QoS, marque una Y en la columna de recopilación de datos sobre el flujo de las clases que requieran recopilación de datos.**

- Véase también**
- Para añadir más clases a la directiva QoS, consulte la sección [“Cómo definir las clases de la directiva QoS” en la página 816](#).
 - Para añadir más filtros a la directiva QoS, consulte la sección [“Cómo definir filtros en la directiva QoS” en la página 819](#).
 - Para definir un esquema de control de flujo, consulte la sección [“Cómo planificar el control de flujo” en la página 820](#).

- Para definir los comportamientos de reenvío para flujos cuando los paquetes vuelven al flujo de red, consulte la sección [“Cómo planificar el comportamiento de reenvío” en la página 823](#).
- Para planificar la recopilación de datos adicional para determinados tipos de tráfico, consulte la sección [“Cómo planificar la recopilación de datos de flujo” en la página 825](#).
- Para crear el archivo de configuración IPQoS, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834](#).

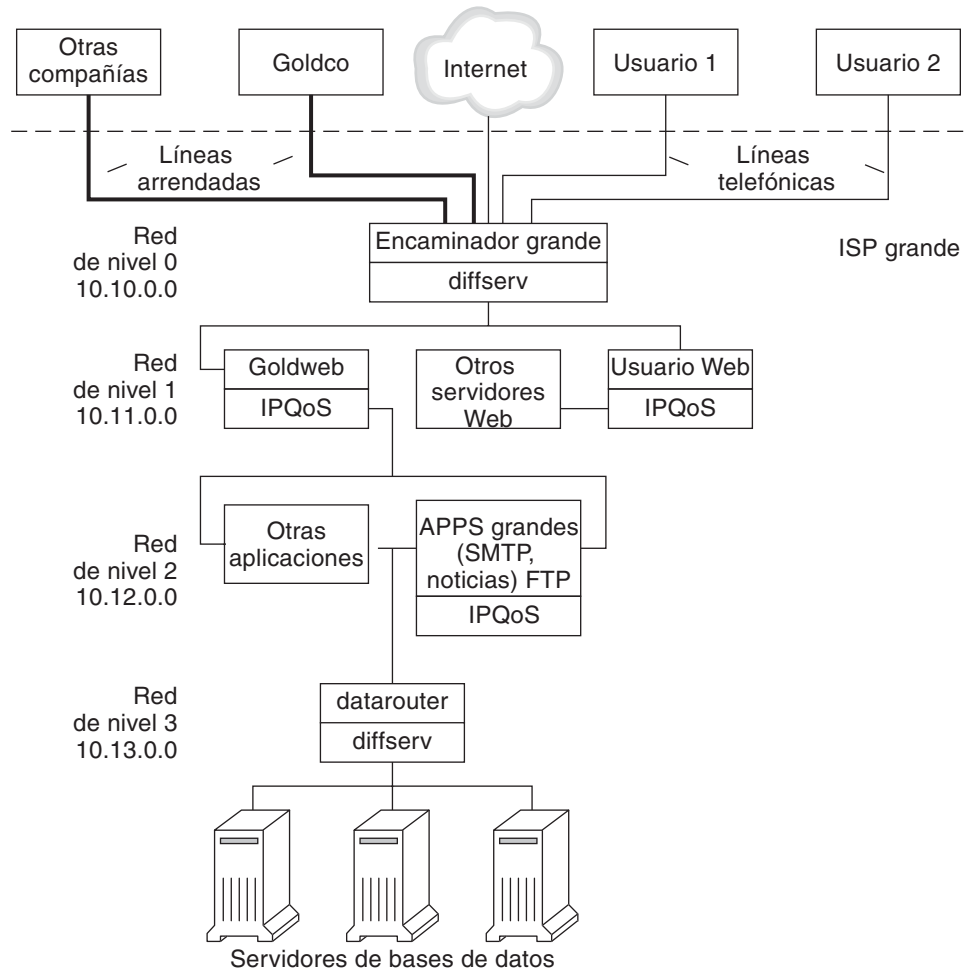
Introducción al ejemplo de configuración IPQoS

Las tareas de los siguientes capítulos de la guía utilizan la configuración IPQoS de ejemplo de esta sección. El ejemplo muestra la solución de servicios diferenciados de la intranet pública de BigISP, un proveedor de servicios ficticio. BigISP ofrece servicios a grandes empresas que acceder a BigISP a través de líneas arrendadas. Los individuos que se conectan desde módems también pueden adquirir servicios de BigISP.

Distribución IPQoS

La siguiente figura muestra la distribución de red que utiliza la intranet pública de BigISP.

FIGURA 33-4 Ejemplo de distribución IPQoS



BigISP utiliza cuatro niveles en su intranet pública:

- **Nivel 0:** la red 10.10.0.0 incluye un enrutador Diffserv llamado Bigrouter, con interfaz externa e interna. Varias empresas, entre ellas una organización llamada Goldco, han alquilado servicios de línea arrendada que finalizan en Bigrouter. EL nivel 0 también gestiona los clientes individuales que llaman desde líneas telefónicas o RDSI.
- **Nivel 1:** la red 10.11.0.0 proporciona servicios web. El servidor Goldweb aloja el sitio web adquirido por Goldco como parte del servicio de alto nivel que Goldco ha adquirido de BigISP. El servidor Userweb aloja sitios web pequeños adquiridos por clientes individuales. Ambos servidores, Goldweb y Userweb utilizan IPQoS.

- **Nivel 2** – La red 10.12.0.0 proporciona aplicaciones para todos los clientes. BigAPPS, uno de los servidores de aplicaciones, utiliza IPQoS. BigAPPS proporciona servicios SMTP, de noticias y FTP.
- **Nivel 3** – La red 10.13.0.0 aloja grandes servidores de base de datos. El acceso al Nivel 3 está controlado por datarouter, un enrutador Diffserv.

Creación del archivo de configuración IPQoS (Tareas)

En este capítulo se explica cómo crear archivos de configuración IPQoS. El capítulo trata los siguientes temas.

- “Definición de una directiva QoS en el archivo de configuración IPQoS (Mapa de tarea)” en la página 829
- “Herramientas para crear una directiva QoS” en la página 831
- “Crear archivos de configuración IPQoS para servidores web” en la página 832
- “Crear un archivo de configuración IPQoS para un servidor de aplicaciones” en la página 845
- “Suministro de servicios diferenciados en un enrutador” en la página 854

En este capítulo se asume que el usuario ha definido una directiva QoS completa y que está listo para utilizarla como base para el archivo de configuración IPQoS. Si necesita instrucciones sobre la planificación de directivas QoS, consulte el tema “[Planificación de la directiva de calidad de servicio](#)” en la página 813.

Definición de una directiva QoS en el archivo de configuración IPQoS (Mapa de tarea)

Este mapa de tarea enumera las tareas generales para crear un archivo de configuración IPQoS y contiene vínculos a las secciones en que se describe cómo realizar esas tareas.

Tarea	Descripción	Para obtener instrucciones
1. Planificar la configuración de red con IPQoS.	Decidir qué sistemas de la red local van a utilizar IPQoS.	“Cómo preparar una red para IPQoS” en la página 815

Tarea	Descripción	Para obtener instrucciones
2. Planificar la directiva QoS para sistemas IPQoS de la red.	Identificar flujos de tráfico como diferentes clases de servicio. A continuación, determinar qué flujos requieren administración del tráfico.	“Planificación de la directiva de calidad de servicio” en la página 813
3. Crear el archivo de configuración IPQoS y definir la primera acción.	Crear el archivo IPQoS, invocar el clasificador IP y definir una clase para procesar.	“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834
4. Crear filtros para un clase.	Añadir los filtros que determinan qué tráfico se selecciona y organiza en una clase.	“Cómo definir filtros en el archivo de configuración IPQoS” en la página 836
5. Añadir más clases y filtros al archivo de configuración IPQoS.	Crear más clases y filtros para que los procese el clasificador IP.	“Cómo crear un archivo de configuración IPQoS para un servidor web “Best-Effort” en la página 842
6. Añadir una instrucción <code>action</code> con parámetros para configurar los módulos de medición.	Si la directiva QoS solicita control de flujo, asigne tasas de control de flujo y niveles de cumplimiento al medidor.	“Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 851
7. Añadir una instrucción <code>action</code> con parámetros para configurar el marcador.	Si la política QoS solicita comportamientos de reenvío diferenciados, defina cómo deben reenviarse las clases de tráfico.	“Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS” en la página 838
8. Añadir una instrucción <code>action</code> con parámetros para configurar el módulo de control de flujo.	Si la directiva QoS solicita recopilación de estadísticas sobre flujos de tráfico, defina cómo deben recopilarse las estadísticas de control.	“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 841
9. Aplicar el archivo de configuración IPQoS.	Añadir el contenido de un archivo de configuración IPQoS especificado a los módulos de núcleo apropiados.	“Cómo aplicar una nueva configuración a los módulos de kernel IPQoS” en la página 858
10. Configurar los comportamientos de reenvío en los archivos de enrutador.	Si algún archivo de configuración IPQoS de la red define los comportamientos de reenvío, añada los puntos DSCP resultantes a los archivos de planificación correspondientes del enrutador.	“Cómo configurar un enrutador en una red con IPQoS” en la página 855

Herramientas para crear una directiva QoS

La directiva QoS de la red está definida en el archivo de configuración IPQoS. Este archivo de configuración se crea con un editor de texto. Después, se proporciona el archivo como un argumento a `ipqos conf`, la herramienta de configuración IPQoS. Al solicitar a `ipqos conf` que aplique la directiva definida en el archivo de configuración, la directiva se escribe en el núcleo del sistema IPQoS. Si necesita información detallada sobre el comando `ipqos conf`, consulte la página de comando `man ipqos conf(1M)`. Si necesita instrucciones sobre el uso de `ipqos conf`, consulte la sección “[Cómo aplicar una nueva configuración a los módulos de kernel IPQoS](#)” en la página 858.

Archivo de configuración IPQoS básico

Un archivo de configuración IPQoS consiste en un árbol de instrucciones de acción que implementan la directiva QoS definida en la sección “[Planificación de la directiva de calidad de servicio](#)” en la página 813. El archivo de configuración IPQoS configura los módulos IPQoS. Cada instrucción de acción contiene un conjunto de *clases*, *filtros* o *parámetros* que procesará el módulo al que llame la instrucción de acción.

Para ver la sintaxis completa del archivo de configuración IPQoS, consulte el [Ejemplo 37–3](#) y la página de comando `man ipqos conf(1M)`.

Configurar la topología de ejemplo IPQoS

Las tareas de este capítulo explican cómo crear archivos de configuración IPQoS para tres sistemas con IPQoS. Estos sistemas forman parte de la topología de red de la empresa BigISP, introducida en la [Figura 33–4](#).

- Goldweb: Un servidor web que aloja sitios web de clientes que tienen acuerdos SLA de nivel alto
- Userweb: Un servidor web menos potente que aloja páginas personales de usuarios que tienen acuerdos SLA de tipo “best-effort”
- BigAPPS – Servidor de aplicaciones que ofrece servicios de correo, noticias y FTP a clientes con servicios de nivel alto y “best-effort”

Estos tres archivos de configuración ilustran las configuraciones IPQoS más comunes. Puede usar los archivos de muestra de la siguiente sección como plantilla para su implementación IPQoS.

Crear archivos de configuración IPQoS para servidores web

Esta sección es una introducción al archivo de configuración IPQoS en la que se muestra cómo crear una configuración para un servidor web de nivel alto. También se muestra cómo configurar un nivel de servicio diferente mediante otro archivo de configuración para un servidor que aloja páginas web personales. Ambos servidores forman parte del ejemplo de red que se muestra en la [Figura 33-4](#).

El siguiente archivo de configuración define actividades IPQoS para el servidor Goldweb. Este servidor aloja el sitio web de Goldco, la compañía que tiene un acuerdo SLA de nivel alto.

EJEMPLO 34-1 Archivo de configuración IPQoS de ejemplo para un servidor web de nivel alto

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name goldweb
        next_action markAF11
        enable_stats FALSE
    }
    class {
        name video
        next_action markEF
        enable_stats FALSE
    }
    filter {
        name webout
        sport 80
        direction LOCAL_OUT
        class goldweb
    }
    filter {
        name videoout
        sport videosrv
        direction LOCAL_OUT
        class video
    }
}

action {
    module dscpmk
    name markAF11
    params {
        global_stats FALSE
        dscp_map{0-63:10}
        next_action continue
    }
}

action {
    module dscpmk
```


EJEMPLO 34-1 Archivo de configuración IPQoS de ejemplo para un servidor web de nivel alto
(Continuación)

```

    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
action {
    module flowacct
    name acct
    params {
        enable_stats TRUE
        timer 10000
        timeout 10000
        max_limit 2048
    }
}

```

El siguiente archivo de configuración define actividades IPQoS en Userweb. Este servidor aloja sitios web de usuarios con acuerdos SLA de bajo precio o *"best-effort"*. Este nivel de servicio garantiza el mejor servicio que puede ofrecerse a clientes "best-effort" después de que el sistema IPQoS administre el tráfico de clientes con acuerdos SLA de nivel alto.

EJEMPLO 34-2 Configuración de muestra para un servidor web "Best-Effort"

```

fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name Userweb
        next_action markAF12
        enable_stats FALSE
    }
    filter {
        name webout
        sport 80
        direction LOCAL_OUT
        class Userweb
    }
}
action {
    module dscpmk
    name markAF12
    params {
        global_stats FALSE
        dscp_map{0-63:12}
        next_action continue
    }
}

```

EJEMPLO 34-2 Configuración de muestra para un servidor web "Best-Effort" (Continuación)

```
}  
}
```

▼ Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico

Puede crear el primer archivo de configuración IPQoS en el directorio que le resulte más fácil para su mantenimiento. En las tareas de este capítulo se utiliza el directorio `/var/ipqos` como ubicación para archivos de configuración IPQoS. En el siguiente procedimiento se genera el segmento inicial del archivo de configuración IPQoS introducido en el [Ejemplo 34-1](#).

Nota – Al crear el archivo de configuración IPQoS, asegúrese de comenzar y finalizar cada instrucción de acción y cláusula con llaves (`{ }`). Para ver un ejemplo del uso de llaves, consulte el [Ejemplo 34-1](#).

1 Inicie una sesión en el servidor web de nivel alto y cree un archivo de configuración IPQoS con extensión `.qos`.

Los archivos de configuración IPQoS deben comenzar con el número de versión `fmt_version 1.0` como primera línea sin comentar.

2 A continuación del parámetro de abertura, escriba la instrucción de acción, que configura el clasificador IP genérico `ipgpc`.

Esta primera acción inicia el árbol de instrucciones de acción que compone el archivo de configuración IPQoS. Por ejemplo, el archivo `/var/ipqos/Goldweb.qos` comienza con la instrucción de acción inicial para llamar al clasificador `ipgpc`.

```
fmt_version 1.0
```

```
action {  
    module ipgpc  
    name ipgpc.classify
```

`fmt_version 1.0` Inicia el archivo de configuración IPQoS.

`action {` Inicia la instrucción de acción.

`module ipgpc` Configura el clasificador `ipgpc` como la primera acción del archivo de configuración.

`name ipgpc.classify` Define el nombre de la instrucción de acción de clasificador, que siempre debe ser `ipgpc.classify`.

Si necesita información sintáctica detallada sobre instrucciones de acción, consulte la sección “Instrucción `action`” en la [página 885](#) y la página de comando `man ipqosconf(1M)`.

3 Añada una cláusula `params` con el parámetro de estadísticas `global_stats`.

```
params {
    global_stats TRUE
}
```

El parámetro `global_stats TRUE` de la instrucción `ipgpc.classify` activa la recopilación de estadísticas para dicha acción. `global_stats TRUE` también activa la recopilación de estadísticas por clase cuando una definición de cláusula de clase específica `enable_stats TRUE`.

Activar las estadísticas afecta al rendimiento. Puede ser útil recopilar estadísticas en un archivo de configuración IPQoS nuevo para verificar que IPQoS funciona correctamente. Más adelante, puede desactivar la recopilación de estadísticas cambiando el argumento de `global_stats` a `FALSE`.

Las estadísticas globales son tan solo uno de los parámetros que se pueden definir en la cláusula `params`. Si necesita más información sobre sintaxis y otros datos de las cláusulas `params`, consulte la sección “Cláusula `params`” en la página 887 y la página de comando `man ipqosconf(1M)`.

4 Defina una cláusula que identifique el tráfico vinculado al servidor de nivel alto.

```
class {
    name goldweb
    next_action markAF11
    enable_stats FALSE
}
```

Esta instrucción se denomina una *cláusula class*. Una cláusula `class` tiene el siguiente contenido.

<code>name goldweb</code>	Crea la clase <code>goldweb</code> para identificar el tráfico vinculado al servidor <code>Goldweb</code> .
<code>next_action markAF11</code>	Indica al módulo <code>ipgpc</code> que debe pasar los paquetes de la clase <code>goldweb</code> a la instrucción de acción <code>markAF11</code> . La instrucción de acción <code>markAF11</code> llama al marcador <code>dscpmk</code> .
<code>enable_stats FALSE</code>	Activa la recopilación de estadísticas de la clase <code>goldweb</code> . Aunque, debido a que el valor de <code>enable_stats</code> es <code>FALSE</code> , las estadísticas de esta clase no están activadas.

Si necesita información detallada sobre la sintaxis de la cláusula `class`, consulte la sección “Cláusula `class`” en la página 886 y la página de comando `man ipqosconf(1M)`.

5 Defina una clase que identifique una aplicación que deba tener reenvío de máxima prioridad.

```
class {
    name video
    next_action markEF
    enable_stats FALSE
}
```

<code>name video</code>	Crea la clase <code>video</code> para identificar el tráfico saliente de video streaming del servidor Goldweb.
<code>next_action markEF</code>	Indica al módulo <code>ipgpc</code> que debe pasar los paquetes de la clase <code>video</code> a la instrucción <code>markEF</code> después de que <code>ipgpc</code> haya terminado el procesamiento. La instrucción <code>markEF</code> llama al marcador <code>dscpmk</code> .
<code>enable_stats FALSE</code>	Activa la recopilación de estadísticas de la clase <code>video</code> . Aunque, debido a que el valor de <code>enable_stats</code> es <code>FALSE</code> , la recopilación de estadísticas para esta clase no se activa.

- Véase también**
- Para definir filtros para la clase creada, consulte la sección [“Cómo definir filtros en el archivo de configuración IPQoS”](#) en la página 836.
 - Para crear otra cláusula para el archivo de configuración, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico”](#) en la página 834.

▼ Cómo definir filtros en el archivo de configuración IPQoS

El siguiente procedimiento muestra cómo definir filtros para una clase en el archivo de configuración IPQoS.

Antes de empezar En el procedimiento se asume que ya ha comenzado la creación del archivo y ha definido clases. Los pasos continúan con la generación del archivo `/var/ipqos/Goldweb.qos` creado en la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico”](#) en la página 834.

Nota – Al crear el archivo de configuración IPQoS, asegúrese de comenzar y finalizar cada cláusula `class` y cada `filtro` con llaves (`{ }`). Para ver un ejemplo del uso de llaves, consulte el [Ejemplo 34–1](#).

1 Abra el archivo de configuración IPQoS y busque la última clase definida.

Por ejemplo, en el servidor con IPQoS Goldweb, empezaría después de la siguiente cláusula `class` de `/var/ipqos/Goldweb.qos`:

```
class {
    name video
    next_action markEF
    enable_stats FALSE
}
```

2 Defina una cláusula `filter` para seleccionar el tráfico saliente del sistema IPQoS.

```
filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class goldweb
}
```

<code>name webout</code>	Asigna el nombre <code>webout</code> al filtro.
<code>sport 80</code>	Selecciona el tráfico con origen en el puerto 80, el puerto de tráfico HTTP (web).
<code>direction LOCAL_OUT</code>	Selecciona el tráfico saliente del sistema local.
<code>class goldweb</code>	Identifica la clase a la que pertenece el filtro, en este caso, la clase <code>goldweb</code> .

Si necesita información detallada y sintáctica sobre la cláusula `filter` del archivo de configuración IPQoS, consulte la sección [“Cláusula `filter`” en la página 887](#).

3 Defina una cláusula `filter` para seleccionar el tráfico de video streaming del sistema IPQoS.

```
filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
}
```

<code>name videoout</code>	Asigna el nombre <code>videoout</code> al filtro.
<code>sport videosrv</code>	Selecciona el tráfico con un puerto de origen <code>videosrv</code> , un puerto definido anteriormente para la aplicación de video streaming en este sistema.
<code>direction LOCAL_OUT</code>	Selecciona el tráfico saliente del sistema local.
<code>class video</code>	Identifica la clase a la que pertenece el filtro, en este caso, la clase <code>video</code> .

- Véase también**
- Para definir comportamientos de reenvío para los módulos de marcador, consulte la sección [“Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS” en la página 838](#).
 - Para definir parámetros de control de flujo para los módulos de medidor, consulte la sección [“Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 851](#).
 - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de kernel IPQoS” en la página 858](#).
 - Para definir filtros adicionales, consulte la sección [“Cómo definir filtros en el archivo de configuración IPQoS” en la página 836](#).

- Para crear clases para flujos de tráfico de aplicaciones, consulte la sección [“Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones”](#) en la página 847.

▼ Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS

El siguiente procedimiento muestra cómo definir el reenvío de tráfico añadiendo comportamientos por salto para una clase en el archivo de configuración IPQoS.

Antes de empezar

En el procedimiento se asume que ya tiene un archivo de configuración IPQoS con clases y filtros definidos. Los pasos continúan con la creación del archivo `/var/ipqos/Goldweb.qos` del [Ejemplo 34-1](#).

Nota – El procedimiento muestra cómo configurar el reenvío de tráfico utilizando el módulo de marcador `dscpmk`. Si necesita información sobre el reenvío de tráfico en sistemas VLAN utilizando el marcador `dlcosmk`, consulte la sección [“Uso del marcador `dlcosmk` con dispositivos VLAN”](#) en la página 879.

1 Abra el archivo de configuración IPQoS y localice el final del último filtro definido.

Por ejemplo, en el servidor con IPQoS Goldweb, empezaría después de la siguiente cláusula `filter` en `/var/ipqos/Goldweb.qos`:

```
filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
}
```

Observe que esta cláusula `filter` se encuentra al final de la instrucción `action` del clasificador `ipgpc`. Por lo tanto, necesita una llave de cierre para finalizar el filtro y otra para finalizar la instrucción `action`.

2 Invoque al marcador con la siguiente instrucción `action`.

```
action {
    module dscpmk
    name markAF11
```

`module dscpmk` Llama al módulo de marcador `dscpmk`.

`name markAF11` Asigna el nombre `markAF11` a la instrucción `action`.

La clase `goldweb` definida anteriormente incluye una instrucción `next_action markAF11`. Esta instrucción envía los flujos de tráfico a la instrucción de acción `markAF11` cuando el clasificador ha finalizado el procesamiento.

3 Defina acciones que debe ejecutar el marcador en el flujo de tráfico.

```
params {
    global_stats FALSE
    dscp_map{0-63:10}
    next_action continue
}
```

<code>global_stats FALSE</code>	Activa la recopilación de estadísticas de la instrucción <code>action</code> del marcador <code>markAF11</code> . Aunque, debido a que el valor de <code>enable_stats</code> es <code>FALSE</code> , no se recopilan estadísticas.
<code>dscp_map{0-63:10}</code>	Asigna un DSCP de valor <code>10</code> a los encabezados de paquetes de la clase de tráfico <code>goldweb</code> , que el marcador está procesando en ese momento.
<code>next_action continue</code>	Indica que no se necesita más procesamiento en los paquetes de la clase de tráfico <code>goldweb</code> , y que estos paquetes pueden volver al flujo de red.

El DSCP de valor `10` indica al marcador que debe definir todas las entradas del mapa `dscp` en el valor decimal `10` (binario `001010`). Este punto de código indica que los paquetes de la clase de tráfico `goldweb` están sujetos al comportamiento por salto `AF11`. `AF11` garantiza que todos los paquetes con DSCP de valor `10` reciben un servicio de alta prioridad y baja probabilidad de descarte. Por lo tanto, el tráfico saliente para clientes de nivel alto en `Goldweb` recibe la prioridad más alta disponible para el PHB de reenvío asegurado (AF). Para ver una tabla de puntos DSCP para AF, consulte la [Tabla 37-2](#).

4 Inicie otra instrucción `action` de marcador.

```
action {
    module dscpmk
    name markEF
```

<code>module dscpmk</code>	Llama al módulo de marcador <code>dscpmk</code> .
<code>name markEF</code>	Asigna el nombre <code>markEF</code> a la instrucción <code>action</code> .

5 Defina acciones que deba ejecutar el marcador en el flujo de tráfico.

```
params {
    global_stats TRUE
    dscp_map{0-63:46}
    next_action acct
}
```

<code>global_stats TRUE</code>	Activa la recopilación de estadísticas en la clase <code>video</code> , que selecciona paquetes de video streaming.
--------------------------------	---

<code>dscp_map{0-63:46}</code>	Asigna un DSCP de valor 46 a los encabezados de paquetes de la clase de tráfico video, que el marcador está procesando en ese momento.
<code>next_action acct</code>	Indica al módulo <code>dscpmk</code> que debe pasar los paquetes de la clase video a la instrucción <code>acct action</code> cuando <code>dscpmk</code> haya completado el procesamiento. La instrucción <code>acct action</code> invoca al módulo <code>flowacct</code> .

El DSCP de valor 46 indica al módulo `dscpmk` que debe establecer todas las entradas del mapa `dscp` en el valor decimal 46 (binario 101110) en el campo DS. Este punto de código indica que los paquetes de la clase de tráfico video están sujetos al comportamiento por salto de reenvío acelerado (EF).

Nota – El punto de código recomendado para EF es 46 (binario 101110). Otros puntos DSCP asignan comportamientos PHB AF a un paquete.

El PHB EF garantiza que los paquetes con el DSCP de valor 46 reciben la máxima precedencia en sistemas IPQoS y Diffserv. Las aplicaciones streaming requieren el servicio de prioridad más alta, por eso se les asignan comportamientos PHB EF en la directiva QoS. Si necesita más información sobre PHB de reenvío acelerado, consulte la sección [“Reenvío acelerado \(EF\) PHB” en la página 877](#).

- 6 Añada los puntos DSCP que ha creado a los archivos correspondientes del enrutador Diffserv.**
Si necesita más información, consulte [“Cómo configurar un enrutador en una red con IPQoS” en la página 855](#).

- Véase también**
- Para empezar a recopilar estadísticas de control de flujo sobre el tráfico, consulte la sección [“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 841](#).
 - Para definir comportamientos de reenvío para los módulos de marcador, consulte la sección [“Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS” en la página 838](#).
 - Para definir parámetros de control de flujo para los módulos de medidor, consulte la sección [“Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 851](#).
 - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de kernel IPQoS” en la página 858](#).
 - Para definir filtros adicionales, consulte la sección [“Cómo definir filtros en el archivo de configuración IPQoS” en la página 836](#).
 - Para crear clases para flujos de tráfico de aplicaciones, consulte la sección [“Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones” en la página 847](#).

▼ Cómo activar el control para una clase en el archivo de configuración IPQoS

El siguiente procedimiento muestra como activar el control de una clase de tráfico en el archivo de configuración IPQoS. El procedimiento muestra como definir el control de flujo para la clase video, introducida en la sección “[Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico](#)” en la [página 834](#). Esta clase selecciona el tráfico de video streaming, que debe formar parte de un acuerdo SLA de nivel alto del cliente.

Antes de empezar

En el procedimiento se asume que ya tiene un archivo de configuración IPQoS con clases, filtros y acciones de medición definidas, si corresponde, y acciones de marcado, si corresponde. Los pasos continúan con la creación del archivo `/var/ipqos/Goldweb.qos` del [Ejemplo 34-1](#).

1 Abra el archivo de configuración IPQoS y localice el final de la última instrucción `action` definida.

Por ejemplo, en el servidor con IPQoS Goldweb, empezaría después de la siguiente instrucción `action markEF` en `/var/ipqos/Goldweb.qos`.

```
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

2 Inicie una instrucción `action` que llame al control de flujo.

```
action {
    module flowacct
    name acct
```

`module flowacct` Invoca al módulo de control de flujo `flowacct`.

`name acct` Asigna el nombre `acct` a la instrucción `action`

3 Defina una cláusula `params` para el control de la clase de tráfico.

```
params {
    global_stats TRUE
    timer 10000
    timeout 10000
    max_limit 2048
    next_action continue
}
```

`global_stats TRUE` Activa la recopilación de estadísticas de la clase video, que selecciona paquetes de video streaming.

<code>timer 10000</code>	Especifica la duración del intervalo, en milisegundos, que se utiliza al explorar la tabla de flujos para detectar flujos con tiempo de espera superado. En este parámetro, el intervalo es de 10000 milisegundos.
<code>timeout 10000</code>	Especifica el valor de tiempo de espera de intervalo mínimo. El tiempo de espera de un flujo se supera cuando los paquetes del flujo no se envían durante un intervalo de tiempo de espera. En este parámetro, se supera el tiempo de espera de paquetes cuando transcurren 10000 milisegundos.
<code>max_limit 2048</code>	Determina el número máximo de registros de flujos en la tabla de flujos para esta instancia de acción.
<code>next_action continue</code>	Indica que no es necesario más procesamiento en los paquetes de la clase de tráfico video y que los paquetes pueden volver al flujo de red.

El módulo `flowacct` recopila información estadística sobre los flujos de paquetes de una clase específica hasta que se supera un valor de `timeout`.

- Véase también**
- Para configurar comportamientos por salto en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS”](#) en la página 855.
 - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de kernel IPQoS”](#) en la página 858.
 - Para crear clases para flujos de tráfico de aplicaciones, consulte la sección [“Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones”](#) en la página 847.

▼ Cómo crear un archivo de configuración IPQoS para un servidor web "Best-Effort"

El archivo de configuración IPQoS para un servidor web "best-effort" es ligeramente diferente al de un servidor web de nivel alto. Como muestra, en el procedimiento se utiliza el archivo de configuración del [Ejemplo 34-2](#).

- 1 Inicie una sesión en el servidor web "best-effort".
- 2 Cree un archivo de configuración IPQoS con extensión `.qos`.

```
fmt_version 1.0
action {
    module ipgpc
    name ipgpc.classify
    params {
```

```

    global_stats TRUE
}

```

El archivo `/var/ipqos/userweb.qos` debe comenzar con la instrucción `action` parcial para invocar al clasificador `ipgpc`. Además, la instrucción `action` también tiene una cláusula `params` para activar la recopilación de estadísticas. Si necesita una explicación de esta instrucción `action`, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834](#).

3 Defina una clase que identifique el tráfico vinculado con el servidor web "best-effort".

```

class {
    name userweb
    next_action markAF12
    enable_stats FALSE
}

```

<code>name userweb</code>	Crea una clase llamada <code>userweb</code> para reenviar el tráfico web de usuarios.
<code>next_action markAF1</code>	Indica al módulo <code>ipgpc</code> que debe transferir los paquetes de la clase <code>userweb</code> a la instrucción <code>action markAF12</code> cuando <code>ipgpc</code> haya completado el procesamiento. La instrucción <code>action markAF12</code> invoca al marcador <code>dscpmk</code> .
<code>enable_stats FALSE</code>	Activa la recopilación de estadísticas para la clase <code>userweb</code> . Aunque, debido a que el valor de <code>enable_stats</code> es <code>FALSE</code> , no se recopilan estadísticas para esta clase.

Para ver una explicación de la tarea de la cláusula `class`, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834](#).

4 Defina una cláusula `filter` para seleccionar los flujos de tráfico de la clase `userweb`.

```

filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class userweb
}

```

<code>name webout</code>	Asigna el nombre <code>webout</code> al filtro.
<code>sport 80</code>	Selecciona el tráfico con origen en el puerto 80, el puerto de tráfico HTTP (web).
<code>direction LOCAL_OUT</code>	Selecciona el tráfico saliente del sistema local.
<code>class userweb</code>	Identifica la clase a la que pertenece el filtro, en este caso, la clase <code>userweb</code> .

Para ver una explicación de la tarea de la cláusula `filter`, consulte la sección [“Cómo definir filtros en el archivo de configuración IPQoS” en la página 836.](#)

5 Inicie la instrucción `action` para invocar al marcador `dscpmk`.

```
action {
    module dscpmk
    name markAF12
```

`module dscpmk` Invoca al módulo de marcador `dscpmk`.

`name markAF12` Asigna el nombre `markAF12` a la instrucción `action`.

La clase definida previamente `userweb` incluye una instrucción `next_action markAF12`. Esta instrucción envía flujos de tráfico a la instrucción `action markAF12` cuando el clasificador finaliza el procesamiento.

6 Defina parámetros que debe usar el marcador para procesar el flujo de tráfico.

```
    params {
        global_stats FALSE
        dscp_map{0-63:12}
        next_action continue
    }
}
```

`global_stats FALSE` Activa la recopilación de estadísticas para la instrucción `action` del marcador `markAF12`. Aunque, debido a que el valor de `enable_stats` es `FALSE`, no se recopilan estadísticas.

`dscp_map{0-63:12}` Asigna un valor DSCP de 12 a los encabezados de paquetes de la clase de tráfico `userweb`, que esté procesando el marcador en ese momento.

`next_action continue` Indica que no es necesario más procesamiento en los paquetes de la clase de tráfico `userweb`, y que los paquetes pueden volver al flujo de red.

El valor DSCP de 12 indica al marcador que debe definir todas las entradas del mapa `dscp` en el valor decimal 12 (binario 001100). Este punto de código indica que los paquetes de la clase de tráfico `userweb` están sujetos al comportamiento por salto AF12. AF12 garantiza que todos los paquetes con el DSCP de valor 12 en el campo DS reciben un servicio de probabilidad de descarte media y prioridad alta.

7 Cuando haya completado el archivo de configuración IPQoS, aplique la configuración.

Véase también

- Para añadir clases y otra configuración para flujos de tráfico de aplicaciones, consulte la sección [“Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones” en la página 847.](#)
- Para configurar comportamientos por salto en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS” en la página 855.](#)

- Para activar el archivo de configuración IPQoS, consulte la sección “[Cómo aplicar una nueva configuración a los módulos de kernel IPQoS](#)” en la página 858.

Crear un archivo de configuración IPQoS para un servidor de aplicaciones

En esta sección se explica cómo crear un archivo de configuración para un servidor de aplicaciones que proporciona aplicaciones básicas a clientes. En el procedimiento se usa como ejemplo el servidor BigAPPS de la [Figura 33-4](#).

El siguiente archivo de configuración define actividades IPQoS para el servidor BigAPPS. Este servidor aloja FTP, correo electrónico (SMTP) y noticias de red (NNTP) para clientes.

EJEMPLO 34-3 Archivo de configuración IPQoS para un servidor de aplicaciones

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name smtp
        enable_stats FALSE
        next_action markAF13
    }
    class {
        name news
        next_action markAF21
    }
    class {
        name ftp
        next_action meterftp
    }
    filter {
        name smtpout
        sport smtp
        class smtp
    }
    filter {
        name newsout
        sport nntp
        class news
    }
    filter {
        name ftpout
        sport ftp
        class ftp
    }
}
```

EJEMPLO 34-3 Archivo de configuración IPQoS para un servidor de aplicaciones *(Continuación)*

```

    filter {
        name ftpdata
        sport ftp-data
        class ftp
    }
}
action {
    module dscpmk
    name markAF13
    params {
        global_stats FALSE
        dscp_map{0-63:14}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
action {
    module tokenmt
    name meterftp
    params {
        committed_rate 50000000
        committed_burst 50000000
        red_action_name AF31
        green_action_name markAF22
        global_stats TRUE
    }
}
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
}

```

▼ Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones

- 1 **Inicie una sesión en el servidor de aplicaciones con IPQoS y cree un archivo IPQoS con extensión .qos.**

Por ejemplo, `/var/ipqos/BigAPPS.qos` para el servidor de aplicaciones. Empezee con los siguientes comandos necesarios para iniciar la instrucción `action` que invoca al clasificador `ipgpc`:

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
}
```

Si necesita una explicación de la instrucción `action` inicial, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834.](#)

- 2 **Cree clases para seleccionar el tráfico de tres aplicaciones en el servidor BigAPPS.**

Añada las definiciones de clases después de la instrucción `action` de apertura.

```
class {
    name smtp
    enable_stats FALSE
    next_action markAF13
}
class {
    name news
    next_action markAF21
}
class {
    name ftp
    enable_stats TRUE
    next_action meterftp
}
```

<code>name smtp</code>	Crea una clase llamada <code>smtp</code> , que incluye los flujos de tráfico de correo electrónico que debe administrar la aplicación SMTP
<code>enable_stats FALSE</code>	Activa la recopilación de estadísticas para la clase <code>smtp</code> . Aunque, debido a que el valor de <code>enable_stats</code> es <code>FALSE</code> , no se recopilan estadísticas para esta clase.
<code>next_action markAF13</code>	Indica al módulo <code>ipgpc</code> que debe transferir los paquetes de la clase <code>smtp</code> a la instrucción <code>action markAF13</code> cuando <code>ipgpc</code> haya completado el procesamiento.

<code>name news</code>	Crea una clase llamada <code>news</code> , que incluye los flujos de tráfico de noticias de red que debe administrar la aplicación NNTP.
<code>next_action markAF21</code>	Indica al módulo <code>ipgpc</code> que debe transferir los paquetes de la clase <code>news</code> a la instrucción <code>action markAF21</code> cuando <code>ipgpc</code> haya completado el procesamiento.
<code>name ftp</code>	Crea una clase llamada <code>ftp</code> , que administra el tráfico saliente gestionado por la aplicación FTP.
<code>enable_stats TRUE</code>	Activa la recopilación de estadísticas para la clase <code>ftp</code> .
<code>next_action meterftp</code>	Indica al módulo <code>ipgpc</code> que debe transferir los paquetes de la clase <code>ftp</code> a la instrucción <code>action meterftp</code> cuando <code>ipgpc</code> haya completado el procesamiento.

Si necesita más información sobre cómo definir clases, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834](#).

3 Defina cláusulas `filter` para seleccionar el tráfico de las clases definidas en el paso 2.

```

filter {
    name smtpout
    sport smtp
    class smtp
}
filter {
    name newsout
    sport nntp
    class news
}
filter {
    name ftpout
    sport ftp
    class ftp
}
filter {
    name ftpdata
    sport ftp-data
    class ftp
}
}

```

<code>name smtpout</code>	Asigna el nombre <code>smtpout</code> al filtro.
<code>sport smtp</code>	Selecciona el tráfico con puerto de origen 25, el puerto para la aplicación <code>sendmail</code> (SMTP).
<code>class smtp</code>	Identifica la clase a la que pertenece el filtro, en este caso, la clase <code>smtp</code> .
<code>name newsout</code>	Asigna el nombre <code>newsout</code> al filtro.
<code>sport nntp</code>	Selecciona el tráfico con nombre de puerto origen <code>nntp</code> , el nombre de puerto para la aplicación de noticias de red (NNTP).

<code>class news</code>	Identifica la clase a la que pertenece el filtro, en este caso, la clase <code>news</code> .
<code>name ftpout</code>	Asigna el nombre <code>ftpout</code> al filtro.
<code>sport ftp</code>	Selecciona los datos de control con un puerto origen 21, el número de puerto para tráfico FTP.
<code>name ftpdata</code>	Asigna el nombre <code>ftpdata</code> al filtro.
<code>sport ftp-data</code>	Selecciona el tráfico con puerto de origen 20, el número de puerto para tráfico FTP.
<code>class ftp</code>	Identifica la clase a la que pertenecen los filtros <code>ftpout</code> y <code>ftpdata</code> , en este caso <code>ftp</code> .

- Véase también**
- Para definir filtros, consulte la sección [“Cómo definir filtros en el archivo de configuración IPQoS” en la página 836](#).
 - Para definir comportamientos de reenvío para el tráfico de aplicaciones, consulte la sección [“Cómo configurar el reenvío para el tráfico de aplicaciones en el archivo de configuración IPQoS” en la página 849](#).
 - Para configurar el control de flujo utilizando los módulos de medición, consulte la sección [“Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 851](#).
 - Para configurar la recopilación de datos sobre el flujo, consulte la sección [“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 841](#).

▼ Cómo configurar el reenvío para el tráfico de aplicaciones en el archivo de configuración IPQoS

En el siguiente procedimiento se muestra cómo configurar el reenvío para el tráfico de aplicaciones. En el procedimiento, se definen comportamientos por salto para clases de tráfico de aplicaciones que pueden tener precedencia más baja que otro tráfico de la red. Los pasos continúan con la creación del archivo `/var/ipqos/BigAPPS.qos` del [Ejemplo 34-3](#).

Antes de empezar En el procedimiento se asume que ya tiene un archivo de configuración IPQoS con clases y filtros definidos para las aplicaciones que se van a marcar.

- 1 Abra el archivo de configuración IPQoS creado para el servidor de aplicaciones y localice el final de la última cláusula `filter`.**

En el archivo `/var/ipqos/BigAPPS.qos`, el último filtro es el siguiente:

```
filter {
    name ftpdata
    sport ftp-data
    class ftp
```

```
}
}
```

2 Invoque al marcador del siguiente modo:

```
action {
    module dscpmk
    name markAF13
}
```

`module dscpmk` Invoca al módulo de marcador `dscpmk`.

`name markAF13` Asigna el nombre `markAF13` a la instrucción `action`.

3 Defina el comportamiento por salto que debe marcarse en los flujos de tráfico de correo electrónico.

```
params {
    global_stats FALSE
    dscp_map{0-63:14}
    next_action continue
}
```

`global_stats FALSE` Activa la recopilación de estadísticas para la instrucción `action` del marcador `markAF13`. Aunque, debido a que el valor de `enable_stats` es `FALSE`, no se recopilan estadísticas.

`dscp_map{0-63:14}` Asigna un DSCP de valor 14 a los encabezados de paquetes de la clase de tráfico `smtp`, que esté procesando el marcador en ese momento.

`next_action continue` Indica que no se necesita más procesamiento en los paquetes de la clase de tráfico `smtp`. Estos paquetes pueden volver al flujo de red.

El valor DSCP de 14 indica al marcador que debe definir todas las entradas del mapa `dscp` en el valor decimal 14 (binario 001110). El DSCP de valor 14 define el comportamiento por salto AF13. El marcador marca paquetes de la clase de tráfico `smtp` con el DSCP de valor 14 en el campo DS.

AF13 asigna todos los paquetes con un DSCP de 14 a una precedencia de alta probabilidad de descarte. Aunque, debido a que AF13 también garantiza una prioridad de Clase 1, el enrutador sigue garantizando una alta prioridad en cola al tráfico de correo electrónico saliente. Para ver una tabla de códigos para AF, consulte la [Tabla 37-2](#).

4 Añada una instrucción `action` de marcador para definir un comportamiento por salto para el tráfico de noticias de red:

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
    }
}
```

```
        next_action continue
    }
}
```

`name markAF21` Asigna el nombre `markAF21` a la instrucción `action`.

`dscp_map{0-63:18}` Asigna un valor DSCP de 18 a los encabezados de paquetes de la clase de tráfico `nntp` que esté procesando el marcador en ese momento.

El valor DSCP de 18 indica al marcador que debe definir todas las entradas del mapa `dscp` en el valor decimal 18 (binario 010010). El valor DSCP 18 define el comportamiento por salto AF21. El marcador marca los paquetes de la clase de tráfico `news` con el valor DSCP 18 en el campo DS.

AF21 garantiza que todos los paquetes con un valor DSCP de 18 reciben una precedencia de baja probabilidad de descarte, pero sólo con prioridad Clase 2. Por lo tanto, la posibilidad de que se descarte el tráfico de noticias de red es bajo.

- Véase también**
- Para añadir información de configuración para servidores web, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834](#).
 - Para configurar el control de flujo utilizando los módulos de medición, consulte la sección [“Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 851](#).
 - Para configurar la recopilación de datos sobre el flujo, consulte la sección [“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 841](#).
 - Para configurar comportamientos de reenvío en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS” en la página 855](#).
 - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de kernel IPQoS” en la página 858](#).

▼ Cómo configurar el control de flujo en el archivo de configuración IPQoS

Para controlar la tasa a la que un flujo de tráfico específico se envía en la red, debe definir parámetros para el medidor. Puede usar cualquiera de los dos módulos de medidor, `tokenmt` o `tswtclmt`, en el archivo de configuración IPQoS.

El siguiente procedimiento continúa con la creación del archivo de configuración IPQoS para el servidor de aplicaciones del [Ejemplo 34-3](#). En el procedimiento, no sólo se configura el medidor, sino también las acciones de marcador a las que se llama desde la instrucción `action`.

Antes de empezar En los pasos se asume que ya ha definido una clase y un filtro para controlar el flujo de la aplicación.

1 Abra el archivo de configuración IPQoS que ha creado para el servidor de aplicaciones.

En el archivo `/var/ipqos/BigAPPS.qos` , empiece después de la siguiente acción de marcador:

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

2 Cree una instrucción `action` de medidor para controlar el flujo de tráfico de la clase `ftp`.

```
action {
    module tokenmt
    name meterftp
```

`module tokenmt` Invoca al medidor `tokenmt`.

`name meterftp` Asigna el nombre `meterftp` a la instrucción `action` .

3 Añada parámetros para configurar la tasa del medidor.

```
params {
    committed_rate 50000000
    committed_burst 50000000
```

`committed_rate 50000000` Asigna una tasa de transmisión de 50.000.000 bps al tráfico de la clase `ftp`.

`committed_burst 50000000` Dedicar un tamaño de ráfaga de 50.000.000 al tráfico de la clase `ftp`.

Para ver una explicación de los parámetros `tokenmt`, consulte la sección [“Configuración de `tokenmt` como medidor de doble tasa” en la página 875](#).

4 Añada parámetros para configurar las precedencias de cumplimiento de tráfico:

```
    red_action markAF31
    green_action_name markAF22
    global_stats TRUE
}
```

`red_action_name markAF31` Indica que si el flujo de tráfico de la clase `ftp` excede la tasa asignada, los paquetes se envían a la instrucción `action` del marcador `markAF31`.

`green_action_name markAF22` Indica que si los flujos de tráfico de la clase `ftp` cumplen la tasa asignada, los paquetes se envían a la instrucción `action` de `markAF22`.

`global_stats TRUE` Activa las estadísticas de medición para la clase ftp.

Si necesita más información sobre el cumplimiento del tráfico, consulte la sección “[Módulo Meter](#)” en la [página 874](#).

5 Añada una instrucción `action` de marcador para asignar un comportamiento por salto a los flujos de tráfico de la clase ftp que no cumplan la tasa.

```
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
```

`module dscpmk` Invoca al módulo de marcador dscpmk.

`name markAF31` Asigna el nombre markAF31 a la instrucción action.

`global_stats TRUE` Activa las estadísticas para la clase ftp.

`dscp_map{0-63:26}` Asigna un valor DSCP de 26 a los encabezados de paquetes de la clase de tráfico ftp cuando el tráfico excede la tasa asignada.

`next_action continue` Indica que no se requiere más procesamiento para los paquetes de la clase de tráfico ftp. Estos paquetes pueden devolverse al flujo de red.

El valor DSCP de 26 indica al marcador que debe establecer todas las entradas del mapa dscp en el valor decimal 26 (binario 011010). El valor DSCP 26 define el comportamiento por salto AF31. El marcador marca los paquetes de la clase de tráfico ftp con el valor DSCP 26 en el campo DS.

AF31 garantiza que todos los paquetes con un valor DSCP de 26 reciben una precedencia de baja probabilidad de descarte, pero sólo con prioridad Clase 3. Por lo tanto, la posibilidad de que se descarte el tráfico FTP que no cumple la tasa es baja. Para ver una tabla de códigos para AF, consulte la [Tabla 37-2](#).

6 Añada una instrucción `action` de marcador para asignar un comportamiento por salto a los flujos de tráfico ftp que cumplen la tasa asignada.

```
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
```

<code>name markAF22</code>	Asigna el nombre markAF22 a la acción marker.
<code>dscp_map{0–63:20}</code>	Asigna un valor DSCP de 20 a los encabezados de paquetes de la clase de tráfico ftp cuando el tráfico ftp cumple la tasa configurada.

El valor DSCP de 20 indica al marcador que debe definir todas las entradas del mapa dscp en el valor decimal 20 (binario 010100). El valor DSCP de 20 define el comportamiento por salto AF22. El marcador marca los paquetes de la clase de tráfico ftp con el valor DSCP de 20 en el campo DS.

AF22 garantiza que todos los paquetes con un valor DSCP de 20 reciben una precedencia de probabilidad de descarte media con prioridad de Clase 2. Por lo tanto, el tráfico FTP que cumple la tasa tiene garantizada una precedencia con probabilidad de descarte media entre los flujos enviados simultáneamente por el sistema IPQoS. Aunque el enrutador asigna una prioridad de reenvío más alta a las clases de tráfico con una marca de precedencia de probabilidad de descarte media de Clase 1 o superior. Para ver una tabla de códigos para AF, consulte la [Tabla 37–2](#).

7 Añada los puntos DSCP que ha creado para el servidor de aplicaciones a los archivos correspondientes del enrutador Diffserv.

- Véase también**
- Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de kernel IPQoS”](#) en la página 858.
 - Para añadir información de configuración para servidores web, consulte la sección [“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico”](#) en la página 834.
 - Para configurar la recopilación de datos sobre el flujo, consulte la sección [“Cómo activar el control para una clase en el archivo de configuración IPQoS”](#) en la página 841.
 - Para configurar comportamientos de reenvío en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS”](#) en la página 855.

Suministro de servicios diferenciados en un enrutador

Para proporcionar servicios diferenciados reales, debe incluir un enrutador con Diffserv en la red, como se describe en [“Estrategias de hardware para la red Diffserv”](#) en la página 810. Los pasos necesarios para configurar Diffserv en un enrutador y actualizar los archivos del enrutador no se explican en esta guía.

En esta sección se detallan los pasos generales para coordinar la información de reenvío entre varios sistemas con IPQoS en la red y el enrutador Diffserv.

▼ Cómo configurar un enrutador en una red con IPQoS

En el siguiente procedimiento se utiliza como ejemplo la topología de la [Figura 33–4](#).

Antes de empezar En el siguiente procedimiento se asume que ya ha configurado los sistemas IPQoS de la red realizando las tareas anteriores de este capítulo.

- 1 **Revise los archivos de configuración de todos los sistemas con IPQoS de la red.**
- 2 **Identifique cada punto de código utilizado en las directivas QoS.**

Haga una lista de los puntos de código, y los sistemas y clases a los que se aplican. La siguiente tabla ilustra áreas en las que puede haberse usado el mismo punto de código. Esta práctica es aceptable. Aunque debe especificar otros criterios en el archivo de configuración IPQoS, como un selector de precedencia, para determinar la precedencia de las clases con marcas idénticas.

Por ejemplo, en la red de muestra que se utiliza en los procedimientos de este capítulo, puede generar la siguiente tabla de puntos de código.

Sistema	Clase	PHB	Punto de código DS
Goldweb	video	EF	46 (101110)
Goldweb	goldweb	AF11	10 (001010)
Userweb	webout	AF12	12 (001100)
BigAPPS	smtp	AF13	14 (001110)
BigAPPS	news	AF18	18 (010010)
BigAPPS	ftp conformant traffic	AF22	20 (010100)
BigAPPS	ftp nonconformant traffic	AF31	26 (011010)

- 3 **Añada los puntos de código de los archivos de configuración IPQoS de la red a los archivos correspondientes del enrutador Diffserv.**

Los puntos de código proporcionados deben facilitar la configuración del mecanismo de planificación Diffserv del enrutador. Consulte la documentación y el sitio web del fabricante del enrutador si necesita instrucciones.

Inicio y mantenimiento de IPQoS (Tareas)

Este capítulo contiene tareas para activar un archivo de configuración IPQoS y para el registro de eventos relacionados con IPQoS. Contiene los temas siguientes:

- “Administración IPQoS (Mapa de tareas)” en la página 857
- “Aplicación de una configuración IPQoS” en la página 858
- “Activación del registro syslog para mensajes IPQoS” en la página 859
- “Resolución de problemas con mensajes de error IPQoS” en la página 861

Administración IPQoS (Mapa de tareas)

Esta sección contiene el conjunto de tareas para iniciar y mantener el servicio IPQoS en un sistema Oracle Solaris. Antes de utilizar las tareas, debe tener un archivo de configuración IPQoS completado, como se describe en “Definición de una directiva QoS en el archivo de configuración IPQoS (Mapa de tarea)” en la página 829.

La tabla siguiente enumera y describe esas tareas y contiene vínculos a las secciones que describen cómo realizarlas.

Tarea	Descripción	Para obtener instrucciones
1. Configure IPQoS en un sistema.	Utilice el comando <code>ipqosconf</code> para activar el archivo de configuración IPQoS en un sistema.	“Cómo aplicar una nueva configuración a los módulos de kernel IPQoS” en la página 858
2. Haga que los comandos de inicio de Oracle Solaris apliquen el archivo de configuración IPQoS depurado cada vez que se inicie el sistema.	Asegúrese de que la configuración IPQoS se aplica cada vez que se reinicia el sistema.	“Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia” en la página 859.
3. Active el registro syslog para IPQoS.	Añada una entrada para activar el registro syslog de mensajes IPQoS.	“Cómo activar el registro de mensajes IPQoS durante el inicio” en la página 860.

Tarea	Descripción	Para obtener instrucciones
4. Solucione cualquier problema IPQoS que surja.	Solucione los problemas IPQoS utilizando mensajes de error.	Consulte los mensajes de error de la Tabla 35–1 .

Aplicación de una configuración IPQoS

La configuración IPQoS se activa y manipula con el comando `ipqosconf`.

▼ Cómo aplicar una nueva configuración a los módulos de kernel IPQoS

Se utiliza el comando `ipqosconf` para leer el archivo de configuración IPQoS y para configurar los módulos IPQoS del kernel UNIX. En el siguiente procedimiento se utiliza como ejemplo el archivo `/var/ipqos/Goldweb.qos`, creado en la sección “[Crear archivos de configuración IPQoS para servidores web](#)” en la [página 832](#). Si necesita información detallada, consulte la página de comando `man ipqosconf(1M)`.

- 1 **Asuma la función de administrador principal o hágase superusuario en el sistema con IPQoS.**
La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2](#), “[Trabajo con Solaris Management Console \(tareas\)](#)” de *Guía de administración del sistema: administración básica*.

- 2 **Aplique la nueva configuración.**

```
# /usr/sbin/ipqosconf -a/var/ipqos/Goldweb.qos
```

`ipqosconf` escribe la información en el archivo de configuración IPQoS especificado de los módulos IPQoS del kernel de Oracle Solaris. En este ejemplo, el contenido de `/var/ipqos/Goldweb.qos` se aplica al kernel de Oracle Solaris actual.

Nota – Cuando se aplica un archivo de configuración IPQoS con la opción `-a`, las acciones del archivo sólo se activan para la sesión actual.

- 3 **Compruebe y depure la nueva configuración IPQoS.**

Utilice las herramientas de UNIX para supervisar el comportamiento IPQoS y recopilar estadísticas sobre la implementación IPQoS. Esta información permite determinar si la configuración funciona como se esperaba.

Véase también ■ Para ver estadísticas sobre cómo funcionan los módulos IPQoS, consulte la sección “[Recopilación de estadísticas](#)” en la [página 868](#).

- Para registrar los mensajes `ipqosconf`, consulte la sección [“Activación del registro syslog para mensajes IPQoS” en la página 859](#).
- Para asegurarse de que la configuración IPQoS actual se aplica en cada inicio, consulte la sección [“Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia” en la página 859](#).

▼ Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia

Debe hacer que la configuración IPQoS sea persistente en cada reinicio. En caso contrario, la configuración actual sólo se aplica hasta que el sistema se reinicia. Cuando la configuración IPQoS funcione correctamente en un sistema, haga lo siguiente para que la configuración sea persistente cada vez que se reinicia.

1 Asuma la función de administrador principal o hágase superusuario en el sistema con IPQoS.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 Compruebe que existe una configuración IPQoS en los módulos de kernel.

```
# ipqosconf -l
```

Si existe una configuración, `ipqosconf` la muestra en pantalla. Si no recibe ninguna respuesta, aplique la configuración, como se explica en la sección [“Cómo aplicar una nueva configuración a los módulos de kernel IPQoS” en la página 858](#).

3 Asegúrese de que la configuración IPQoS se aplica cada vez que el sistema IPQoS se reinicia.

```
# /usr/sbin/ipqosconf -c
```

La opción `-c` hace que la configuración IPQoS actual esté presente en el archivo de configuración de inicio `/etc/inet/ipqosinit.conf`.

Activación del registro syslog para mensajes IPQoS

Para registrar mensajes de inicio IPQoS, es necesario modificar el archivo `/etc/syslog.conf` como se explica en el siguiente procedimiento.

▼ Cómo activar el registro de mensajes IPQoS durante el inicio

- 1 **Asuma la función de administrador principal o hágase superusuario en el sistema con IPQoS.**

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Abra el archivo `/etc/syslog.conf`.**

- 3 **Añada el siguiente texto como última entrada en el archivo.**

```
user.info                /var/adm/messages
```

Utilice tabuladores en lugar de espacios entre las columnas.

La entrada registra todos los mensajes de inicio generados por IPQoS en el archivo `/var/adm/messages`.

- 4 **Reinicie el sistema para aplicar los mensajes.**

Ejemplo 35–1 Salida IPQoS de `/var/adm/messages`

Al revisar `/var/adm/messages` después de reiniciar el sistema, la salida puede contener mensajes de registro IPQoS similares a los siguientes.

```
May 14 10:44:33 ipqos-14 ipqosconf: [ID 815575 user.info]
New configuration applied.
May 14 10:44:46 ipqos-14 ipqosconf: [ID 469457 user.info]
Current configuration saved to init file.
May 14 10:44:55 ipqos-14 ipqosconf: [ID 435810 user.info]
Configuration flushed.
```

También puede encontrar mensajes de error IPQoS similares a los siguientes en el archivo `/var/adm/messages` del sistema con IPQoS.

```
May 14 10:56:47 ipqos-14 ipqosconf: [ID 123217 user.error]
Missing/Invalid config file fmt_version.
May 14 10:58:19 ipqos-14 ipqosconf: [ID 671991 user.error]
No ipgpc action defined.
```

Para ver una descripción de estos mensajes de error, consulte la [Tabla 35–1](#).

Resolución de problemas con mensajes de error IPQoS

Esta sección contiene una tabla de mensajes de error generados por IPQoS y su posible solución.

TABLA 35-1 Mensajes de error IPQoS

Mensaje de error	Descripción	Solución
Undefined action in parameter <i>nombre de parámetro</i> action <i>nombre de acción</i>	En el archivo de configuración IPQoS, el nombre de acción especificado en <i>nombre de parámetro</i> no existe en el archivo de configuración.	Cree la acción. O haga referencia a otra acción en el parámetro.
action <i>nombre de acción</i> involved in cycle	En el archivo de configuración IPQoS, <i>nombre de acción</i> forma parte de un ciclo de acciones, lo que no está permitido por IPQoS.	Determine el ciclo de acciones. A continuación, elimine una de las referencias cíclicas del archivo de configuración IPQoS.
Action <i>nombre de acción</i> isn't referenced by any other actions	Una definición de acción no <i>ipgpc</i> no es referenciada por ninguna otra acción definida en la configuración IPQoS, lo que no está permitido por IPQoS.	Elimine la acción no referenciada. También puede hacer que otra acción haga referencia a la acción no referenciada.
Missing/Invalid config file <i>fmt_version</i>	El formato del archivo de configuración no está especificado como primera entrada del archivo como requiere IPQoS.	Añada la versión de formato, como se explica en “Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834 .
Unsupported config file format version	La versión de formato especificada en el archivo de configuración no es compatible con IPQoS.	Cambie la versión de formato por <i>fmt_version 1.0</i> , esto es necesario para ejecutar la versión Solaris 9 9/02 de IPQoS y versiones posteriores.
No <i>ipgpc</i> action defined.	No ha definido una acción para el clasificador <i>ipgpc</i> en el archivo de configuración, como requiere IPQoS.	Defina una acción para <i>ipgpc</i> , como se muestra en la sección “Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 834 .
Can't commit a null configuration	Cuando ejecutó <i>ipqosconf -c</i> para confirmar una configuración, dicha configuración estaba vacía, lo que no está permitido por IPQoS.	Asegúrese de aplicar un archivo de configuración antes de intentar confirmar una configuración. Si necesita instrucciones, consulte “Cómo aplicar una nueva configuración a los módulos de kernel IPQoS” en la página 858 .
Invalid CIDR mask on line <i>número de línea</i>	En el archivo de configuración, ha utilizado una máscara CIDR como parte de la dirección IP que está fuera del intervalo de direcciones IP válidas.	Cambie el valor de máscara por uno que se encuentre entre 1–32 para IPv4 y 1–128 para IPv6.
Address masks aren't allowed for host names line <i>número de línea</i>	En el archivo de configuración, ha definido una máscara CIDR para un nombre de host, lo que no está permitido en IPQoS.	Elimine la máscara o cambie el nombre de host por una dirección IP.

TABLA 35-1 Mensajes de error IPQoS (Continuación)

Mensaje de error	Descripción	Solución
Invalid module name line <i>número de línea</i>	En el archivo de configuración, el nombre de módulo que ha especificado en una instrucción de acción no es válido.	Compruebe que el nombre de módulo esté bien escrito. Para ver una lista de módulos IPQoS, consulte la Tabla 37-5 .
ipgpc action has incorrect name line <i>número de línea</i>	El nombre asignado a la acción ipgpc en el archivo de configuración no es el nombre ipgpc.classify requerido.	Cambie el nombre de la acción ipgpc.classify.
Second parameter clause not supported line <i>número de línea</i>	En el archivo de configuración, ha especificado dos cláusulas de parámetro para una única acción, lo que no está permitido por IPQoS.	Combine todos los parámetros de la acción en una única cláusula de parámetro.
Duplicate named action	En el archivo de configuración, ha asignado el mismo nombre a dos acciones.	Cambie el nombre de una de las acciones o elimínela.
Duplicate named filter/class in action <i>nombre de acción</i>	Ha asignado el mismo nombre a dos filtros o dos clases en la misma acción, lo que no se permite en el archivo de configuración IPQoS.	Cambie el nombre de uno de los filtros o clases, o elimínelo.
Undefined class in filter <i>nombre de filtro in action nombre de acción</i>	En el archivo de configuración, el filtro hace referencia a una clase no definida en la acción.	Cree la clase, o cambie la referencia del filtro a una clase existente.
Undefined action in class <i>nombre de clase action nombre de acción</i>	La clase hace referencia a una acción no definida en el archivo de configuración.	Cree la acción, o cambie la referencia a una acción existente.
Invalid parameters for action <i>nombre de acción</i>	En el archivo de configuración, uno de los parámetros no es válido.	Para ver el módulo al que llama la acción especificada, consulte la entrada de módulo de la sección “Arquitectura IPQoS y el modelo Diffserv” en la página 871 . También puede consultar la página de comando man ipqosconf(1M) .
Mandatory parameter missing for action <i>nombre de acción</i>	No ha definido un parámetro requerido para una acción en el archivo de configuración.	Para ver el módulo al que llama la acción especificada, consulte la entrada de módulo de la sección “Arquitectura IPQoS y el modelo Diffserv” en la página 871 . También puede consultar la página de comando man ipqosconf(1M) .
Max number of classes reached in ipgpc	Ha especificado más clases de las permitidas en la acción ipgpc del archivo de configuración IPQoS. El número máximo es 10007.	Revise el archivo de configuración y elimine las clases innecesarias. También puede aumentar el número máximo de clases añadiendo al archivo <code>/etc/system</code> la entrada <code>ipgpc_max_classes</code> <i>número de clases</i> .

TABLA 35-1 Mensajes de error IPQoS (Continuación)

Mensaje de error	Descripción	Solución
Max number of filters reached in action ipgpc	Ha especificado más filtros de los permitidos en la acción ipgpc del archivo de configuración IPQoS. El número máximo es 10007.	Revise el archivo de configuración y elimine los filtros innecesarios. También puede aumentar el número máximo de filtros añadiendo al archivo <code>/etc/system</code> la entrada <code>ipgpc_max_filters</code> número de filtros.
Invalid/missing parameters for filter <i>nombre de filtro</i> in action ipgpc	En el archivo de configuración, el filtro <i>nombre de filtro</i> tiene parámetros no válidos o no especificados.	Consulte la página de comando <code>man ipqosconf(1M)</code> para ver una lista de parámetros válidos.
Name not allowed to start with '!', line <i>número de línea</i>	Inicia una acción, un filtro o un nombre de clase con un signo de exclamación (!), lo cual no está permitido en el archivo IPQoS.	Elimine el signo de exclamación o cambie el nombre completo de la acción, clase o filtro.
Name exceeds the maximum name length line <i>número de línea</i>	Ha definido un nombre de una acción, clase o filtro en el archivo de configuración que excede la longitud máxima de 23 caracteres.	Asigne un nombre más corto a la acción, clase o filtro.
Array declaration line <i>número de línea</i> is invalid	En el archivo de configuración, la declaración de matriz del parámetro de la línea <i>número de línea</i> no es válido.	Para ver la sintaxis correcta de la declaración de matriz a la que llama la instrucción de acción con la matriz no válida, consulte la sección “ Arquitectura IPQoS y el modelo Diffserv ” en la página 871. También puede consultar la página de comando <code>man ipqosconf(1M)</code> .
Quoted string exceeds line, <i>número de línea</i>	La cadena no tiene las comillas de cierre en la misma línea, lo que es obligatorio en el archivo de configuración.	Asegúrese de que la cadena citada empieza y termina en la misma línea en el archivo de configuración.
Invalid value, line <i>número de línea</i>	El valor definido en la línea <i>número de línea</i> del archivo de configuración no es compatible con el parámetro.	Para ver los valores aceptables para el módulo al que llama la instrucción de acción, consulte la descripción del módulo en la sección “ Arquitectura IPQoS y el modelo Diffserv ” en la página 871. También puede consultar la página de comando <code>man ipqosconf(1M)</code> .
Unrecognized value, line <i>número de línea</i>	El valor de <i>número de línea</i> del archivo de configuración no es un valor de enumeración admitido para este parámetro.	Compruebe que el valor de enumeración es correcto para el parámetro. Para ver una descripción del módulo al que llama la instrucción de acción con el número de línea no reconocido, consulte la sección “ Arquitectura IPQoS y el modelo Diffserv ” en la página 871. También puede consultar la página de comando <code>man ipqosconf(1M)</code> .
Malformed value list line <i>número de línea</i>	La enumeración especificada en <i>número de línea</i> del archivo de configuración no cumple la sintaxis de especificación.	Para ver la sintaxis correcta del módulo al que llama la instrucción de acción con la lista de valores mal formada, consulte la descripción del módulo en la sección “ Arquitectura IPQoS y el modelo Diffserv ” en la página 871. También puede consultar la página de comando <code>man ipqosconf(1M)</code> .

TABLA 35-1 Mensajes de error IPQoS (Continuación)

Mensaje de error	Descripción	Solución
Duplicate parameter line <i>número de línea</i>	Se ha especificado un parámetro duplicado en <i>número de línea</i> , lo que no está permitido en el archivo de configuración.	Elimine uno de los parámetros duplicados.
Invalid action name line <i>número de línea</i>	Ha asignado a la acción de <i>número de línea</i> del archivo de configuración un nombre que utiliza el nombre predefinido “continue” o “drop”.	Cambie el nombre de la acción de modo que no utilice un nombre predefinido.
Failed to resolve src/dst host name for filter at line <i>número de línea</i> , ignoring filter	ipqosconf no ha podido determinar la dirección de origen o destino definida para el filtro en el archivo de configuración. Por lo tanto, se omite el filtro.	Si el filtro es importante, intente aplicar la configuración más adelante.
Incompatible address version line <i>número de línea</i>	La versión IP de la dirección de <i>número de línea</i> es incompatible con la versión de una dirección IP especificada previamente o parámetro <i>ip_version</i> .	Cambie las dos entradas en conflicto para que sean compatibles.
Action at line <i>número de línea</i> has the same name as currently installed action, but is for a different module	Ha intentado cambiar el módulo de una acción que ya existe en la configuración IPQoS del sistema, lo que no está permitido.	Vacíe la configuración actual antes de aplicar la nueva configuración.

Uso de control de flujo y recopilación de estadísticas (Tareas)

En este capítulo se explica como obtener datos de control y estadísticas sobre el tráfico administrador por un sistema IPQoS. Se explican los siguientes temas:

- “Establecimiento del control de flujo (Mapa de tareas)” en la página 865
- “Registro de información sobre flujos de tráfico” en la página 866
- “Recopilación de estadísticas” en la página 868

Establecimiento del control de flujo (Mapa de tareas)

En el siguiente mapa de tareas se enumeran las tareas genéricas para obtener información sobre flujos de tráfico utilizando el módulo `flowacct`. El mapa también ofrece vínculos a los procedimientos para realizar estas tareas.

Tarea	Descripción	Para obtener instrucciones
1. Cree un archivo para guardar la información de control de flujos de tráfico.	Utilice el comando <code>acctadm</code> para crear un archivo en el que se almacenarán los resultados del procesamiento de <code>flowacct</code> .	“Cómo crear un archivo para datos de control de flujo” en la página 866
2. Defina los parámetros <code>flowacct</code> en el archivo de configuración IPQoS.	Defina valores para los parámetros <code>timer</code> , <code>timeout</code> y <code>max_limit</code> .	“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 841

Registro de información sobre flujos de tráfico

Se utiliza el módulo IPQoS `flowacct` para recopilar información sobre flujos de tráfico. Por ejemplo, puede recopilar direcciones de origen y destino, número de paquetes de un flujo y datos similares. El proceso de recopilar y registrar información sobre flujos se denomina *control de flujo*.

Los resultados del control de flujo de tráfico de una clase determinada se guardan en una tabla de *registros de flujo*. Cada registro de flujo contiene una serie de atributos. Estos atributos contienen datos sobre flujos de tráfico de una clase determinada en un intervalo de tiempo. Para ver una lista de los atributos de `flowacct`, consulte la [Tabla 37-4](#).

El control de flujo es especialmente útil para facturar a los clientes como está definido en su acuerdo de nivel de servicio. También puede utilizar el control de flujo para obtener estadísticas de aplicaciones importantes. Esta sección contiene tareas para utilizar `flowacct` con la herramienta de contabilidad ampliada de Oracle Solaris para obtener datos sobre flujos de tráfico.

La siguiente información se encuentra en otras fuentes, no en este capítulo:

- Si necesita instrucciones para crear una instrucción de acción para `flowacct` en el archivo de configuración IPQoS, consulte “[Cómo configurar el control de flujo en el archivo de configuración IPQoS](#)” en la página 851.
- Para aprender cómo funciona `flowacct`, consulte “[Módulo Classifier](#)” en la página 871.
- Si necesita información técnica, consulte la página de comando `man flowacct(7ipp)`.

▼ Cómo crear un archivo para datos de control de flujo

Antes de añadir una acción `flowacct` al archivo de configuración IPQoS, debe crear un archivo para los registros de flujo desde el módulo `flowacct`. Para esto se utiliza el comando `acctadm`. `acctadm` puede registrar atributos básicos o extendidos en el archivo. Todos los atributos `flowacct` están enumerados en la [Tabla 37-4](#). Si necesita información detallada sobre `acctadm`, consulte la página de comando `man acctadm(1M)`.

1 Asuma la función de administrador principal o hágase superusuario en el sistema con IPQoS.

La función de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

2 Cree un archivo de control de flujo básico.

En el siguiente ejemplo se muestra cómo crear un archivo de control de flujo básico para el servidor web configurado en el [Ejemplo 34-1](#).

```
# /usr/sbin/acctadm -e basic -f /var/ipqos/goldweb/account.info flow
```

<code>acctadm -e</code>	Invoca a <code>acctadm</code> con la opción <code>-e</code> . La opción <code>-e</code> activa los argumentos que hay a continuación.
<code>basic</code>	Determina que sólo los datos de los ocho atributos básicos <code>flowacct</code> se registran en el archivo.
<code>/var/ipqos/goldweb/account.info</code>	Especifica el nombre de ruta completo del archivo que contendrá los registros de flujo de <code>flowacct</code> .
<code>flow</code>	Indica a <code>acctadm</code> que debe activar el control de flujo.

3 Para ver la información de control de flujo del sistema IPQoS, escriba `acctadm` sin argumentos.

`acctadm` genera la siguiente salida:

```
Task accounting: inactive
  Task accounting file: none
  Tracked task resources: none
  Untracked task resources: extended
  Process accounting: inactive
  Process accounting file: none
  Tracked process resources: none
  Untracked process resources: extended,host,mstate
  Flow accounting: active
  Flow accounting file: /var/ipqos/goldweb/account.info
  Tracked flow resources: basic
  Untracked flow resources: dsfield,ctime,lseen,projid,uid
```

Todas las entradas menos las cuatro últimas son para su uso con la función Solaris Resource Manager. En la siguiente tabla se explican las entras específicas de IPQoS.

Entrada	Descripción
<code>Flow accounting: active</code>	Indica que el control de flujo está activado.
<code>Flow accounting file:</code> <code>/var/ipqos/goldweb/account.info</code>	Da el nombre del archivo de control de flujo actual.
<code>Tracked flow resources: basic</code>	Indica que sólo se supervisan los atributos de flujo básicos.
<code>Untracked flow resources:</code> <code>dsfield,ctime,lseen,projid,uid</code>	Enumera los atributos <code>flowacct</code> que no se supervisan en el archivo.

4 (Optativo) Añadir los atributos ampliados al archivo de control.

```
# acctadm -e extended -f /var/ipqos/goldweb/account.info flow
```

5 (Optativo) Volver a registrar sólo los atributos básicos en el archivo de control.

```
# acctadm -d extended -e basic -f /var/ipqos/goldweb/account.info
```

La opción `-d` desactiva la contabilidad ampliada.

6 Ver el contenido de un archivo de control de flujo.

Las instrucciones para ver los contenidos de un archivo de control de flujo se encuentran en [“Interfaz Perl para libexacct” de Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#).

- Véase también**
- Para ver información detallada sobre la función de contabilidad ampliada, consulte el [Capítulo 4, “Contabilidad ampliada \(descripción general\)” de Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#).
 - Para definir parámetros flowacct en el archivo de configuración IPQoS, consulte [“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 841](#).
 - Para imprimir los datos del archivo creado con acctadm, consulte [“Interfaz Perl para libexacct” de Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#).

Recopilación de estadísticas

Puede utilizar el comando `kstat` para generar estadísticas de los módulos IPQoS. Use la sintaxis siguiente:

```
/bin/kstat -m ipqos-module-name
```

Puede especificar cualquier nombre de módulo IPQoS válido, como se muestra en la [Tabla 37–5](#). Por ejemplo, para ver estadísticas generadas por el marcador `dscpmk`, utilice el siguiente comando de `kstat`:

```
/bin/kstat -m dscpmk
```

Si necesita información técnica, consulte la página de comando `man kstat(1M)`.

EJEMPLO 36–1 Estadísticas kstat de IPQoS

A continuación se muestra un ejemplo del posible resultado al ejecutar `kstat` para obtener estadísticas sobre el módulo `flowacct`.

```
# kstat -m flowacct
module: flowacct          instance: 3
name:   Flowacct statistics class:   flacct
        bytes_in_tbl      84
        crtime            345728.504106363
        epackets          0
        flows_in_tbl      1
        nbytes            84
        npackets          1
        snaptime          345774.031843301
        usedmem            256
```

EJEMPLO 36-1 Estadísticas kstat de IPQoS (Continuación)

<code>class: flacct</code>	Da el nombre de la clase a la que pertenecen los flujos de tráfico, en este caso <code>flacct</code> .
<code>bytes_in_tbl</code>	Número total de bytes en la tabla de flujo. El número total de bytes es la suma en bytes de todos los registros de flujo actuales de la tabla de flujo. La cantidad total de bytes de esta tabla de flujo es de 84. Si no hay ningún flujo en la tabla, el valor de <code>bytes_in_tbl</code> es 0.
<code>crtime</code>	La última vez que se creó esta salida de kstat.
<code>epackets</code>	Número de paquetes que resultaron en un error durante el procesamiento, en este ejemplo 0.
<code>flows_in_tbl</code>	Número de registros de flujo que hay en la tabla de flujos, en este ejemplo es 1. Si no hay ningún registro en la tabla, el valor de <code>flows_in_tbl</code> es 0.
<code>nbytes</code>	Número total de bytes observados por esta instancia de acción <code>flowacct</code> , en este ejemplo 84. El valor incluye bytes que se encuentran actualmente en la tabla de flujo. El valor también incluye bytes obsoletos que ya no se encuentran en la tabla de flujo.
<code>npackets</code>	Número total de paquetes observados por esta instancia de acción <code>flowacct</code> , en este ejemplo 1. <code>npackets</code> incluye paquetes que se encuentran actualmente en la tabla de flujo. <code>npackets</code> también incluye paquetes obsoletos, que ya no se encuentran en la tabla de flujo.
<code>usedmem</code>	Memoria en bytes en uso por la tabla de flujo mantenida por esta instancia <code>flowacct</code> . En el ejemplo, el valor <code>usedmem</code> es 256. El valor de <code>usedmem</code> es 0 cuando la tabla de flujo no contiene ningún registro de flujo.

IPQoS detallado (Referencia)

Este capítulo contiene material de referencia con información detallada sobre los siguientes temas de IPQoS:

- “Arquitectura IPQoS y el modelo Diffserv” en la página 871
- “Archivo de configuración IPQoS” en la página 884
- “Herramienta de configuración `ipqosconf`” en la página 887

Para obtener una descripción general, consulte el [Capítulo 32, “Introducción a IPQoS \(Descripción general\)”](#). Si necesita información sobre la planificación, consulte el [Capítulo 33, “Planificación para una red con IPQoS \(Tareas\)”](#). Para ver los procedimientos para configurar IPQoS, consulte el [Capítulo 34, “Creación del archivo de configuración IPQoS \(Tareas\)”](#).

Arquitectura IPQoS y el modelo Diffserv

En esta sección se describe la arquitectura IPQoS y cómo IPQoS implementa el modelo de servicios diferenciados (Diffserv) definido en [RFC 2475, An Architecture for Differentiated Services](http://www.ietf.org/rfc/rfc2475.txt?number=2475) (<http://www.ietf.org/rfc/rfc2475.txt?number=2475>). Los siguientes elementos del modelo Diffserv están incluidos en IPQoS:

- Clasificador
- Medidor
- Marcador

Además, IPQoS incluye el módulo de control de flujo y el marcador `dlcosmk` para su uso en dispositivos VLAN (red de área local virtual).

Módulo Classifier

En el modelo Diffserv, el módulo *classifier* se encarga de organizar los flujos de tráfico seleccionados en grupos a los que se aplican diferentes niveles de servicio. Los clasificadores definidos en RFC 2475 se diseñaron originalmente para enrutadores de límite de sistema. En

cambio, el clasificador IPQoS `ipgpc` está diseñado para administrar flujos de tráfico en hosts internos de la red local. Por lo tanto, una red con sistemas IPQoS y un enrutador Diffserv puede proporcionar un alto nivel de servicios diferenciados. Para ver una descripción técnica de `ipgpc`, consulte la página de comando `man ipgpc(7ipp)`.

El clasificador `ipgpc` se encarga de lo siguiente:

1. Selecciona los flujos de tráfico que cumplen los criterios especificados en el archivo de configuración IPQoS en el sistema con IPQoS
La directiva QoS define varios criterios que deben estar presentes en los encabezados de paquetes. Estos criterios se denominan *selectores*. El clasificador `ipgpc` compara estos selectores con los encabezados de paquetes que recibe el sistema IPQoS. Después, `ipgpc` selecciona todos los paquetes que coinciden.
2. Separa los flujos de paquetes en *clases*, tráfico de red con las mismas características, como se ha definido en el archivo de configuración IPQoS
3. Examina el valor del campo de servicios diferenciados (DS) del paquete para comprobar si contiene un punto de código de servicios diferenciados (DSCP)
La presencia de un punto de código DSCP indica si el tráfico entrante ha sido marcado en su origen con un comportamiento de reenvío.
4. Determina qué otras acciones están especificadas en la configuración IPQoS para paquetes de una clase específica
5. Transfiere los paquetes al siguiente módulo IPQoS especificado en el archivo de configuración IPQoS, o los devuelve al flujo de red

Para ver una descripción general del clasificador, consulte “[Descripción general del clasificador \(ipgpc\)](#)” en la [página 799](#). Si necesita información sobre cómo invocar al clasificador en el archivo de configuración IPQoS, consulte “[Archivo de configuración IPQoS](#)” en la [página 884](#).

Selectores IPQoS

El clasificador `ipgpc` admite varios selectores que se pueden usar en la cláusula `filter` del archivo de configuración IPQoS. Al usar un filtro, utilice siempre el número mínimo de selectores necesarios para extraer el tráfico de una clase determinada. El número de filtros definidos repercute en el rendimiento de IPQoS.

En la siguiente tabla se muestran los selectores disponibles para `ipgpc`.

TABLA 37-1 Selectores de filtro para el clasificador IPQoS

Selector	Argumento	Información seleccionada
saddr	Número de dirección IP.	Dirección de origen.
daddr	Número de dirección IP.	Dirección de destino.

TABLA 37-1 Selectores de filtro para el clasificador IPQoS (Continuación)

Selector	Argumento	Información seleccionada
sport	Un número de puerto o nombre de servicio, definido en <code>/etc/services</code> .	Puerto de origen del que proviene una clase de tráfico.
dport	Un número de puerto o nombre de servicio, definido en <code>/etc/services</code> .	Puerto de destino de una clase de tráfico.
protocol	Un número o nombre de protocolo, definido en <code>/etc/protocols</code> .	Protocolo que usará esta clase de tráfico.
dsfield	Punto de código DS (DSCP) con un valor de 0-63.	DSCP que define cualquier comportamiento de reenvío que deb aplicarse al paquete. Si se especifica este parámetro, el parámetro <code>dsfield_mask</code> también debe especificarse.
dsfield_mask	Máscara de bit con un valor de 0-255.	Se utiliza en combinación con el selector <code>dsfield</code> . <code>dsfield_mask</code> se aplica al selector <code>dsfield</code> para determinar qué bit se utiliza para la comparación.
if_name	Nombre de interfaz.	Interfaz que se utiliza para el tráfico entrante o saliente de una clase determinada.
user	Número del ID de usuario o nombre de usuario de UNIX que se seleccionará. Si no hay ningún ID de usuario ni nombre de usuario en el paquete, se utilizará la opción predeterminada, -1.	ID de usuario que se suministra a una aplicación.
projid	Número de ID de proyecto que se seleccionará.	ID de proyecto que se suministra a una aplicación.
priority	Número de prioridad. La prioridad más baja es 0.	Prioridad que se asigna a paquetes de esta clase. La prioridad se utiliza para ordenar la importancia de filtros de la misma clase.
direction	El argumento puede ser uno de los siguientes:	Dirección del flujo de paquete en el equipo IPQoS.
	LOCAL_IN	Tráfico de entrada local del sistema IPQoS.
	LOCAL_OUT	Tráfico de salida local del sistema IPQoS.
	FWD_IN	Tráfico de entrada que se debe reenviar.
	FWD_OUT	Tráfico de salida que se debe reenviar.
precedence	Valor de precedencia. La precedencia más alta es 0.	La precedencia se utiliza para ordenar filtros con la misma prioridad.
ip_version	V4 o V6	Esquema de direcciones utilizado por los paquetes, IPv4 o IPv6.

Módulo Meter

El *medidor* controla la tasa de transmisión de flujos por paquete. Después, determina si el paquete cumple los parámetros configurados. El módulo medidor (Meter) determina la siguiente acción para un paquete de un conjunto de acciones, que dependen del tamaño del paquete, los parámetros configurados y la tasa de flujo.

Meter consta de dos módulos de medición, `tokenmt` y `tswtclmt`, que se configuran en el archivo de configuración IPQoS. Puede configurar uno de los módulos, o ambos, para una clase.

Al configurar un módulo de medición, puede definir dos parámetros de tasa:

- `committed-rate` – Define la tasa de transmisión aceptable, en bits por segundo, para paquetes de una clase determinada
- `peak-rate` – Define la tasa de transmisión máxima, en bits por segundo, que se permite para paquetes de una clase determinada

Una acción de medición en un paquete puede dar tres resultados:

- `green` – El paquete permite que el flujo se mantenga en la tasa aprobada.
- `yellow` – El paquete hace que el flujo sobrepase su tasa aprobada pero no la máxima.
- `red` – El paquete hace que el flujo sobrepase su tasa máxima.

Puede configurar cada resultado con acciones diferentes en el archivo de configuración IPQoS. La tasa aprobada y la tasa máxima se explican en la siguiente sección.

Módulo de medición `tokenmt`

El módulo `tokenmt` utiliza *conjuntos de tokens* para medir la tasa de transmisión de un flujo. Puede configurar `tokenmt` para que funcione como medidor de tasa única o de doble tasa. Una instancia de acción `tokenmt` mantiene dos conjuntos de tokens que determinan si el flujo de tráfico cumple los parámetros configurados.

En la página de comando `man tokenmt(7ipp)` se explica cómo utiliza IPQoS el paradigma de medidor de tokens. Puede encontrar más información general sobre conjuntos de tokens en el documento *Differentiated Services for the Internet* escrito por Kalevi Kilkki y en varias páginas web.

Los parámetros de configuración de `tokenmt` son los siguientes:

- `committed_rate` – Especifica la tasa aprobada para el flujo, en bits por segundo.
- `committed_burst` – Especifica el tamaño de ráfaga aprobado en bits. El parámetro `committed_burst` define cuántos paquetes de una clase determinada pueden transmitirse a la red a la tasa aprobada.
- `peak_rate` – Especifica la tasa máxima en bits por segundo.
- `peak_burst` – Especifica el tamaño de ráfaga máxima en bits. El parámetro `peak_burst` asigna a una clase de tráfico un tamaño de ráfaga máxima que sobrepasa la tasa aprobada.

- `color_aware` – Establece tokenmt en modo de activación.
- `color_map` – Define una matriz de enteros que asigna valores DSCP a verde, amarillo o rojo.

Configuración de tokenmt como medidor de tasa única

Para configurar tokenmt como medidor de tasa única, no especifique un parámetro `peak_rate` para tokenmt en el archivo de configuración IPQoS. Para configurar una instancia de tokenmt de tasa única para que dé un resultado rojo, verde o amarillo, debe especificar el parámetro `peak_burst`. Si no utiliza el parámetro `peak_burst`, sólo puede configurar tokenmt para que dé un resultado rojo o verde. Para ver una muestra de tokenmt de tasa única con dos resultados consulte el [Ejemplo 34-3](#).

Cuando tokenmt funciona como medidor de tasa única, el parámetro `peak_burst` es el tamaño de ráfaga de exceso. `committed_rate`, y `committed_burst` o `peak_burst` deben ser números enteros positivos (no cero).

Configuración de tokenmt como medidor de doble tasa

Para configurar tokenmt como medidor de doble tasa, especifique un parámetro `peak_rate` para la acción tokenmt en el archivo de configuración IPQoS. Un tokenmt de doble tasa siempre tiene los tres resultados: rojo, amarillo y verde. Los parámetros `committed_rate`, `committed_burst` y `peak_burst` deben ser números enteros positivos (no cero).

Configuración de tokenmt para que reconozca los colores

Para configurar un tokenmt de doble tasa para que reconozca los colores, debe añadir parámetros para agregar específicamente "reconocimiento de color". A continuación se muestra un ejemplo de instrucción de acción que configura tokenmt para que reconozca colores.

EJEMPLO 37-1 Acción tokenmt de reconocimiento de color para el archivo de configuración IPQoS

```
action {
  module tokenmt
  name meter1
  params {
    committed_rate 4000000
    peak_rate 8000000
    committed_burst 4000000
    peak_burst 8000000
    global_stats true
    red_action_name continue
    yellow_action_name continue
    green_action_name continue
    color_aware true
    color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
  }
}
```

Para activar el reconocimiento de color, hay que establecer el parámetro `color_aware` en `true`. Como medidor con reconocimiento de color, `tokenmt` asume que el paquete ya se ha marcado como rojo, amarillo o verde por una acción `tokenmt` anterior. `tokenmt` con reconocimiento de color evalúa los paquetes utilizando el punto de código DSCP del encabezado, además de los parámetros de un medidor de doble tasa.

El parámetro `color_map` contiene una matriz en la que se asigna el punto de código DSCP del encabezado del paquete. Observe la siguiente matriz `color_map`:

```
color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
```

Los paquetes con un DSCP de 0–20 y 22 se asignan al verde. Los paquetes con un DSCP de 21 y 23–42 se asignan al rojo. Los paquetes con un DSCP de 43–63 se asignan al amarillo. `tokenmt` mantiene un mapa de color predeterminado. Aunque puede cambiar los valores predeterminados utilizando los parámetros `color_map`.

En los parámetros `color_action_name`, puede especificar `continue` para completar el procesamiento del paquete. También puede añadir un argumento para enviar el paquete a una acción de marcador, por ejemplo `yellow_action_name mark22`.

Módulo de medición `tswtclmt`

El módulo de medición `tswtclmt` realiza una estimación del ancho de banda medio para una clase de tráfico utilizando un *estimador de tasa* basado en tiempo. `tswtclmt` siempre funciona como medidor con tres resultados. El estimador de tasa proporciona una estimación de la tasa de llegada del flujo. Esta tasa debe ser aproximada al ancho de banda medio del flujo de tráfico en un periodo de tiempo determinado, la *fase temporal*. El algoritmo de estimación de tasa se toma de RFC 2859, *un marcador de tres colores con fase temporal de desplazamiento*.

Para configurar `tswtclmt`, se utilizan los siguiente parámetros:

- `committed_rate` – Especifica la tasa aprobada en bits por segundo
- `peak_rate` – Especifica la tasa máxima en bits por segundo
- `window` – Define la fase temporal, en milisegundos en los cuales se mantiene el historial de ancho de banda medio

Si necesita información técnica sobre `tswtclmt`, consulte la página de comando `man tswtclmt(7ipp)`. Si necesita información general sobre formadores de tasa similares a `tswtclmt`, consulte RFC 2963, *A Rate Adaptive Shaper for Differentiated Services* (<http://www.ietf.org/rfc/rfc2963.txt?number=2963>).

Módulo marcador

IPQoS incluye dos módulos de marcador, `dscpmk` y `dlcosmk`. Esta sección contiene información sobre cómo usar ambos marcadores. Normalmente se utiliza `dscpmk`, porque `dlcosmk` sólo está disponible para sistemas IPQoS con dispositivos VLAN.

Si necesita información técnica sobre `ds cpmk`, consulte la página de comando `man ds cpmk(7ipp)`. Si necesita información técnica sobre `dl cosmk`, consulte la página de comando `man dl cosmk(7ipp)`.

Utilización del marcador `ds cpmk` para reenviar paquetes

El marcador recibe flujos de tráfico después de que el clasificador o los módulos de medición los hayan procesado. El marcador marca el tráfico con un comportamiento de reenvío. Este comportamiento de reenvío es la acción que se realizará en los flujos cuando salgan del sistema IPQoS. El comportamiento de reenvío para una clase de tráfico se define en el *comportamiento por salto (PHB)*. El PHB asigna una prioridad a una clase de tráfico, que indica los flujos de precedencia de esa clase en relación con otras clases de tráfico. Los comportamientos PHB sólo determinan los comportamientos de reenvío en la red contigua del sistema IPQoS. Si necesita más información sobre comportamientos PHB, consulte [“Comportamientos por salto” en la página 804](#).

El *reenvío de paquetes* es el proceso de enviar tráfico de una clase determinada a su siguiente destino en una red. En un host como un sistema IPQoS, un paquete se reenvía del host al flujo de red local. Para un enrutador Diffserv, un paquete se reenvía de la red local al siguiente salto del enrutador.

El marcador marca el campo DS del encabezado del paquete con un comportamiento de reenvío común, definido en el archivo de configuración IPQoS. A partir de ahí, el sistema IPQoS y los sistemas con Diffserv siguientes, reenvían el tráfico como se indica en el campo DS, hasta que cambia la marca. Para asignar un PHB, el sistema IPQoS marca un valor en el campo DS del encabezado del paquete. Este valor se denomina punto de código de servicios diferenciados (DSCP). La arquitectura Diffserv define dos tipos de comportamientos de reenvío, EF y AF, que utilizan diferentes puntos DSCP. Si necesita información general sobre DSCP, consulte [“Punto de código DS” en la página 804](#).

El sistema IPQoS lee el punto de código DSCP del flujo de tráfico y evalúa la precedencia del flujo con respecto a otros flujos de tráfico saliente. A continuación, el sistema IPQoS prioriza todos los flujos de tráfico concurrentes y envía cada flujo a la red según su prioridad.

El enrutador Diffserv recibe los flujos de tráfico saliente y lee el campo DS de los encabezados de los paquetes. El punto de código DSCP permite al enrutador priorizar y programar los flujos de tráfico concurrentes. El enrutador reenvía cada flujo según la prioridad indicada en el PHB. Tenga en cuenta que el PHB no puede aplicarse fuera del enrutador de límite de sistema de la red, a no ser que haya sistemas con Diffserv en los siguientes puntos que también reconozcan el mismo PHB.

Reenvío acelerado (EF) PHB

El *reenvío acelerado (EF)* garantiza que los paquetes con el punto de código EF recomendado, 46 (101110), reciben el mejor tratamiento posible al enviarse a la red. El reenvío acelerado puede compararse con una línea alquilada. Los paquetes con el punto de código 46 (101110)

tienen garantizado un tratamiento preferencial por todos los enrutadores Diffserv que se encuentren hasta el destino del paquete. Si necesita información técnica sobre EF, consulte RFC 2598, *Un PHB de reenvío acelerado*.

Reenvío asegurado (AF) PHB

El *reenvío asegurado* (AF) proporciona cuatro clases diferentes de comportamientos de reenvío que pueden especificarse al marcador. La siguiente tabla muestra las clases, las tres precedencias de descarte proporcionadas para cada clase y los puntos de código DSCP recomendados asociados con cada precedencia. Cada DSCP está representado por su valor AF, su valor decimal y su valor binario.

TABLA 37-2 Puntos de código de reenvío asegurado

	Clase 1	Clase 2	Clase 3	Clase 4
Precedencia con baja probabilidad de descarte	AF11 =	AF21 =	AF31 =	AF41 =
	10 (001010)	18 (010010)	26 (011010)	34 (100010)
Precedencia con probabilidad de descarte media	AF12 =	AF22 =	AF32 =	AF42 =
	12 (001100)	20 (010100)	28 (011100)	36 (100100)
Precedencia con alta probabilidad de descarte	AF13 =	AF23 =	AF33 =	AF43 =
	14 (001110)	22 (010110)	30 (011110)	38 (100110)

Cualquier sistema con Diffserv puede utilizar el punto de código AF como guía para proporcionar comportamientos de reenvío diferenciados a diferentes clases de tráfico.

Cuando estos paquetes llegan a un enrutador con Diffserv, el enrutador evalúa los puntos de código de los paquetes junto con los puntos de código DSCP de otro tráfico en cola. Después, el enrutador reenvía o descarta paquetes, según el ancho de banda disponible y las prioridades asignadas por los puntos DSCP de los paquetes. Los paquetes marcados con PHB EF tienen ancho de banda garantizado con respecto a paquetes marcados con cualquier comportamiento PHB AF.

El marcado de paquetes debe coordinarse entre cualquier sistema IPQoS de la red y el enrutador Diffserv, para garantizar que los paquetes se reenvían de manera apropiada. Por ejemplo, suponga que los sistemas IPQoS de la red marcan los paquetes con puntos de código AF21 (010010), AF13 (001110), AF43 (100110) y EF (101110). Deberá añadir los puntos de código DSCP AF21, AF13, AF43 y EF al archivo correspondiente del enrutador Diffserv.

Para obtener una explicación técnica sobre la tabla de puntos de código AF, consulte RFC 2597. En las páginas web de los fabricantes de enrutadores Cisco Systems y Juniper Networks puede encontrar información detallada acerca de la configuración de comportamientos AF PHB.

Puede usar esta información para definir comportamientos PHB AF para sistemas IPQoS y enrutadores. La documentación del fabricante del enrutador contiene instrucciones para definir puntos de código DS en el equipo.

Suministrar un DSCP al marcador

El DSCP tiene un tamaño de 6 bits. El campo DS tiene un tamaño de 1 byte. Al definir un DSCP, el marcador marca los 6 primeros bits significativos del encabezado del paquete con el punto de código DS. Los 2 bits menos significativos no se utilizan.

Para definir un DSCP, se utiliza el siguiente parámetro en una instrucción de acción de marcador:

```
dscp_map{0-63:DS_codepoint}
```

El parámetro `dscp_map` es una matriz de 64 elementos, que se rellena con el valor (DSCP). `dscp_map` se utiliza para asignar puntos DSCP entrantes a puntos DSCP salientes que aplica el marcador `ds_cpmk`.

Debe especificar el valor DSCP de `dscp_map` en notación decimal. Por ejemplo, el punto de código EF 101110 debe traducirse al valor decimal 46, que da como resultado `dscp_map{0-63:46}`. Para puntos de código AF, debe convertir los diferentes puntos de código que se muestran en la [Tabla 37-2](#) a notación decimal para usarlos con `dscp_map`.

Uso del marcador `d_lcosmk` con dispositivos VLAN

El módulo de marcador `d_lcosmk` marca un comportamiento de reenvío en el encabezado MAC de un datagrama. `d_lcosmk` sólo se puede usar en un sistema IPQoS con una interfaz VLAN.

`d_lcosmk` añade cuatro bytes, denominados *etiqueta VLAN*, al encabezado MAC. La etiqueta VLAN incluye un valor de prioridad de usuario de 3 bits, definido en el estándar IEEE 801.D. Los nodos de red con Diffserv que admitan VLAN pueden leer el campo de prioridad de usuario en un datagrama. Los valores de prioridad de usuario 801.D utilizan marcas CoS (Class of Service), que son comunes e interpretables para nodos de red comerciales.

Puede utilizar los valores de prioridad de usuario de la acción de marcador `d_lcosmk` definiendo la clase de marcas de servicio de la siguiente tabla.

TABLA 37-3 Valores de prioridad de usuario 801.D

Clase de servicio	Definición
0	Mejor posible
1	Segundo plano
2	Momentos libres

TABLA 37-3 Valores de prioridad de usuario 801.D (Continuación)

Clase de servicio	Definición
3	Excelente
4	Carga controlada
5	Vídeo, latencia de menos de 100ms
6	Vídeo, latencia de menos de 10ms
7	Control de red

Si necesita más información sobre `dlcosmk`, consulte la página de comando `man dlcosmk(7ipp)`.

Configuración IPQoS para sistemas con dispositivos VLAN

En esta sección se presenta un escenario de red simple para mostrar cómo utilizar IPQoS en sistemas con dispositivos VLAN. El escenario incluye dos sistemas IPQoS, `machine1` y `machine2`, conectados mediante un nodo. El dispositivo VLAN de `machine1` tiene la dirección IP `10.10.8.1`. El dispositivo VLAN de `machine2` tiene la dirección IP `10.10.8.3`.

El siguiente archivo de configuración IPQoS de `machine1` muestra una solución simple para marcar el tráfico a través del nodo a `machine2`.

EJEMPLO 37-2 Archivo de configuración IPQoS para un sistema con un dispositivo VLAN

```
fmt_version 1.0
action {
    module ipgpc
    name ipgpc.classify

    filter {
        name myfilter2
        daddr 10.10.8.3
        class myclass
    }

    class {
        name myclass
        next_action mark4
    }
}

action {
    name mark4
    module dlcosmk
    params {
        cos 4
        next_action continue
    }
    global_stats true
}
```


En esta configuración, todo el tráfico de `machine1` destinado para el dispositivo VLAN de `machine2` se transfiere al marcador `dlcosmk`. La acción de marcador `mark4` indica a `dlcosmk` que debe añadir una marca VLAN a datagramas de la clase `myclass` con un valor CoS de 4. El valor de prioridad de usuario de 4 indica que el conmutador que hay entre los dos equipos debe proporcionar reenvío de carga controlado a los flujos de tráfico `myclass` desde `machine1`.

Módulo `flowacct`

El módulo IPQoS `flowacct` registra información sobre flujos de tráfico, un proceso que se denomina *control de flujo*. El control de flujo genera datos que pueden utilizarse para la facturación de clientes o para evaluar la cantidad de tráfico de una clase determinada.

El control de flujo es optativo. `flowacct` es, generalmente, el último módulo que los módulos medidos o marcados encuentras antes de enviarse al flujo de red. Para ver una ilustración de la ubicación de `flowacct` en el modelo Diffserv, consulte la [Figura 32–1](#). Para ver información técnica detallada sobre `flowacct`, consulte la página de comando `man flowacct(7ipp)`.

Para activar el control de flujo, debe usar la herramienta de control de Oracle Solaris `exacct` y el comando `acctadm`, además de `flowacct`. Para ver los pasos necesarios para configurar el control de flujo, consulte la sección “[Establecimiento del control de flujo \(Mapa de tareas\)](#)” en la [página 865](#).

Parámetros de `flowacct`

El módulo `flowacct` recopila información sobre flujos en una *tabla de flujo* compuesta por *registros de flujo*. Cada entrada de la tabla contiene un registro de flujo. No se puede ver una tabla de flujo.

En el archivo de configuración IPQoS, se definen los siguientes parámetros de `flowacct` para medir los registros de flujo y escribirlos en la tabla de flujo:

- `timer` – Define un intervalo, en milisegundos, en el que los flujos con tiempo de espera superado se eliminan de la tabla de flujo y se escriben en el archivo creado por `acctadm`
- `timeout` – Define un intervalo, en milisegundos, que especifica cuánto tiempo debe estar inactivo un flujo de paquete para que se supere el tiempo de espera del flujo

Nota – Puede configurar `timer` y `timeout` para que tengan diferentes valores.

- `max_limit` – Define el límite máximo para el número de registros de flujo que pueden almacenarse en la tabla de flujo

Para ver un ejemplo de cómo se utilizan los parámetros `flowacct` en el archivo de configuración IPQoS, consulte “[Cómo configurar el control de flujo en el archivo de configuración IPQoS](#)” en la [página 851](#).

Tabla de flujo

El módulo `flowacct` mantiene una tabla de flujo que registra todos los flujos de paquetes supervisados por una instancia de `flowacct`. Un flujo se identifica mediante los siguientes parámetros, que incluyen `flowacct` 8-tuple:

- Dirección de origen
- Dirección de destino
- Puerto de origen
- Puerto de destino
- DSCP
- ID de usuario
- ID de proyecto
- Número de protocolo

Si todos los parámetros de 8-tuple de un flujo siguen siendo los mismos, la tabla de flujo contiene sólo una entrada. El parámetro `max_limit` determina el número de entradas que puede contener una tabla de flujo.

La tabla de flujo se explora en el intervalo especificado en el archivo de configuración IPQoS del parámetro `timer`. El tiempo predeterminado es 15 segundos. El tiempo de espera de un flujo se supera cuando el sistema IPQoS no envía los paquetes del flujo en el intervalo `timeout` definido en el archivo de configuración IPQoS. El intervalo de tiempo de espera predeterminado es de 60 segundos. Las entradas con tiempo de espera superado se escriben en el archivo de control creado con el comando `acctadm`.

Registros `flowacct`

Un registro `flowacct` contiene los atributos descritos en la siguiente tabla.

TABLA 37-4 Atributos de un registro `flowacct`

Nombre de atributo	Contenido de atributo	Tipo
<code>src-addr-tipo de dirección</code>	Dirección de origen del originador. El <i>tipo de dirección</i> es v4 para IPv4 o v6 para IPv6, especificado en el archivo de configuración IPQoS.	Básico
<code>dest-addr-tipo de dirección</code>	Dirección de destino de los paquetes. El <i>tipo de dirección</i> es v4 para IPv4 o v6 para IPv6, especificado en el archivo de configuración IPQoS.	Básico
<code>src-port</code>	Puerto de origen del que proviene el flujo.	Básico
<code>dest-port</code>	Número de puerto de destino al que está vinculado el flujo.	Básico
<code>protocol</code>	Número de protocolo del flujo.	Básico
<code>total-packets</code>	Número de paquetes del flujo.	Básico

TABLA 37-4 Atributos de un registro flowacct (Continuación)

Nombre de atributo	Contenido de atributo	Tipo
total-bytes	Número de bytes del flujo.	Básico
nombre de acción	Nombre de la acción flowacct que ha registrado este flujo.	Básico
creation-time	Primera vez que flowacct examina un paquete del flujo.	Sólo ampliado
last-seen	Última vez que se observó un paquete del flujo.	Sólo ampliado
diffserv-field	DSCP en los encabezados del paquete saliente del flujo.	Sólo ampliado
user	ID o nombre de usuario UNIX, obtenido de la aplicación.	Sólo ampliado
projid	ID de proyecto, obtenido de la aplicación.	Sólo ampliado

Utilización de acctadm con el módulo flowacct

El comando acctadm se utiliza para crear un archivo en el que se almacenan los registros de flujo generados por flowacct. acctadm funciona en combinación con la herramienta de contabilidad ampliada. Si necesita información técnica sobre acctadm, consulte la página de comando man [acctadm\(1M\)](#).

El módulo flowacct observa los flujos y rellena la tabla de flujo con registros. A continuación, flowacct evalúa los parámetros y atributos en el intervalo especificado por timer. Cuando un paquete no se detecta durante el tiempo definido en el valor last_seen más el valor timeout, se supera su tiempo de espera. Todas las entradas con tiempo de espera superado se eliminan de la tabla de flujo. Estas entradas se escriben en el archivo de control cada vez que pasa el intervalo de tiempo especificado en el parámetro timer.

Para invocar a acctadm para utilizarlo con el módulo flowacct, utilice la siguiente sintaxis:

```
acctadm -e file-type -f filename flow
```

acctadm -e Invoca a acctadm con la opción -e. "-e" indica que a continuación hay una lista de recursos.

tipo de archivo Especifica los atributos que se deben recopilar. tipo de archivo debe reemplazarse por basic o extended. Para ver una lista de atributos de cada tipo de archivo, consulte la [Tabla 37-4](#).

-f nombre de archivo Crea el archivo nombre de archivo que contendrá los registros de flujo.

flow Indica que acctadm debe ejecutarse con IPQoS.

Archivo de configuración IPQoS

Esta sección contiene información detallada sobre las secciones del archivo de configuración IPQoS. La directiva IPQoS activada en el inicio se almacena en el archivo `/etc/inet/ipqosinit.conf`. Aunque puede editar este archivo, el mejor método para un sistema IPQoS nuevo es crear un archivo de configuración con un nombre diferente. Las tareas necesarias para aplicar y depurar una configuración IPQoS se encuentran en el [Capítulo 34, “Creación del archivo de configuración IPQoS \(Tareas\)”](#).

La sintaxis del archivo de configuración IPQoS se muestra en el [Ejemplo 37–3](#). El ejemplo utiliza las siguientes convenciones:

- **texto con estilo de ordenador** – Información sintáctica proporcionada para explicar las secciones del archivo de configuración. El usuario no necesita escribir el texto con estilo de ordenador en ningún momento.
- **texto en negrita** – Texto literal que debe escribir en el archivo de configuración IPQoS. Por ejemplo, siempre debe empezar el archivo de configuración IPQoS con **fmt_version**.
- *texto en cursiva* – Texto variable que se reemplaza con información descriptiva sobre la configuración. Por ejemplo, *nombre de acción* o *nombre de módulo* deben reemplazarse siempre por información sobre la configuración.

EJEMPLO 37–3 Sintaxis del archivo de configuración IPQoS

```
file_format_version ::= fmt_version version

action_clause ::= action {
    name action-name
    module module-name
    params-clause | ""
    cf-clauses
}
action_name ::= string
module_name ::= ipgpc | dlcosmk | dscpmk | tswtclmt | tokenmt | flowacct

params_clause ::= params {
    parameters
    params-stats | ""
}
parameters ::= prm-name-value parameters | ""
prm_name_value ::= param-name param-value

params_stats ::= global-stats boolean

cf_clauses ::= class-clause cf-clauses |
              filter-clause cf-clauses | ""

class_clause ::= class {
    name class-name
    next_action next-action-name
    class-stats | ""
}
```

EJEMPLO 37-3 Sintaxis del archivo de configuración IPQoS (Continuación)

```
class_name ::= string
next_action_name ::= string
class_stats ::= enable_stats boolean
boolean ::= TRUE | FALSE

filter_clause ::= filter {
    name filter-name
    class class-name
    parameters
}
filter_name ::= string
```

El texto restante describe cada sección principal del archivo de configuración IPQoS.

Instrucción action

Las instrucciones `action` se utilizan para invocar a los diferentes módulos IPQoS descritos en “Arquitectura IPQoS y el modelo Diffserv” en la página 871.

Al crear el archivo de configuración IPQoS, siempre se debe empezar por el número de versión. Después, se debe añadir la siguiente instrucción `action` para invocar al clasificador:

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
}
```

A continuación de la instrucción `action` de clasificador, añada una cláusula `params` o `class`.

Utilice la siguiente sintaxis para el resto de instrucciones `action`:

```
action {
    name action-name
    module module-name
    params-clause | ""
    cf-clauses
}
```

`name` *nombre de acción*

Asigna un nombre a la acción.

`module` *nombre de módulo*

Identifica el módulo IPQoS que se debe invocar, que debe ser uno de los módulos de la [Tabla 37-5](#).

cláusula params

Pueden ser parámetros que debe procesar el clasificador, como estadísticas globales, o la siguiente acción que procesar.

cláusulas *cf*

Conjunto de cero o más cláusulas `class` o `filter`

Definiciones de módulo

La definición de módulo indica qué módulo procesará los parámetros de la instrucción `action`. El archivo de configuración IPQoS puede incluir los siguientes módulos.

TABLA 37-5 Módulos IPQoS

Nombre de módulo	Definición
<code>ipgpc</code>	Clasificador IP
<code>dscpmk</code>	Marcador que se debe utilizar para crear puntos de código DSCP en paquetes IP
<code>dlcosmk</code>	Marcador que se debe utilizar con dispositivos VLAN
<code>tokenmt</code>	Medidor de conjunto de tokens
<code>tswtclmt</code>	Medidor de fase temporal de desplazamiento
<code>flowacct</code>	Módulo de control de flujo

Cláusula `class`

Se define una cláusula `class` para cada clase de tráfico.

Utilice esta sintaxis para definir las clases restantes de la configuración IPQoS:

```
class {  
    name class-name  
    next_action next-action-name  
}
```

Para activar la recopilación de estadísticas de una clase determinada, primero debe activar las estadísticas globales en la instrucción `action ipgpc.classify`. Si necesita más información, consulte [“Instrucción `action`” en la página 885](#).

Utilice la instrucción `enable_stats TRUE` cuando quiera activar la recopilación de estadísticas de una clase. Si no necesita recopilar estadísticas de una clase, puede especificar `enable_stats FALSE`. También puede eliminar la instrucción `enable_stats`.

El tráfico de una red con IPQoS que no esté definido específicamente pertenece a la *clase predeterminada*.

Cláusula `filter`

Los *filtros* están compuestos por selectores que agrupan los flujos de tráfico en clases. Estos selectores definen específicamente los criterios que deben aplicarse al tráfico de la clase creada en la cláusula `class`. Si un paquete cumple todos los selectores del filtro de máxima prioridad, se considera un miembro de la clase del filtro. Para ver una lista completa de los selectores que pueden usarse con el clasificador `ipgpc`, consulte la [Tabla 37-1](#).

Los filtros se definen en el archivo de configuración IPQoS utilizando una *cláusula filter*, que tiene la siguiente sintaxis:

```
filter {
    name filter-name
    class class-name
    parameters (selectors)
}
```

Cláusula `params`

La cláusula `params` contiene instrucciones de procesamiento para el módulo definido en la instrucción de acción. Utilice la siguiente sintaxis para la cláusula `params`:

```
params {
    parameters
    params-stats | ""
}
```

En la cláusula `params` se utilizan parámetros aplicables al módulo.

El valor *estadísticas_ parámetros* de la cláusula `params` es `global_stats TRUE` o `global_stats FALSE`. La instrucción `global_stats TRUE` activa estadísticas de estilo UNIX para la instrucción `action` en la que se invocan las estadísticas globales. Puede ver las estadísticas con el comando `kstat`. Debe activar las estadísticas de la instrucción `action` antes de poder activar las estadísticas por clase.

Herramienta de configuración `ipqosconf`

La herramienta `ipqosconf` se utiliza para leer el archivo de configuración IPQoS y configurar los módulos IPQoS del kernel UNIX. `ipqosconf` realiza las siguientes acciones:

- Aplica el archivo de configuración a los módulos de kernel IPQoS (`ipqosconf -a nombre de archivo`)
- Indica el archivo de configuración IPQoS actual del kernel (`ipqosconf -l`)
- Asegura que la configuración IPQoS actual se lee y aplica cada vez que se reinicia el equipo (`ipqosconf -c`)

- Vacía los módulos de kernel IPQoS actuales (`ipqosconf -f`)

Si necesita información técnica, consulte la página de comando `man ipqosconf(1M)`.

Glosario

3DES	Consulte Triple-DES .
administración de claves	El modo en que puede gestionar asociaciones de seguridad (SA).
AES	Advanced Encryption Standard. Una técnica de cifrado de datos en bloques de 128 bits simétricos. En octubre del año 2000, el gobierno de Estados Unidos adoptó la variante Rijndael del algoritmo como estándar de cifrado. AES sustituye al cifrado DES como estándar gubernamental.
agente de movilidad	Puede ser un agente interno o externo.
agente externo	Enrutador o servidor de la red externa a la que accede el nodo móvil.
agente interno	Enrutador o servidor de la red principal de un nodo móvil.
agrupación de direcciones	En IP para móviles, conjunto de direcciones designadas por el administrador de red principal para que lo utilicen los nodos móviles que necesitan una dirección permanente.
anuncio de agente	En IP para móviles, mensaje que los agentes internos y externos envían para avisar de su presencia en cualquier vínculo con el que se haya conectado.
anuncio de enrutador	Proceso en el que los enrutadores anuncian su presencia junto con otros parámetros de vínculo e Internet, de manera periódica o como respuesta a un mensaje de solicitud de enrutador.
anuncio de vecinos	Respuesta a mensaje de solicitud de vecino o proceso de un nodo que envía anuncios de vecino no solicitados para anunciar un cambio de dirección de capa de vínculo.
asociación de seguridad de la movilidad	Serie de medidas de seguridad, por ejemplo un algoritmo de autenticación, entre un par de nodos, que se aplican a mensajes de protocolo IP para móviles y que los dos nodos se intercambian.
ataque smurf	Uso de paquetes de solicitud de ICMP echo dirigidos a una dirección de difusión IP o a varias direcciones de difusión desde ubicaciones remotas para crear interrupciones o congestiones graves de la red.
autoconfiguración	Proceso mediante el cual un host configura automáticamente su dirección IPv6 a partir del prefijo del sitio y la dirección MAC local.
autoconfiguración sin estado	Proceso mediante el cual un host genera sus propias direcciones IPv6 combinando su dirección MAC y un prefijo de IPv6 anunciado por un enrutador IPv6 local.

autoridad de certificación	Organización externa o empresa que ofrece confianza y que emite los certificados digitales utilizados para crear firmas digitales y pares de claves públicas-privadas. La autoridad de certificación garantiza la identidad de la persona a la que se concede el certificado exclusivo.
base de datos de directivas de seguridad (SPD)	Base de datos que determina el nivel de protección que debe aplicarse a un paquete. La SPD filtra el tráfico de IP para establecer si se debe descartar un paquete, autorizarle el paso o protegerlo con IPsec.
Blowfish	Algoritmo cifrado de bloques simétricos con una clave de tamaño variable que va de 32 a 448 bits. Bruce Schneier, su creador, afirma que Blowfish se optimiza en el caso de aplicaciones en que la clave se modifica con poca frecuencia.
CA	Consulte autoridad de certificación .
capa de vínculo	Capa inmediatamente inferior a IPv4/IPv6 .
carga útil	Los datos que se transportan en un paquete. La carga útil no incluye la información de encabezado que se necesita para que el paquete llegue a su destino.
cifrado de claves asimétricas	Sistema de cifrado en el que el emisor y el receptor de un mensaje emplean claves distintas para cifrar y descifrar dicho mensaje. Las claves asimétricas se usan para establecer un canal seguro de cifrado simétrico de claves. protocolo de Diffie-Hellman es un ejemplo de protocolo de claves asimétricas. Se contrapone a criptografía de clave simétrica .
clase	En IPQoS, grupo de flujos de datos de red que comparten características similares. Las clases se definen en el archivo de configuración de IPQoS.
conmutación por error	Proceso de conmutar la conexión del acceso a la red de una interfaz defectuosa a otra que se encuentra en buen estado. El acceso a red incluye unidifusión, multidifusión y tráfico de emisión IPv4, así como unidifusión, multidifusión y tráfico de emisión IPv6.
contabilidad de flujos	En IPQoS, proceso de recopilación y registro de información relativa a los flujos de tráfico. La contabilidad de flujos se establece definiendo los parámetros del módulo <code>flowacct</code> en el archivo de configuración de IPQoS.
cortafuegos	Cualquier programa o dispositivo que aisle la intranet o red de una organización particular de Internet, con lo cual queda protegida de intrusiones externas. Un cortafuegos puede abarcar filtrado de paquetes, servidores proxy y NAT (Network Address Translation, traducción de direcciones de red).
criptografía de clave simétrica	Sistema de cifrado en que el emisor y el receptor de un mensaje comparten una sola clave común. Esa clave común se emplea para cifrar y descifrar el mensaje. Las claves simétricas se usan para cifrar la mayor parte de las transmisiones de datos en IPsec. DES constituye un ejemplo de sistema de claves simétricas.
criptografía por clave pública	Sistema criptográfico basado en dos claves. La clave pública es de dominio general. La clave privada sólo la conoce el destinatario del mensaje. IKE proporciona claves públicas para IPsec.
datagrama	Consulte datagrama IP .
datagrama IP	Paquete de información que se transfiere por IP. Un datagrama IP contiene un encabezado y datos. En el encabezado figuran las direcciones del origen y el destino del datagrama. Otros campos del encabezado permiten identificar y volver a combinar los datos con los datagramas adjuntos en el destino.

DES	Siglas en inglés de Data Encryption Standard, estándar de cifrado de datos. Un método de cifrado de claves simétricas que se desarrolló en 1975 y que la ANSI estandarizó en 1981 como ANSI X.3.92. DES utiliza una clave de 56 bits.
descubrimiento de agente	En IP para móviles, proceso según el cual un nodo móvil determina si se ha movido, cuál es su ubicación actual, así como su dirección de auxilio en una red externa.
descubrimiento de enrutadores	Proceso de los hosts que buscan enrutadores residentes en un vínculo conectado.
descubrimiento de vecinos	Mecanismo de IP que permite a los host encontrar otros host que residen en un vínculo conectado.
detección de errores	Proceso en el que se detecta que deja de funcionar una interfaz o la ruta de una interfaz a un dispositivo de capa de Internet. IP Multipathing para redes presenta dos clases de detección de errores: detección en vínculos (predeterminada) o en sondeos (opcional).
detección de reparaciones	Proceso en el que se detecta si una tarjeta de interfaz de red o la ruta de dicha tarjeta a un dispositivo de capa 3 comienza a funcionar correctamente después de un fallo.
dirección de auxilio	Dirección temporal de un nodo móvil que sirve como punto de salida del túnel cuando el nodo móvil se conecta a una red externa.
dirección de datos	Dirección IP que puede utilizarse como origen o destino de datos. Las direcciones de datos forman parte de un grupo IPMP y se pueden usar para enviar y recibir tráfico en cualquier interfaz del grupo. Además, el conjunto de direcciones de datos de un grupo IPMP se puede utilizar continuamente siempre que funcione una interfaz en el grupo.
dirección de difusión	Direcciones de red IPv4 cuya parte principal de la dirección es de bits de todo cero (10.50.0.0) o todo uno (10.50.255.255). Un paquete que se envía a una dirección de difusión desde un equipo de la red local se distribuye a todos los equipos de dicha red.
dirección de difusión por proximidad	Dirección IPv6 que se asigna a un grupo de interfaces (en general pertenecientes a nodos distintos). El paquete que se envía a una dirección de difusión por proximidad se dirige a la interfaz <i>más próxima</i> que contenga dicha dirección. La ruta del paquete se atiene a la medición de distancia del protocolo de encaminamiento.
dirección de encaminamiento entre dominios sin clase (CIDR)	Formato de dirección IPv4 que no se basa en clases de red (clase A, B y C). Las direcciones CIDR tienen un tamaño de 32 bits. Utilizan la notación decimal con puntos IPv4 estándar, más un prefijo de red. Dicho prefijo define el número de red y la máscara de red.
dirección de multidifusión	Dirección IPv6 que identifica un grupo de interfaces de una manera determinada. Un paquete enviado a una dirección multidifusión se distribuye a todas las interfaces del grupo. La dirección de multidifusión IPv6 funciona de manera similar a la dirección de emisión IPv4.
dirección de prueba	Dirección IP en un grupo IPMP que debe usarse como dirección de origen o destino de sondas; no debe emplearse como dirección de origen o destino para tráfico de datos.

dirección de unidifusión	Dirección IPv6 que identifica una sola interfaz de un nodo compatible con IPv6. Una dirección de unidifusión se compone de prefijo de sitio, ID de subred e ID de interfaz.
dirección de uso local	Dirección de unidifusión que sólo tiene un ámbito de encaminamiento local (dentro de una subred o una red de suscriptores). Esta dirección puede tener también un ámbito de exclusividad local o global.
dirección de uso local de sitio	Designación que se usa para dirección en un solo sitio.
dirección DEPRECATED	Dirección IP que no sirve como dirección de origen de datos que están en un grupo IPMP. En general, las direcciones de prueba IPMP son del tipo DEPRECATED . Ahora bien, cualquier dirección se puede marcar como DEPRECATED para impedir que pueda utilizarse como dirección de origen.
dirección local de vínculo	En IPv6, designación que se usa para asignar una dirección a un solo vínculo para, por ejemplo, la configuración automática de direcciones. De forma predeterminada, la dirección local de vínculo se crea a partir de la dirección MAC del sistema.
dirección permanente	Dirección IP que se asigna a un nodo móvil durante un periodo de tiempo prolongado. La dirección permanece inalterable en tanto el nodo se conecta con cualquier otra ubicación de Internet o la red de una organización.
dirección privada	Dirección IP que no se puede encaminar por Internet. Las redes internas utilizan las direcciones privadas en los host que no necesitan conexión con Internet. Las direcciones están definidas en Address Allocation for Private Internets (http://www.ietf.org/rfc/rfc1918.txt?number=1918) y con frecuencia se las denomina direcciones “1918”.
dispositivo LAN virtual (VLAN)	Interfaces de red que proporcionan reenvío de tráfico en el nivel de Ethernet (vínculo de datos) del protocolo de pila IP.
dominio de interpretación	El dominio de interpretación define los formatos de los datos, los tipos de intercambio de tráfico de red y las convenciones de denominación de información relacionada con la seguridad. Ejemplos de información relacionada con la seguridad son los algoritmos y modos criptográficos, y las directrices de seguridad.
DSA	Siglas en inglés de Digital Signature Algorithm, algoritmo de firma digital. Algoritmo de clave pública con un tamaño de clave variable que va de 512 a 4096 bits. DSS, el estándar del gobierno de Estados Unidos, llega hasta los 1024 bits. DSA se basa en el algoritmo SHA-1 para las entradas.
encabezado	Consulte encabezado IP .
encabezado de autenticación	Encabezado de extensión que proporciona autenticación e integridad, sin confidencialidad, a datagramas IP.
encabezado de paquete	Consulte encabezado IP .
encabezado IP	Veinte bytes de datos que identifican un paquete de Internet de forma exclusiva. El encabezado contiene direcciones de origen y destino del paquete. Una opción del encabezado permite agregar más bytes.
encapsulado	Proceso de colocación de un encabezado y carga útil en el primer paquete, que posteriormente se coloca en la carga útil del segundo paquete.

encapsulado mínimo	Forma opcional de túnel de IPv4 en IPv4 válida para agentes internos, externos y nodos móviles. El encapsulado mínimo presenta 8 o 12 bytes menos de estructura general que IP en encapsulado IP.
Encapsulating Security Payload (ESP)	Encabezado de extensión que proporciona integridad y confidencialidad a los datagramas. ESP es uno de los cinco componentes de la arquitectura para seguridad IP (IPsec).
enlace de movilidad	Asociación entre una dirección permanente y una de auxilio, junto con la vida útil que tenga dicha asociación.
enrutador	Sistema que en general tiene más de una interfaz, ejecuta protocolos de encaminamiento y reenvía paquetes. Un sistema se puede configurar con una sola interfaz como enrutador si el sistema es el punto final de un vínculo PPP.
expansión de carga	Proceso de distribuir tráfico de entrada o salida en un conjunto de interfaces. Como consecuencia de la expansión de carga, se obtiene un mayor rendimiento. La expansión de carga sólo se produce cuando el tráfico de red fluye hacia varios destinos que utilizan múltiples conexiones. Hay dos clases de expansión de carga: expansión de carga de entrada, para tráfico de entrada, y de salida, para tráfico de salida.
filtro	Conjunto de reglas que establecen las características de una clase en el archivo de configuración de IPQoS. El sistema IPQoS selecciona para procesar cualquier flujo de tráfico de datos que se adecue a los filtros de su archivo de configuración de IPQoS. Consulte filtro de paquetes .
filtro de paquetes	Función de cortafuegos que se puede configurar para permitir o denegar el paso de determinados paquetes a través de un cortafuegos.
filtro de paquetes con estado	Un filtro de paquetes que puede supervisar el estado de las conexiones activas y recurrir a la información obtenida para establecer los paquetes de red que podrán pasar a través del cortafuegos . Al efectuar el seguimiento y relacionar solicitudes y respuestas, un filtro de paquetes con estado puede detectar respuestas que no coincidan con una consulta.
filtro de paquetes dinámico	Consulte filtro de paquetes con estado .
firma digital	Código digital que se vincula con un mensaje transmitido electrónicamente y que identifica al remitente de forma exclusiva.
Generic Routing Encapsulation (GRE)	Forma opcional de túnel válida para agentes internos, externos y nodos móviles. GRE permite encapsular un paquete de cualquier protocolo de capa de red en un paquete de distribución del mismo o cualquier otro protocolo de capa de red.
grupo de difusión por proximidad	Grupo de interfaces que tienen la misma dirección de dirección por proximidad IPv6. La implementación de IPv6 en Oracle Solaris no permite crear direcciones ni grupos de difusión por proximidad. Ahora bien, los nodos IPv6 de Oracle Solaris pueden enviar tráfico a grupos de difusión por proximidad.
grupo IPMP	Grupo con varias rutas IP, compuesto por una serie de interfaces de red con un conjunto de direcciones de datos que el sistema trata como intercambiables para mejorar la disponibilidad y utilización de la red. El grupo IPMP, incluidas todas sus direcciones de datos e interfaces IP subyacentes, lo representa una interfaz IPMP.

HMAC	Un método de hashing por clave para autenticar mensajes. HMAC es un algoritmo de autenticación de claves secretas. HMAC se utiliza junto a una función de hash criptográfica iterativa, como por ejemplo MD5 o SHA-1, en combinación con una clave secreta compartida. La capacidad criptográfica de HMAC depende de las propiedades de la función de hash subyacente.
host	Sistema que no reenvía paquetes. Al instalar Oracle Solaris, de forma predeterminada un sistema se convierte en host. Es decir, el sistema no puede reenviar paquetes. En general, un host tiene una interfaz física, aunque también puede constar de varias interfaces.
host multired	Sistema con más de una interfaz física y que no reenvía paquetes. Un host multired puede ejecutar protocolos de encaminamiento.
ICMP	Siglas inglesas de Internet Control Message Protocol (protocolo de mensajes de control de Internet). Se utiliza para administrar e intercambiar mensajes de control.
IKE	Siglas inglesas de Internet Key Exchange (intercambio de claves en Internet). IKE automatiza el suministro de material de claves autenticadas para las asociaciones de seguridad (SA) de IPsec.
inactividad	Interfaz física que no se emplea para transportar tráfico de datos a menos que otra interfaz física haya sufrido algún problema.
índice de parámetros de seguridad	Valor entero que indica la fila de la base de datos de asociaciones de seguridad (SDAB) que debe utilizar un destinatario para descifrar un paquete recibido.
interfaz de red virtual (VNIC)	Se trata de una pseudointerfaz que proporciona conexión de red virtual aunque no esté configurada en una interfaz de red física. Los contenedores tales como dominios xVM o zonas IP exclusivos se configuran conforme a interfaces de red virtual (VNIC) para formar una red virtual.
interfaz física	Conexión de un sistema con un vínculo. Esta conexión se suele implementar entre un controlador de dispositivo y una tarjeta de interfaz de red. Algunas tarjetas de interfaz de red pueden presentar varios puntos de conexión, por ejemplo, iGb.
IP	Consulte Protocolo de Internet (IP) , IPv4 , IPv6 .
IP en encapsulado IP	Mecanismo para colocar en túneles paquetes IP dentro de paquetes IP.
IPQoS	Función de software que permite la implementación del estándar modelo DiffServ , además de contabilidad de flujo y marcación 802.1 D para LAN virtuales. Mediante IPQoS se pueden proporcionar varios niveles de servicios de red a clientes y aplicaciones, según lo que se establezca en el archivo de configuración de IPQoS.
IPsec	Seguridad IP. Arquitectura de seguridad que proporciona protección a los datagramas IP.
IPv4	Internet Protocol version 4. IPv4 en ocasiones se denomina IP. Esta versión admite un espacio de direcciones de 32 bits.
IPv6	Internet Protocol version 6. IPv6 admite espacio de direcciones de 128 bits.

lista de revocación de certificados (CRL)	Lista de certificados de claves públicas revocados por una autoridad de certificación. Estas listas se almacenan en la base de datos de CRL que se mantiene con IKE.
MAC (Message Authentication Code)	MAC proporciona seguridad en la integridad de los datos y autentica el origen de los datos. MAC no proporciona protección contra intromisiones externas.
marcador	<ol style="list-style-type: none"> 1. Módulo de la arquitectura DiffServ e IPQoS que marca el campo DS de un paquete IP con un valor que indica la forma en que se reenvía el paquete. En la implementación de IPQoS, el módulo marker es dsccpmk. 2. Módulo de la implementación de IPQoS que marca la etiqueta de LAN virtual de un datagrama de Ethernet con un valor de prioridad de usuario. El valor de prioridad de usuario indica la forma en que los datagramas deben reenviarse en una red con dispositivos VLAN. Este módulo se denomina d\cosmk.
MD5	Una función de hash criptográfica iterativa utilizada para autenticar mensajes, incluso las firmas digitales. Rivest desarrolló esta función en 1991.
medidor	Módulo de la arquitectura DiffServ que mide la velocidad del flujo de tráfico de una determinada clase. La implementación de IPQoS presenta dos medidores, tokenmt y tswtclmt.
migración de direcciones	Proceso que traslada una dirección de una interfaz de red a otra interfaz de red. La migración de direcciones tiene lugar como proceso de recuperación de errores cuando falla una interfaz, o de recuperación si se repara una interfaz.
modelo DiffServ	Estándar de arquitectura de Internet Engineering Task Force para implementar distintas clases de servicios en redes IP. Los módulos principales son classifier (clasificador), meter (medidor), marker (marcador), scheduler (programador) y dropper (descartador). IPQoS implementa los módulos classifier, meter y marker. El modelo DiffServ se describe en RFC 2475, <i>An Architecture for Differentiated Services</i> .
MTU	Siglas en inglés de Maximum Transmission Unit, unidad de transmisión máxima. El tamaño, en octetos, que puede transmitirse por un vínculo. Por ejemplo, una red Ethernet tiene una MTU de 1500 octetos.
NAI (Network Access Identifier)	Denominación que identifica de forma exclusiva el nodo móvil con el formato usuario@dominio.
NAT	Consulte traducción de la dirección de red .
nodo	En IPv6, cualquier sistema compatible con IPv6, ya sea host o enrutador.
nodo móvil	Host o enrutador capaz de cambiar su punto de conexión de una red a otra y mantener todas las comunicaciones utilizando su dirección IP permanente.
nombre de keystore	Nombre que un administrador asigna a un área de almacenamiento o keystore, en una tarjeta de interfaz de red . El nombre de keystore también se denomina token o ID de token.
paquete	Grupo de información que se transmite como una unidad a través de líneas de comunicaciones. Contiene un encabezado IP y una carga útil .

paquete icmp echo request	Paquete que se envía a un sistema en Internet para solicitar una respuesta. Esta clase de paquetes suelen denominarse "ping".
PFS (Perfect Forward Secrecy)	<p>En PFS, la clave que se emplea para proteger la transmisión de datos no se aplica en la derivación de claves adicionales. La fuente de la clave que se usa para proteger la transmisión de datos tampoco se emplea en la derivación de claves adicionales.</p> <p>PFS sólo se aplica en el intercambio de claves autenticadas. Consulte también protocolo de Diffie-Hellman.</p>
PHB (Per-Hop Behavior, comportamiento por salto)	Prioridad que se asigna a una clase de tráfico. PHB indica la prioridad que tienen los flujos de datos de esa clase respecto a otras clases de tráfico.
pila	Consulte pila de IP .
pila de IP	TCP/IP se suele denominar "pila". Este término designa las capas (TCP, IP y en ocasiones otras) a través de las cuales se transfieren todos los datos en los extremos de cliente y servidor de un intercambio de datos.
pila de protocolos	Consulte pila de IP .
pila doble	Pila de protocolo TCP/IP con IPv4 e IPv6 en la capa de red; el resto de la pila permanece idéntico. Si al instalar Oracle Solaris se habilita IPv6, el sistema recibe la versión de pila doble de TCP/IP.
PKI	Siglas en inglés de Public Key Infrastructure, infraestructura de clave pública. Sistema de certificados digitales, autoridades de certificación y otras autoridades de registro que verifican y autentican la validez de cada parte que interviene en una transacción por Internet.
prioridad de usuario	Valor de 3 bits que implementa marcas de CoS (Class-of-Service, clase de servicio), que definen la forma en que los datagramas de Ethernet se reenvían en una red de dispositivos VLAN.
protocolo de Diffie-Hellman	También se lo denomina "criptografía de claves públicas". Se trata de un protocolo de claves criptográficas asimétricas que desarrollaron Diffie y Hellman en 1976. Este protocolo permite a dos usuarios intercambiar una clave secreta mediante un medio no seguro, sin ningún otro secreto. El protocolo IKE utiliza el de Diffie-Hellman.
Protocolo de Internet (IP)	Método o protocolo con el cual se envían datos de un sistema a otro por Internet.
punto de código DS	Valor de 6 bits que, al incluirse en el campo DS o un encabezado IP, indica la manera en que se reenvía un paquete.
reconfiguración dinámica (DR)	Función que permite volver a configurar un sistema aunque esté ejecutándose, sin apenas afectar o sin afectar en absoluto a los procesos que estén en curso. No todas las plataformas de Sun admiten DR. Es posible que algunas plataformas de Sun sólo admitan DR de determinados tipos de hardware como NIC.
recuperación tras los errores	Proceso de recuperar la conexión del acceso a la red de una interfaz cuya reparación se ha detectado.

red externa	Cualquier otra red que no sea la red principal del nodo móvil.
red principal	Red cuyo prefijo coincide con el prefijo de red de una dirección permanente de nodo móvil.
red privada virtual (VPN)	Una sola red lógica y segura que emplea túneles en una red pública como Internet.
red virtual	Se trata de una combinación de recursos de red de software y hardware y de funciones que se administran de manera conjunta como una única entidad de software. Una red virtual <i>interna</i> consolida los recursos de red en un único sistema, el cual en ocasiones se denomina “red en una caja”.
redireccionar	En un enrutador, proceso para informar a un host sobre un primer salto más apropiado para llegar a un determinado destino.
registro	Proceso según el cual un nodo móvil registra su dirección de auxilio con su agente interno y agente externo cuando no se encuentra en su ubicación permanente.
repetición de ataque	En IPsec, ataque en el cual un intruso se apropia de un paquete. El paquete almacenado sustituye o repite el original posteriormente. Para protegerse contra tales ataques, un paquete puede contener un campo que se incrementa durante la vida útil de la clave secreta que protege el paquete.
resultado	Acción que se realiza como consecuencia de la medición del tráfico. Los medidores de IPQoS tienen tres resultados, rojo, amarillo y verde, que se definen en el archivo de configuración de IPQoS.
RSA	Método para la obtención de firmas digitales y criptosistemas de claves públicas. Dicho método lo describieron sus creadores, Rivest, Shamir y Adleman, en 1978.
SA	Consulte SA (Security Association) .
SA (Security Association)	Asociación que establece las propiedades de seguridad entre un primer host y un segundo.
SADB	Siglas en inglés de Security Associations Database, base de datos de asociaciones de seguridad. Tabla en la que se especifican claves y algoritmos criptográficos. Las claves y los algoritmos se utilizan en la transmisión segura de datos.
salto	Medida que se usa para identificar la cantidad de enrutadores que hay entre dos hosts o sistemas. Si un origen y un destino están separados por tres enrutadores, los sistemas están a una distancia de cuatro saltos.
SCTP	Consulte protocolo SCTP (Streams Control Transport Protocol).
SCTP	Siglas en inglés de Stream Control Transport Protocol, protocolo de transporte de control del flujo. Protocolo de capas de transporte que brinda comunicaciones relativas a las conexiones de manera parecida a TCP. Además, SCTP permite varias direcciones permanentes, en que uno de los puntos finales de la conexión puede tener más de una dirección IP.
selector	Elemento que define los criterios de aplicación en los paquetes de una determinada clase, a fin de seleccionar ese tráfico en el flujo de datos de la red. Los selectores se definen en la cláusula de filtro en el archivo de configuración de IPQoS.

servidor proxy	Servidor que se emplaza entre una aplicación cliente, por ejemplo un navegador de web, y otro servidor. Se utiliza para filtrar solicitudes, por ejemplo para impedir el acceso a determinados sitios web.
SHA-1	Siglas en inglés de Secure Hashing Algorithm, algoritmo de hash seguro. El algoritmo funciona en cualquier tamaño de entrada que sea inferior a 2^{64} para generar una síntesis del mensaje. El algoritmo SHA-1 es la entrada de DSA.
sniff	Acceso no autorizado a redes de equipos; con frecuencia se usa como parte de programas automatizados para tamizar información, por ejemplo contraseñas de texto no cifrado, de última hora.
solicitud de enrutador	Proceso de los hosts que solicitan enrutadores para la generación inmediata de anuncios de enrutador, en lugar de hacerlo la próxima vez que se hubiera programado.
solicitud de vecino	Solicitud enviada por un nodo para determinar la dirección de capa de vínculo de un vecino. Asimismo, una solicitud de vecino verifica que se pueda contactar con un vecino mediante una dirección de capa de vínculo almacenada en caché.
sondear	Acción de abrir un dispositivo asociado con un nombre de interfaz física. Al sondear una interfaz, los flujos se configuran para que el protocolo IP pueda utilizar el dispositivo. Utilice el comando <code>ifconfig</code> para sondear una interfaz durante una sesión activa del sistema.
SPD	Consulte base de datos de directivas de seguridad (SPD) .
SPI	Consulte índice de parámetros de seguridad .
spoof	Obtener acceso no autorizado a un equipo mediante el envío de un mensaje con una dirección IP indicando que el mensaje procede de un host de confianza. Para efectuar spoofing en IP, el agresor debe recurrir a una serie de técnicas para averiguar la dirección IP de un host de confianza; a continuación, debe modificar los encabezados de paquete para suplantar dicha identidad y simular que los paquetes proceden de ese host.
tabla de enlace	En IP para móviles, tabla de agentes internos que asocia una dirección permanente con una auxiliar, incluyendo la vida útil de que dispone y el tiempo que se otorga.
tarjeta de interfaz de red	Tarjeta de adaptador de red que actúa como interfaz de una red. Algunas tarjetas de interfaz de red pueden tener varias interfaces físicas, por ejemplo la tarjeta <code>igb</code> .
TCP/IP	TCP/IP (Transmission Control Protocol/Internet Protocol) es el protocolo o lenguaje de comunicaciones básico de Internet. También se usa como protocolo de comunicaciones en redes privadas (tanto intranets como extranets).
traducción de la dirección de red	También se conoce como NAT (del inglés Network Address Translation). Traducción de una dirección IP que se utiliza en una red a otra dirección IP conocida en otra red. Se utiliza para limitar la cantidad de direcciones IP globales que se necesitan.
Triple-DES	Acrónimo en inglés de Triple-Data Encryption Standard. Método de cifrado de claves simétricas. Triple-DES necesita un tamaño de clave de 168 bits. Triple-DES también se escribe 3DES.
túnel	La ruta a la que sigue un datagrama cuando se encapsula. Consulte encapsulado .
túnel bidireccional	Túnel capaz de transmitir datagramas en ambos sentidos.

túnel de reenvío	Túnel que comienza en el agente interno y termina en la dirección de auxilio del nodo móvil.
túnel inverso	Túnel que comienza en la dirección de auxilio del nodo móvil y termina en el agente interno.
valor hash	Número que se genera a partir de una cadena de texto. Las funciones hash se usan para asegurarse de que no se alteren los mensajes transmitidos. MD5 y SHA-1 son ejemplos de funciones hash de una dirección.
vínculo IP	Infraestructura o medio de comunicación que permite a los nodos comunicarse en la capa de vínculo. La capa de vínculo es la inmediatamente inferior a IPv4/IPv6. Ejemplos son las redes Ethernet (simple o con puente) o ATM. Se asignan uno o más números o prefijos de subred IPv4 a un vínculo IP. No se puede asignar el mismo número o prefijo de subred a más de un vínculo IP. En ATM LANE, un vínculo IP es una sola LAN emulada. Al utilizar ARP, el ámbito del protocolo ARP es un solo vínculo IP.

Índice

Números y símbolos

- * (asterisco), comodín en base de datos
 - bootparams, 250
- indicador de comandos >t, modo de comando
 - ipseckey, 521

A

- opción -A
 - comando ikecert, 634
 - comando ikecert certlocal, 597
- acceso http a CRL, palabra clave use_http, 613
- acctadm comando, para el control de flujo, 867
- acelerar
 - cálculos IKE, 580, 622
- activar
 - daemons de configuración de red, 107
 - red habilitada para IPv6, 177–178
- activar filtro IP, en versiones anteriores de Solaris, 660–662
- actualizar, claves previamente compartidas (IKE), 588–589
- acuerdo de nivel de servicio (SLA), 796
 - clases de servicio, 799
 - facturación a clientes, según el control de flujo, 866
 - proporcionar diferentes clases de servicio, 798
- administración de claves
 - automática, 576
 - IKE, 576
 - IPsec, 494–495
 - manual, 571–573
 - administración de claves (*Continuación*)
 - servicio de manual-key, 495
 - servicio ike, 495
 - zonas y, 511
- administración de la red, diseñar la red, 55
- administración de red
 - nombres de host, 64
 - Protocolo simple de administración de red (SNMP), 44
- administración de redes, números de red, 56
- administración del tráfico
 - control del flujo, 800
 - planificar distribuciones de red, 811
 - priorizar los flujos de tráfico, 798
 - reenvío del tráfico, 804, 805, 806
 - regulación del ancho de banda, 797
- Administrador de DHCP
 - descripción, 309
 - detener, 349
 - funciones, 330
 - iniciar, 348
 - menús, 348
 - ventana y fichas, 346
- admisión de ATM, IPv6, en, 298
- agente de movilidad, 700, 708
 - anuncios de enrutador, 730
 - archivo mipagent_state, 744
 - configurar, 743
 - estado, 744
 - sección Address, 740
 - software, 729
- agente de reenvío BOOTP, saltos, 364

- agente de reenvío de BOOTP
 - configurar
 - con dhcpconfig -R, 343
 - con el Administrador de DHCP, 338
- agente externo
 - admisión de asociación de seguridad, 707
 - autenticación, 721
 - autenticación de mensajes, 740
 - compatibilidad con encapsulado, 709
 - consideraciones, 708
 - datagramas, 697
 - definición, 698
 - determinar funcionalidad, 714
 - dirección de auxilio, 702, 705, 709
 - funcionar sin, 702
 - implementación, 729
 - lista de visitantes, 725, 744
 - mensaje de registro, 700
 - registrar mediante uso, 705
 - registrarse con varios, 705
 - registrarse mediante, 705
 - servir a nodos móviles, 701
 - solicitar servicio de, 708
 - transmitir solicitud de registro, 707
- agente interno
 - admisión de asociación de seguridad, 707
 - anular registro, 705
 - asignaciones de direcciones dinámicas, 737
 - autenticación, 721
 - consideraciones, 708
 - descubrimiento dinámico, 709
 - determinar funcionalidad, 714
 - encapsulado, 709
 - entrega de datagrama, 697
 - información de estado, 744
 - mensaje de registro, 700, 705
 - protección de repetición de mensajes, 737
 - reenviar datagramas, 710
 - respuesta de registro, 708
 - sección Address, 739, 740
 - solicitud de registro, 707, 708
 - tabla de enlace, 725, 727, 744
 - ubicación de nodos móviles, 700
- agregaciones
 - configuraciones
 - con nodo, 161
 - de extremo a extremo, 162
 - crear, 164–166
 - definición, 160
 - directiva de equilibrio de la carga, 163
 - distribuciones
 - básicas, 161
 - eliminar interfaces, 167–168
 - funciones, 160
 - modificar, 166–167
 - requisitos, 164
- agregaciones de vínculos, *Ver* agregaciones
- agregar
 - certificados autofirmados (IKE), 597
 - certificados de autoridad de certificación (IKE), 602–608
 - certificados de clave pública (IKE), 602–608
 - claves manualmente (IPsec), 520–525
 - claves previamente compartidas (IKE), 591–594
 - SA IPsec, 513, 520–525
- agrupaciones de direcciones
 - anexar, 677–678
 - configurar, 647–649
 - descripción general, 647–649
 - eliminar, 677
 - ver, 676–677
 - ver estadísticas, 681
- AH, *Ver* encabezado de autenticación (AH)
- algoritmo de autenticación DSS, 634
- algoritmo de autenticación MD5, longitud de clave, 522
- algoritmo de cifrado 3DES
 - IPsec y, 498
 - key length, 522
- algoritmo de cifrado AES, IPsec y, 498
- algoritmo de cifrado Blowfish, IPsec y, 498
- algoritmo de cifrado DES, IPsec y, 498
- algoritmo de cifrado RSA, 634
- algoritmo de cifrado Triple-DES, IPsec y, 498
- algoritmos de autenticación
 - certificados IKE, 634
 - especificar para IPsec, 573

- algoritmos de cifrado
 - especificar para IPsec, 573
 - IPsec
 - 3DES, 498
 - AES, 498
 - Blowfish, 498
 - DES, 498
- almacén de claves de softtoken, almacenamiento de claves con metaslot, 575
- almacén de claves softtoken
 - almacenamiento de claves con metarranura, 488, 633
- almacén de datos de DHCP, descripción general, 307
- almacén de datos DHCP
 - conversión, 418–421
 - exportar datos, 424
 - importar datos, 426
 - modificar datos importados, 427, 428
 - seleccionar, 323
 - transferir datos entre servidores, 421–428
- almacenamiento de claves
 - almacén de claves softtoken, 488
 - almacenamiento de claves softtoken, 624–625
 - asociaciones de seguridad de ISAKMP, 632
 - ID de señal a partir de metarranura, 624–625
 - SA de IPsec, 506
 - softtoken, 633
- almacenamiento de claves softtoken, almacenamiento de claves con metarranura, 624–625
- almacenar
 - claves IKE en disco, 604, 635
 - claves IKE en hardware, 580, 623–625
- ampliar permiso DHCP, 439
- anular registro
 - IP para móviles, 700, 705, 706
- anuncio 6to4, 194
- anuncio de agente
 - a través de interfaces dinámicas, 701
 - IP para móviles, 701
- anuncio de enrutador, 434
 - IP para móviles, 730
 - IPv6, 279, 280, 283, 285–286
 - prefijo, 280
- anuncios de agente, a través de interfaces dinámicas, 735
- archivo `/etc/bootparams`, 249
- archivo `/etc/default/dhcpagent`, 440–441
- archivo `/etc/default/dhcpagent`, descripción, 481
- archivo `/etc/default/inet_type`, 217–218
 - valor `DEFAULT_IP`, 273
- archivo `/etc/default/mpathd`, 788
- archivo `/etc/defaultdomain`
 - configuración de modo de archivos locales, 106
 - descripción, 235
 - eliminar para modo de cliente de red, 109
- archivo `/etc/defaultrouter`
 - configuración de modo de archivos locales, 106
 - descripción, 235
- archivo `/etc/dhcp/dhcpdtags`
 - convertir entradas, 482
 - descripción, 482
- archivo `/etc/dhcp/eventhook`, 449
- archivo `/etc/dhcp/inittab`
 - descripción, 482
 - modificar, 415
- Archivo `/etc/dhcp.interfaz`, 434
- archivo `/etc/dhcp.interfaz`, 440
- archivo `/etc/dhcp.interfaz`, descripción, 481
- archivo `/etc/dhcp/interfaz.dhc`, descripción, 481
- archivo `/etc/ethers`, 250
- archivo `/etc/hostname.interfaz`
 - configuración de modo de archivos locales, 105
- archivo `/etc/hostname.interfaz`
 - configuración de modo de cliente de red, 109
 - configuración manual, 149
- archivo `/etc/hostname.interfaz`
 - descripción, 234
- archivo `/etc/hostname6.interface`, colocar en túneles de IPv6, 288
- archivo `/etc/hostname6.interfaz`, sintaxis, 267–268
- archivo `/etc/hostname6.ip.6to4tun0`, 193
- archivo `/etc/hostname6.ip.tun`, 191, 192
- archivo `/etc/hosts`, Ver archivo `/etc/inet/hosts`
- archivo `/etc/inet/dhcpsvc.conf`, 335
- archivo `/etc/inet/hosts`, 512
 - agregar subredes, 102
 - archivo inicial, 237

- archivo `/etc/inet/hosts` (*Continuación*)
 - configuración de modo de archivos locales, 106
 - configuración de modo de cliente de red, 109
 - dirección en bucle, 236
 - formato, 236
- archivo `/etc/inet/hosts`, interfaces de red múltiples, 237
- archivo `/etc/inet/hosts`
 - nombre de host, 237
- archivo `/etc/inet/ike/config`
 - certificados autofirmados, 600
 - certificados de clave pública, 605, 610
 - claves previamente compartidas, 585
 - colocar certificados en hardware, 610
 - comando `ikecert`, 633
 - consideraciones de seguridad, 631
 - descripción, 578, 630
 - ejemplo, 585
- archivo `/etc/inet/ike/config`, entrada de biblioteca PKCS #11, 633
- archivo `/etc/inet/ike/config`
 - palabra clave `cert_root`, 605, 610
 - palabra clave `cert_trust`, 600, 610
 - palabra clave `ignore_crls`, 606
 - palabra clave `ldap-list`, 613
 - palabra clave `pkcs11_path`, 608, 633
 - palabra clave `proxy`, 613
 - palabra clave `use_http`, 613
 - parámetros de transmisión, 626
 - resumen, 581
- archivo `/etc/inet/ipaddrsel.conf`, 226, 268–269
- archivo `/etc/inet/ipnodes`, 239, 512
- archivo `/etc/inet/ipsecinit.conf`, 569–570
- archivo `/etc/inet/ndpd.conf`, 180, 275
 - anuncio de 6to4, 258
 - anuncio de enrutador 6to4, 194
 - configuración de direcciones temporales, 183
 - crear, 179
 - palabras clave, 264–267, 276
 - variables de configuración de interfaz, 264
 - variables de configuración de prefijo, 266
- archivo `/etc/inet/netmasks`
 - agregar subredes, 102
 - configuración de enrutador, 123
- archivo `/etc/inet/netmasks` (*Continuación*)
 - editar, 243
- archivo `/etc/inet/networks`, descripción general, 251
- archivo `/etc/inet/protocols`, 252
- archivo `/etc/inet/services`, ejemplo, 252
- archivo `/etc/ipf/ipf.conf`, Ver filtro IP
- archivo `/etc/ipf/ipnat.conf`, Ver filtro IP
- archivo `/etc/ipf/ippool.conf`, Ver filtro IP
- archivo `/etc/ipnodes` suprimido, 487–489
- archivo `/etc/netmasks`, 243
- archivo `/etc/nodename`
 - descripción, 235
 - eliminar para el modo de cliente de red, 109
- archivo `/etc/nsswitch.conf`, 247, 249
 - cambiar, 249
 - configuración de modo de cliente de red, 110
 - modificaciones, para admisión de IPv6, 296–297
 - sintaxis, 248
 - uso por DHCP, 480
- archivo `/etc/resolv.conf`, uso por DHCP, 481
- archivo `/net/if_types.h`, 770
- archivo `/var/inet/ndpd_state.interface`, 275
- archivo de configuración `mipagent.conf`, 715, 716, 730, 743
 - configurar, 714
- archivo de registro, vaciar en filtro IP, 684
- archivo de zona, 198
- archivo de zona inversa, 198
- archivo `defaultdomain`
 - configuración de modo de archivos locales, 106
 - descripción, 235
 - eliminar para modo de cliente de red, 109
- archivo `defaultrouter`
 - configuración de modo de archivos locales, 106
 - descripción, 235
 - selección de protocolo de enrutamiento automático y, 133
- archivo `dhcpcsvc.conf`, 480
- archivo `dhcptags`, 482
- archivo `/etc/hostname6.interfaz`, configurar manualmente interfaces, 172–174
- archivo `/etc/nsswitch.conf`, ejemplos, 248
- archivo `eventhook`, 449

- archivo `hostname.interfaz`
 - configuración de encaminador, 123
 - descripción, 234
- archivo `hostname6.interfaz`, configurar manualmente interfaces, 172–174
- archivo `hostname6.interfaz`, sintaxis, 267–268
- archivo `hostname6.ip.tun`, 191, 192
- archivo `hosts`, 512
- archivo `ike.preshared`, 587, 632
- archivo `Ike.preshared`, ejemplo, 593
- archivo `inet_type`, 217–218
- archivo `ipaddrsel.conf`, 226, 268–269
- archivo `ipf.conf`, 643–646
 - Ver filtro IP
- archivo `ipnat.conf`, 646–647
 - Ver filtro IP
- archivo `ipnodes`, 239, 512
- archivo `ippool.conf`, 647–649
 - Ver filtro IP
- archivo `ipsecinit.conf`
 - comprobar sintaxis, 513
 - configurar opciones de túnel, 573
 - consideraciones de seguridad, 570
 - descripción, 505
 - ejemplo, 569
 - eliminar omisión IPsec de LAN, 544, 556
 - objetivo, 499
 - omitir LAN, 538, 553
 - proteger servidor web, 516
 - ubicación y alcance, 504
- archivo `ipseckey`, almacenar claves de IPsec, 506
- archivo `mipagent_state`, 744
- archivo `mpathd`, 788–790
- archivo `ndpd.conf`
 - anuncio 6to4, 194
 - configuración de direcciones temporales, 183
 - crear, en un enrutador IPv6, 179
- archivo `ndpd.conf`
 - lista de palabras clave, 264–267
 - variables de configuración de interfaz, 264
 - variables de configuración de prefijo, 266
- archivo `nodename`
 - descripción, 235
 - eliminar para el modo de cliente de red, 109
- archivo `nsswitch.conf`, 247, 249
 - cambiar, 249
 - configuración de modo de cliente de red, 110
 - ejemplos, 248
 - modificaciones, para admisión de IPv6, 296–297
 - sintaxis, 248
- archivo `ike/config`, Ver `archivo/etc/inet/ike/config`
- archivo `ipsecinit.conf`, proteger el servidor web, 517
- archivos
 - IKE
 - archivo `ike/config`, 506, 578, 581, 630
 - archivo `ike.preshared`, 581, 632
 - directorio `crls`, 581, 636
 - directorio `ike.privatekeys`, 581, 635
 - directorio `publickeys`, 581, 635
 - IPsec
 - archivo `ipsecinit.conf`, 505, 569–570
 - archivo `ipsecinit.conf`, 505
 - archivo `ipseckey`, 506
- archivos de configuración
 - crear para filtro IP, 686–687
 - ejemplos de filtro IP, 642
- IPv6
 - archivo
 - `/etc/inet/hostname6.interfaz`, 267–268
 - archivo `/etc/inet/ipaddrsel.conf`, 268–269
 - archivo `/etc/inet/ndpd.conf`, 264, 266
 - archivo `/etc/inet/ndpd.conf`, 264–267
- redes TCP/IP
 - archivo `/etc/defaultdomain`, 235
 - archivo `/etc/defaultrouter`, 235
 - archivo `/etc/hostname.interfaz`, 234
 - archivo `/etc/nodename`, 109, 235
 - base de datos `hosts`, 235, 238
 - base de datos `netmasks`, 240
- archivos de configuración IPQoS de ejemplo
 - configuración de dispositivo VLAN, 880
 - segmento de reconocimiento de colores, 875
 - servidor de aplicaciones, 845
 - servidor web "best-effort", 833
 - servidor web de nivel alto, 832
- archivos de directiva
 - archivo `ike/config`, 506, 630
 - archivo `ipsecinit.conf`, 569–570

archivos de directiva (*Continuación*)

- archivoike/config, 581
- consideraciones de seguridad, 570

archivos de registro

- crear para filtro IP, 682–683
- ver para filtro IP, 683–684

argumento tokens, comandoikecert, 633

arquitectura de seguridad IP, Ver IPsec

asistente Network Wizard de DHCP, 369

asistente para la configuración de DHCP,

- descripción, 334

asociación de identidad, 432

asociaciones de seguridad

- generación de números aleatorios, 578
- IKE, 630
- IP para móviles, 707
- ISAKMP, 577

asociaciones de seguridad (SA)

- agregar IPsec, 513
- base de datos IPsec, 571
- crear manualmente, 520–525
- IPsec, 494–495, 513
- obtener claves para, 519–520
- reemplazar SA IPsec, 521
- vaciar SA IPsec, 521

asociaciones de seguridad del protocolo de

- administración de claves y asociaciones de seguridad de Internet (ISAKMP), ubicación de
- almacenamiento, 632

aspectos sobre la seguridad, redes habilitadas para

- IPv6, 94

asterisco (*), comodín en base de datos

- bootparams, 250

ATM, compatibilidad con IPMP para, 770

atributo deprecated, comando ifconfig, 756

autenticación de agente externo, 707

autenticación de agente externo-móvil, 707

autenticación de agente interno-móvil, 707

autenticación de mensajes

- IP para móviles, 707, 738, 740

Autoridad de números asignados de Internet (IANA),

- servicios de registro, 60

B

base de datos bootparams

- archivos del servicio de nombres
- correspondiente, 247
- descripción general, 249
- entrada comodín, 250

base de datos de asociaciones de seguridad

- (SADB), 571

base de datos de directivas de seguridad (SPD)

- configurar, 568
- IPsec, 489, 491

base de datos ethers

- archivos del servicio de nombres
- correspondiente, 246
- comprobar entradas, 230
- descripción general, 250

base de datos hosts, 235, 238

- archivo /etc/inet/hosts

- configuración de enrutador, 123
- configuración de modo de archivos locales, 106
- configuración de modo de cliente de red, 110
- dirección en bucle, 236
- formato, 236
- interfaces de red múltiples, 237
- nombre de host, 237

archivos del servicio de nombres

- correspondiente, 246

cómo afectan los servicios de nombres, 238

comprobar entradas, 230

servicio de nombres

- cómo afectan, 237
- formatos, 245

base de datos ike.privatekeys, 635

base de datos netmasks, 240

- agregar subredes, 102, 106

archivo /etc/inet/netmasks

- agregar subredes, 102
- configuración de enrutador, 123
- editar, 243

archivos del servicio de nombres

- correspondiente, 246

máscaras de red

- aplicar a dirección IPv4, 242
- crear, 241, 242

- base de datos netmasks, máscaras de red (*Continuación*)
 - descripción, 241
 - base de datos networks
 - archivos del servicio de nombres
 - correspondiente, 247
 - descripción general, 251
 - base de datos protocols
 - archivos del servicio de nombres
 - correspondiente, 247
 - descripción general, 252
 - base de datos publickeys, 635
 - base de datos services
 - actualizar, para SCTP, 138
 - archivos del servicio de nombres
 - correspondiente, 247
 - descripción general, 252
 - bases de datos
 - base de datos de asociaciones de seguridad (SADB), 571
 - base de datos de directivas de seguridad (SPD), 489
 - base de datos ike/crls, 635, 636
 - base de datos ike.privatekeys, 633, 635
 - base de datos ike/publickeys, 634
 - base de datos ike/publickeys, 635
 - IKE, 632–636
 - bases de datos de red, 244, 247
 - archivo nsswitch.conf y, 245, 247, 249
 - archivos de servicios de nombres
 - correspondientes, 246
 - base de datos bootparams, 249
 - base de datos ethers
 - comprobar entradas, 230
 - descripción general, 250
 - base de datos hosts
 - cómo afectan los servicios de nombres, 237
 - comprobar entradas, 230
 - descripción general, 235, 238
 - servicios de nombres, cómo afectan, 238
 - servicios de nombres, formatos, 245
 - base de datos netmasks, 240, 246
 - base de datos networks, 251
 - base de datos protocols, 252
 - base de datos services, 252
 - bases de datos de red (*Continuación*)
 - cómo afectan los servicios de nombres, 245, 247
 - inicio DNS y archivos de datos, 245
 - BGP, Ver protocolos de enrutamiento
 - biblioteca, PKCS #11, 634
 - biblioteca PKCS #11, en archivo ike/config, 633
 - biblioteca PKCS #11 library, especificar ruta, 634
 - borradores de Internet
 - definición, 50
 - SCTP con IPsec, 490
- ## C
- cálculos
 - acelerar IKE en hardware, 580, 622–623, 623–625
 - calidad de servicio (QoS), directiva QoS, 796
 - calidad del servicio (QoS), tareas, 793
 - cambio de dirección de capa de vínculo, 282
 - Cambio de los parámetros de transmisión de IKE (mapa de tareas), 625
 - campo CRC (comprobación de redundancia cíclica), 48
 - campos de encabezado, IPv6, 261
 - capa de aplicación
 - ciclo de vida del paquete
 - host de envío, 46
 - host de recepción, 49
 - OSI, 38
 - TCP/IP, 42, 44
 - administración de red, 44
 - comandos UNIX "r", 43
 - descripción, 39, 42
 - protocolos de enrutamiento, 44
 - servicios de archivos, 44
 - servicios de nombres, 43
 - servicios TCP/IP estándar, 42, 43
 - capa de Internet (TCP/IP)
 - ciclo de vida del paquete
 - host de envío, 47
 - host de recepción, 48
 - descripción, 39, 40
 - protocolo ARP, 41
 - protocolo ICMP, 41
 - protocolo IP, 40

- capa de presentación (OSI), 38
- capa de red (OSI), 38
- capa de red física (TCP/IP), 40, 48
- capa de red física(TCP/IP), 48
- capa de sesión (OSI), 38
- capa de transporte
 - ciclo de vida del paquete
 - host de envío, 46, 47
 - host de recepción, 49
 - encapsulado de datos, 46, 47
 - obtener estado del protocolo de transporte, 211–212
 - OSI, 38
 - TCP/IP
 - descripción, 39, 41
 - protocolo SCTP, 42, 138–141
 - protocolo TCP, 41
 - protocolo UDP, 42
- capa de vínculo de datos
 - ciclo de vida del paquete
 - host de envío, 48
 - estructura, 48
 - OSI, 39
 - TCP/IP, 39, 40
- capa del vínculo de datos
 - ciclo de vida del paquete
 - host de recepción, 48
- capa física (OSI), 39
- capas de protocolo
 - ciclo de vida del paquete, 46, 49
 - modelo de arquitectura de protocolo TCP/IP, 44
 - capa de aplicación, 39, 42, 44
 - capa de Internet, 39, 40
 - capa de red física, 39, 40
 - capa de transporte, 39, 41
 - capa de vínculo de datos, 39, 40
 - modelo de referencia OSI, 38, 39
- capas de protocolos, modelo de arquitectura del protocolo TCP/IP, 39
- características de IPv6, descubrimiento de vecinos, 82
- Carga de seguridad encapsuladora (ESP)
 - consideraciones de seguridad, 497
 - descripción, 496–497
 - proteger paquetes IP, 489
- Carga de seguridad encapsuladora(ESP), mecanismo de protección IPsec, 495–499
- certificados
 - agregar a base de datos, 604
 - almacenar
 - en hardware, 580, 622
 - IKE, 635
 - crear autofirmados (IKE), 597
 - de autoridad de certificación, 604
 - de autoridad de certificación en hardware, 611
 - descripción, 604
 - en archivo ike/config, 610
 - enumeración, 599
 - guardar
 - en equipo, 596
 - IKE, 579
 - omitir CRL, 606
 - solicitar
 - de autoridad de certificación, 603
 - en hardware, 609
- certificados de claves públicas, *Ver* certificados
- cifrado, *Ver* algoritmos de cifrado
- clases, 799
 - definir, en el archivo de configuración IPQoS, 843, 847
 - selectores, lista de, 872
 - sintaxis de la cláusula `class`, 886
- clases de red, 60
 - asignación de número de red de IANA, 60
 - clase A, 254
 - clase B, 255
 - clase C, 255
 - esquema de direcciones, 60
 - intervalo de números disponibles, 60
- clases de redes, administración de números de red, 56
- clases de servicio, *Ver* clases
- clasificador `ipgpc`, *Ver* módulo clasificador
- cláusula `class`, del archivo de configuración IPQoS, 835
- cláusula `class`, en el archivo de configuración IPQoS, 886
- cláusula `filter`, del archivo de configuración IPQoS, 837

cláusula `filter`, en el archivo de configuración
`IPQoS`, 887

cláusula `params`
 de un marcador `action`, 839
 de una acción `flowacct`, 841
 definir estadísticas globales, 835, 887
 para una instrucción `action` de medición, 852
 sintaxis, 887

claves
 administración automática, 576
 administración manual, 571–573
 administrar IPsec, 494–495
 almacenar (IKE)
 certificados, 635
 claves públicas, 635
 privadas, 633
 almacenar en hardware, 580
 base de datos `ike.privatekeys`, 635
 base de datos `ike/publickeys`, 635
 crear para SA IPsec, 520–525
 generar números aleatorios para, 519–520
 previamente compartidas (IKE), 578

claves precompartidas (IKE), ver, 589–591

claves previamente compartidas (IKE)
 almacenar, 632
 compartidas con otras plataformas, 588
 descripción, 578
 mapa de tareas, 584
 reemplazar, 588–589

claves previamente compartidas (IPsec),
 crear, 520–525

claves privadas, almacenar (IKE), 633

claves públicas, almacenar (IKE), 635

cliente DHCP
 abandonar dirección IP, 440
 administración, 439
 ampliar permiso, 439
 cerrar, 437
 configuración incorrecta, 468
 definición, 315
 desactivar, 438
 desconfigurar, 438
 ejecutar en modo de depuración
 ejemplo de salida, 462

cliente DHCP (*Continuación*)
 ejecutar programas con, 448–451

Cliente DHCP, en sistemas cliente sin disco, 416

cliente DHCP
 generación de nombre de host, 326
 habilitar, 437–438
 ID de cliente, 381
 información de opción, 415
 información de red sin permiso, 418, 439
 iniciar, 439
 inicio, 434
 interfaces lógicas, 441
 liberar dirección IP, 439
 mostrar estado de interfaz, 440
 nombre de host
 especificar, 443
 parámetros, 440–441
 probar interfaz, 440
 secuencias de eventos, 448–451
 servicios de nombres, 363
 solución de problemas, 459
 varias interfaces de red, 441

cliente DHCPv4, gestión de interfaz de red, 435

cliente DHCPv6, gestión de la interfaz de red, 436

clientes de red
 base de datos `ethers`, 250
 configuración de host, 110
 servidor de configuración de red para, 100, 107
 sistemas que funcionan como, 101

Clientes sin disco, DHCP admite, 416

comando `/usr/sbin/6to4relay`, 196

comando `/usr/sbin/ping`, 217
 descripción, 216
 ejecutar, 217
 sintaxis, 216

comando `6to4relay`, 196
 definición, 270
 ejemplos, 271
 sintaxis, 270
 tareas de configuración de túnel, 196

comando `acctadm`, para control de flujo, 801, 883

comando `dhcpcfg`
 descripción, 310, 473

comando `dhcpcmgr`, descripción, 474

- comando dhtadm
 - crear macros con, 403
- comando dhtadm, crear opciones, 409
- comando dhtadm
 - descripción, 310, 473
 - eliminar macros con, 405
 - eliminar opciones, 414
 - modificar macros con, 398
 - modificar opciones con, 412
- comando dladm
 - configurar una VLAN, 158–159
 - eliminar interfaces de una agregación, 168
 - mostrar estado, 147
 - para comprobar el estado de agregación, 165
 - para crear una agregación, 164
 - para modificar una agregación, 167
- comando gethostbyname, 296
- comando getipnodebyname, 296
- comando ifconfig, 288, 642
 - atributo deprecated, 756
 - comprobar el orden de los módulos STREAMS, 770
 - conectar una interfaz, 146
 - configurar
 - túneles de IPv6, 272–273
 - controlar cliente DHCP, 439
 - DHCP y, 474
 - extensiones 6to4, 194
 - extensiones de IPv6, 271
 - extensiones IMPM a, 750
 - formato de resultado, 205
 - información de resultado, 206
 - mostrar grupo IPMP, 781
 - opción de seguridad auth_algs, 573–574
 - opción de seguridad encr_algs, 574
 - opción de seguridad encr_auth_algs, 574
 - opción failover, 755
 - opciones de seguridad de IPsec, 573–574
 - parámetro group, 771, 784
 - parámetro standby, 757
 - parámetro test, 771
 - sintaxis, 205
 - usar como herramienta de resolución de problemas, 229
 - visualizar estado de interfaz, 205, 208, 758
- comando ikeadm
 - descripción, 630, 631–632
 - nivel de privilegio
 - comprobar, 589
 - nivel de privilegios
 - comprobar, 590
- comando ikecert
 - descripción, 630, 632
 - opción -A, 634
 - opción -a, 608
 - opción -T, 608, 634
 - opción -t, 634
- comando ikecert certdb
 - opción -a, 599, 604
- comando ikecert certlocal
 - opción -kc, 603
 - opción -ks, 597
- comando ikecert certrldb, opción -a, 614
- comando ikecert tokens, 624
- comando ipaddrsel, 226, 269–270
- comando ipf
 - Ver también* filtro IP
 - anexar reglas de línea de comandos, 671
 - opción -a, 668–670
 - opción -D, 659
 - opción -E, 655–656
 - opción -F, 657–658, 668–670, 670, 673–674
 - opción -f, 655–656, 668–670, 671, 672
 - opción -I, 672, 673–674
 - opción -s, 672–673
 - opción -6, 650–651
- comando ipfstat, 679
 - Ver también* filtro IP
 - opción -I, 668
 - opción -i, 668
 - opción -o, 668
 - opción -s, 679–680
 - opción -t, 679
 - opción -6, 650–651
- comando ipmon
 - Ver también* filtro IP
 - IPv6 y, 650–651
 - opción -a, 683–684
 - opción -F, 684

comando ipmon (*Continuación*)

opción -o, 683–684

comando ipnat

Ver también filtro IP

opción -F, 658

opción -f, 655–656

opción -C, 658

opción -F, 675

opción -f, 675–676

opción -l, 674–675

opción -s, 680–681

comando ippool

Ver también filtro IP

anexar reglas de línea de comandos, 677–678

IPv6 y, 650–651

opción -F, 677

opción -f, 677–678

opción -l, 676–677

opciones -s, 681

comando ipqosconf

aplicar una configuración, 858, 859

listado de la configuración actual, 859

opciones de comando, 887

comando ipseconf

configurar directiva IPsec, 568–569

configurar túneles, 500

consideraciones de seguridad, 515, 570

descripción, 505

objetivo, 499

opción -a, 515

opción -f, 515

visualizar directiva IPsec, 515–518, 518–519, 569–570

comando ipseckey

consideraciones de seguridad, 572–573

descripción, 506, 571–573

finalidad, 495

modo interactivo, 521

objetivo, 495

comando kstat, usado con IPQoS, 868

comando mipagentconfig

configurar agente de movilidad, 743

descripción de comandos, 743

comando mipagentconfig (*Continuación*)

modificar

archivo de configuración, 719

sección Address, 722

sección Advertisements, 720

sección General, 719

sección GlobalSecurityParameters, 721

sección Pool, 721

sección SPI, 722

comando mipagentstat

estado de agente de movilidad, 744

mostrar estado de agente, 725–727

comando ndd, ver módulo pfil, 665–666

comando netstat

descripción, 209

ejecutar comprobaciones de software, 230

extensiones de IP para móviles, 745

extensiones de IPv6, 273

opción -a, 212

opción -f, 212

opción -r, 215–216

opción inet, 212

opción inet6, 212

sintaxis, 209

visualizar estadísticas por protocolo, 209

visualizar estado de rutas conocidas, 215–216

comando nisaddcred, y DHCP, 456

comando nischmod, y DHCP, 455

comando nislsl, y DHCP, 455

comando nisstat, y DHCP, 454

comando nslookup, 297

IPv6, 200

comando od, 586

comando ping, 217

descripción, 216

ejecutar, 217

extensiones de IPv6, 274

opción -s, 216

sintaxis, 216

comando pntadm

descripción, 311, 473

ejemplos, 379

usar en secuencias, 474

comando rlogin, proceso del paquete, 46

- comando route
 - IPsec, 539, 541, 549, 550, 554, 555, 561
 - opción inet6, 274
- comando routadm
 - activar enrutamiento dinámico, 135
 - configuración de enrutador IPv6, 179
 - configurar VPN con IPsec, 556
 - hosts múltiples, 130
- comando snoop
 - comprobar flujo de paquetes, 221
 - comprobar paquetes entre servidor y cliente, 224
 - extensiones de IP para móviles, 745
 - extensiones de IPv6, 274
 - palabra clave de protocolo ip6, 274
 - supervisar tráfico de IPv6, 224–225
 - supervisar tráfico DHCP, 461–462
 - ejemplo de salida, 466
 - verificar protección de paquetes, 525–526
 - visualizar contenido de paquetes, 222
 - visualizar paquetes protegidos, 573, 574
- comando svcadm
 - actualizar IKE, 593
 - desactivar servicios de red, 537, 546, 552
 - reiniciar directiva IPsec, 593
- comando sys-unconfig
 - y cliente DHCP, 438
- comando traceroute
 - definición, 220–221
 - extensiones de IPv6, 274
 - seguimiento de rutas, 221
- comando ipnat, anexas reglas de línea de comandos, 675–676
- comandos
 - IKE, 632–636
 - comando ikeadm, 581, 630, 631–632
 - comando ikecert, 581, 630, 632
 - daemon in.iked, 630
 - IPsec
 - comando in.iked, 495
 - comando ipsecals, 498, 570–571
 - comando ipsecconf, 505, 515, 568–569
 - comando ipseckey, 506, 521, 571–573
 - comando snoop, 573, 574
 - consideraciones de seguridad, 572–573
 - comandos, IPsec (*Continuación*)
 - lista, 505–507
 - comandos "r", en UNIX, 43
 - comandos UNIX "r", 43
 - comodines en base de datos bootparams, 250
 - comportamiento por salto (PHB), 804
 - definir, en el archivo de configuración IPQoS, 853
 - reenvío AF, 805
 - reenvío EF, 805
 - utilizar, con el marcador dscpmk, 877
- comprobación de redundancia cíclica (CRC), campo, 48
- comprobar
 - archivo ipsecinit.conf
 - sintaxis, 513
 - archivos de configuración IPsec
 - sintaxis, 488
- comunicaciones de datos, 45, 49
 - ciclo de vida del paquete, 46, 49
- comunicaciones de host a host, 40
- comunicaciones inalámbricas
 - IP para móviles, 697, 702, 711
- conectar una interfaz, 146
- conectividad, informes de errores del protocolo ICMP, 41
- confidencialidad directa perfecta (PFS)
 - descripción, 577
 - IKE, 576
- configuración automática de direcciones
 - definición, 83
 - habilitar, en un nodo de IPv6, 173, 174, 176
 - IPv6, 275, 279
- configuración automática de direcciones sin estado, 280
- configuración de cliente, 430
- configuración de conmutador
 - en una topología de agregación, 161
 - protocolo de control de agregación de vínculos (LACP), 163
 - protocolo de control de agregación de vínculos (LACP) modos, 167
- configuración de enrutador 6to4
 - ejemplos, 195
 - tareas, 193

- Configuración de IKE (mapa de tareas), 583
- Configuración de IKE con certificados de clave pública (mapa de tareas), 595
- Configuración de IKE con claves previamente compartidas (mapa de tareas), 584
- Configuración de IKE para buscar el hardware conectado (mapa de tareas), 622
- Configuración de IKE para sistemas portátiles (mapa de tareas), 614
- configuración de interfaz activa-activa, IPMP, 758
- configuración de interfaz activa-reserva, IPMP, 758
- configuración de nodos, en una configuración VLAN, 156
- configuración de pseudo-interfaz 6to4, 193
- configuración de red
 - configurar
 - clientes de red, 109
 - servicios, 137
 - configurar seguridad, 485
 - enrutador, 121
 - enrutador IPv6, 178
 - instalación de servidores de configuración de red, 107
 - modos de configuración de host, 99
 - modos de configuración de TCP/IP, 101
 - información de configuración, 99
 - modo de cliente de red, 101
 - servidores de configuración de red, 100
 - modos de configuración TCP/IP
 - modo de archivos locales, 100
 - salto, descripción, 115
 - tareas de configuración de red IPv4, 104
 - topología de red IPv4, 101
- configuración de redes
 - habilitar IPv6 en un host, 181–189
 - hosts con varias direcciones permanentes habilitados para IPv6, 172–174
- configurar
 - agrupaciones de direcciones, 647–649
 - archivo ike/config, 630
 - archivo ipsecinit.conf, 569–570
 - archivos de configuración TCP/IP, 233
 - archivo /etc/defaultdomain, 235
 - archivo /etc/defaultrouter, 235
 - configurar, archivos de configuración TCP/IP (*Continuación*)
 - archivo /etc/hostname.interface, 234
 - archivo /etc/nodename, 109, 235
 - base de datos hosts, 235, 238
 - base de datos netmasks, 240
 - cliente DHCP, 429
 - enrutadores, 253
 - descripción general, 121
 - interfaces de red, 121, 123
 - enrutadores habilitados para IPv6, 178
 - IKE, 583
 - IKE con certificados autofirmados, 596–602
 - IKE con certificados de autoridad de certificación, 602–608
 - IKE con certificados de clave pública, 595, 596–602
 - IKE con certificados en hardware, 608–611
 - IKE con sistemas portátiles, 614–621
 - interfaces manualmente, para IPv6, 172–174
 - IPsec, 568–569
 - IPsec en LAN, 544, 556
 - modos de configuración de TCP/IP
 - configuraciones mixtas, 101
 - ejemplo de red, 101
 - modo de archivos locales, 99, 107
 - modo de cliente de red, 110
 - redes TCP/IP
 - archivo nsswitch.conf, 247, 249
 - archivos de configuración, 233
 - bases de datos de red, 244, 247, 249
 - clientes de red, 109
 - modos de archivos locales, 107
 - requisitos previos, 98
 - servicios TCP/IP estándar, 137
 - reglas de filtros de paquetes, 643–646
 - reglas NAT, 646–647
 - seguridad de red con un rol, 526–528
 - servicio DHCP, 333
 - servidor de configuración de red, 107
 - VPN en modo transporte con IPsec, 551–557
 - VPN en modo túnel con IPsec, 530, 535–545
 - VPN protegida con IPsec, 535–545

- conjunto de protocolo TCP/IP
 - modelo de arquitectura de protocolo TCP/IP
 - capa de Internet, 39
 - capa de red física, 39
 - capa de transporte, 39
 - capa de vínculo de datos, 39
- conjunto de protocolos TCP/IP
 - admisión de seguimiento interno, 49
 - comunicaciones de datos, 45, 49
 - encapsulado de datos, 45, 49
 - descripción general, 37, 38
 - información adicional, 49
 - FYI, 50
 - manuales, 49
 - modelo de arquitectura de protocolo TCP/IP, 44
 - capa de aplicación, 39, 42, 44
 - capa de Internet, 40
 - capa de red física, 40
 - capa de transporte, 41
 - modelo de arquitectura de TCP/IP
 - capa de vínculo de datos, 40
 - modelo de arquitectura del protocolo TCP/IP, 39
 - modelo de referencia OSI, 38, 39
 - protocolos de pila doble, 90
 - visualizar estadísticas, 209
- conjuntos de reglas
 - Ver Véase filtro IP*
 - filtros de paquetes, 643–649
 - inactivos
 - Ver también filtro IP*
 - NAT, 646–647
- conjuntos de reglas activos, *Ver filtro IP*
- conjuntos de reglas inactivos, *Ver filtro IP*
- conmutación por error
 - definición, 752
 - ejemplos, 761
 - interfaz de reserva, 758
 - reconfiguración dinámica (DR) y, 764
- consideraciones de seguridad
 - archivo ike/config, 630
 - archivo ipsecinit.conf, 570
 - archivo ipseckeys, 524
 - Carga de seguridad encapsuladora (ESP), 497
 - claves precompartidas, 579
 - consideraciones de seguridad (*Continuación*)
 - comando ipsecconf, 570
 - comando ipseckey, 572–573
 - configurar
 - IPsec, 512
 - cuestiones de enrutador de reenvío 6to4, 232
 - encabezado de autenticación (AH), 497
 - IP para móviles, 711–712
 - protocolos de seguridad, 497
 - sockets bloqueados, 570
- control de flujo, 866, 881
 - tabla de registro de flujo, 882
- control del flujo, mediante los módulos de medición, 800
- conversión de binario a decimal, 242
- conversión de decimal a binario, 242
- convertir almacén de datos DHCP, 418–421
- creación de directorio /tftpboot, 107
- crear
 - certificados autofirmados (IKE), 597
 - índice de parámetros de seguridad (SPI), 520
 - macros DHCP, 403
 - manifiesto SMF específico del sitio, 563–565
 - opciones DHCP, 409
 - rol relativo a seguridad, 526–528
 - SA IPsec, 513, 520–525
 - solicitudes de certificados, 603
- crear archivo, ipsecinit.conf, 512
- crear túneles, 698, 712
- CRL
 - acceder desde ubicación central, 612
 - base de datos ike/crls, 636
 - comando ikecert certrldb, 635
 - enumerar, 612
 - omitir, 606
- cumplimiento del tráfico
 - definir, 852
 - parámetros de tasa, 874
 - parámetros de tasas, 874
 - planificación
 - tasas en la directiva QoS, 821
 - planificar
 - resultados en la directiva QoS, 821
 - resultados, 800, 874

D

- daemon /usr/sbin/in.routed
 - descripción, 253
 - modo de ahorro de espacio, 253
- daemon /usr/sbin/inetd
 - comprobar el estado de inetd, 230
 - servicios iniciados por, 137
- daemon dhcpagent
 - archivo de parámetros, 481
 - modo de depuración, 460–461
- daemon in.dhcpd, 310
 - descripción, 474
 - modo de depuración, 461
- daemon in.iked
 - activar, 630
 - descripción, 576
 - detener e iniciar, 515, 589
 - nivel de privilegio
 - comprobar, 589
 - nivel de privilegios
 - comprobar, 590
 - opción -c, 586
 - opción -f, 586
- daemon in.mpathd
 - definición, 750–751
 - destinos de sondeo, 760
 - velocidad de sondeo, 750
- daemon in.ndpd
 - comprobar el estado, 230
 - crear un registro, 219–220
 - opciones, 275
- daemon in.rarpd, 100
- daemon in.ripngd, 179, 276
- daemon in.routed, 135
 - crear un registro, 218–219
 - descripción, 253
 - modo de ahorro de espacio, 253
- daemon in.telnet, 43
- daemon in.tftpd
 - activar, 107
 - descripción, 100
- daemon inetd
 - administrar servicios, 244
- daemon inetd, comprobar el estado, 230
- daemon inetd
 - servicios de IPv6, 276–278
 - servicios iniciados por, 137
- daemon IPMPin.mpathd, 750–751
- daemon mipagent, 715, 730, 744
- daemon rpc.bootparamd, 100
- daemons
 - daemon de enrutamiento in.routed, 135
 - daemon in.iked, 576, 580
 - daemon in.mpathd, 750–751
 - daemon in.ndpd, 275
 - daemon in.ripngd, 179, 276
 - daemon in.tftpd, 107
 - in.iked daemon, 630
 - protocolos de inicio de servidores de configuración
 - de red, 100
 - servicios de Internet inetd, 244
- datagrama encapsulado, IP para móviles, 698
- datagramas
 - encabezado IP, 48
 - formato de protocolo IP, 40
 - funciones de protocolo UDP, 42
 - IP, 489
 - proceso de paquetes, 48
- datagramas de multidifusión, IP para móviles, 710
- datagramas IP
 - encabezado IP, 48
 - formato de protocolo IP, 40
 - funciones de protocolo UDP, 42
 - proceso de paquetes, 48
 - proteger con IPsec, 489
- desactivar filtro IP, 664–665
- descubrimiento de agentes, IP para móviles, 701–702
- descubrimiento de enrutador, en IPv6, 280, 283
- descubrimiento de enrutadores, en IPv6, 83, 275
- descubrimiento de prefijos, en IPv6, 83
- deshabilitar filtro IP, 659
- destinos de sondeo, daemon in.mpathd, 754
- detección de direcciones duplicadas
 - algoritmo, 281
 - IPv6, 83
 - servicio DHCP, 364
- detección de fallos, en IPMP, 758
 - definición, 752

- detección de fallos, en IPMP (*Continuación*)
 - NIC que no estaban al iniciar el sistema, 765
 - velocidad de sondeo, 750
- detección de fallos basada en sondeos
 - configurar sistemas de destino, 775–777
- Detección de fallos basada en sondeos,
 - definición, 759–760
- detección de fallos basada en sondeos
 - destinos de sondeo, 760
 - tráfico de sondeos, IPMP, 754
- detección de fallos basada en vínculos, definición, 759
- detección de fallos basados en sondeos, tiempo de
 - detección de fallos, 760
- detección de inasequibilidad de vecinos
 - IPv6, 83, 281, 284
- detección de reparaciones, con IPMP, 752, 761
- determinación de salto siguiente, IPv6, 83
- DHCP Configuration Wizard, para agente de reenvío de BOOTP, 339
- dhcpcagent daemon, 434
- dhcpcinfo, comando, descripción, 474
- DHCPv4 y DHCPv6, 430
- DHCPv6, nombre de cliente, 431
- DHCPv6 y DHCPv4, 430
- dirección 6to4
 - dirección de host, 259
 - formato, 258
- dirección de auxilio
 - adquirir, 702
 - agente externo, 702, 705, 708
 - agentes de movilidad, 697
 - compartir, 702
 - coubicada, 700, 702, 707, 710
 - información de estado, 744
 - IP para móviles, 696
 - registro de nodos móviles, 705
 - ubicación del nodo móvil, 698
- dirección de auxilio coubicada, 700, 707, 710
 - obtener, 702
- dirección de control de acceso a medios, *Ver* dirección MAC
- dirección de difusión, 738
- dirección DHCP inutilizable, 383
- dirección en bucle, 109, 236
- dirección Ethernet, *Ver* dirección MAC
- dirección IP
 - dirección IP de origen, 709, 710
 - etiqueta BaseAddress, 738
 - nodo móvil, 698, 707
- dirección local de vínculo
 - como dirección de prueba IPMP, 755–756
 - configuración manual, con un token, 188
 - formato, 81
- dirección local de vínculo IPv6, con IPMP, 756
- dirección MAC, 431
 - asignar a IP en base de datos ethers, 250
 - comprobar exclusividad, 152–154
 - ID de interfaz de IPv6, 80
 - requisitos de IPMP, 753–754
 - utilizada en ID de cliente DHCP, 314
- dirección permanente, 696, 697, 698
- dirección temporal, en IPv6
 - configurar, 183–185
 - definición, 182–185
- direcciones
 - dirección en bucle, 236
 - direcciones de datos, IPMP, 754
 - direcciones de prueba, IPMP, 754–756
 - direcciones Ethernet
 - base de datos ethers, 246, 250
 - formato 6to4, 258
 - formato CIDR, 59
 - formato IPv4, 59
 - IPv6, formato 6to4, 193
 - locales de vínculo IPv6, 81
 - máscara de red IPv4, 241
 - mostrar direcciones de todas las interfaces, 208
 - multidifusión, en IPv6, 260–261
 - selección de direcciones predeterminadas, 225–227
 - temporales, en IPv6, 182–185
 - unidifusión global IPv6, 79–80
- direcciones de datos, IPMP, definición, 754
- direcciones de difusión por proximidad, 196
 - definición, 82
- direcciones de prueba, IPMP
 - configuración
 - IPv6, 773

direcciones de prueba, IPMP (*Continuación*)

- configurar
 - en una interfaz de reserva, 778
 - IPv4, 772
- definición, 754
- evitar uso por parte de aplicaciones, 756
- interfaz de reserva, 758
- requisitos de IPv4, 755
- requisitos de IPv6, 755–756
- tráfico de sondeos y, 754

direcciones DHCP no utilizables, 389

direcciones Ethernet, *Ver* base de datos ethers

direcciones IP

- asignación con DHCP, 325
- clases de redes
 - administración de números de red, 56
- DHCP
 - agregar, 383
 - eliminar, 389
 - errores, 457
 - inutilizables, 390
 - modificar propiedades, 387
 - propiedades, 380

Direcciones IP

- DHCP
 - reserva para cliente, 393

direcciones IP

- DHCP
 - tareas, 379
- diseñar el esquema de direcciones, 55
- diseñar un esquema de direcciones, 63
- funciones del protocolo IP, 40
- interfaces de red y, 63
- mostrar direcciones de todas las interfaces, 208
- problemas de subred, 242

direcciones IPv4

- aplicar máscaras de red, 242
- asignación de número de red de IANA, 60
- clases de red, 60
 - clase A, 254
 - clase B, 255
 - clase C, 255
- esquema de direcciones, 60
- formato, 58

direcciones IPv4 (*Continuación*)

- formato de decimales con puntos, 59
- intervalo de números disponibles, 60
- nombres simbólicos para números de red, 243
- número de subred, 61
- partes, 61
- subredes, 240

direcciones IPv6

- configuración automática de direcciones, 83
- difusión por proximidad, 82
- ejemplo de uso de VPN con IPsec, 545–551
- exclusividad, 280
- ID de interfaz, 80
- locales de vínculo, 81
- multidifusión, 81–82
- resolución de direcciones, 83
- unidifusión, 79–80

direcciones locales de sitio, IPv6, 84

direcciones locales de vínculo

- IPv6, 280, 284, 288

direcciones multidifusión, IPv6

- comparación con direcciones de emisión, 283
- descripción general, 81–82
- formato, 260–261

direcciones privadas, IP para móviles, 703–704

directiva de seguridad

- archivo (IPsec) `ipsecinit.conf`, 569–570
- archivo `ike/config` (IKE), 506
- archivo `ipsecinit.conf` (IPsec), 512
- IPsec, 499

directiva IPsec

- datagramas IP en IP, 487–489
- ejemplo de LAN, 544
- ejemplo de túneles en modo transporte, 556
- ejemplo de uso de sintaxis no admitida, 556–557
- ejemplos de sintaxis de túnel, 530–532
- especificar, 547, 559

directiva QoS, 796

- crear filtros, 818
- plantilla para organizar la directiva, 813

directivas, IPsec, 499

directivas, para agregaciones, 163

directorio `/etc/inet/ike/crls`, 636directorio `/etc/inet/ike/publickeys`, 635

- directorio /etc/inet/secret/ike.privatekeys, 635
- directorios
 - certificados (IKE), 635
 - claves previamente compartidas (IKE), 632
 - claves privadas (IKE), 633
 - claves públicas (IKE), 635
 - directorios /etc/inet/publickeys, 635
 - /etc/inet, 581
 - /etc/inet/ike, 581
 - /etc/inet/secret, 581
 - /etc/inet/secret/ike.privatekeys, 633
- diseñar la red
 - descripción general, 55
 - esquema de direcciones IP, 55, 63
 - nombres de hosts, 64
 - selección de nombre de dominio, 65
 - subredes, 240
- dispositivos de LAN virtual (VLAN) en una red IPQoS, 879
- distribuciones de red para IPQoS, 810
 - ejemplo de configuración, 826
 - Red LAN con conjuntos de servidores con IPQoS, 811
 - red LAN con cortafuegos con IPQoS, 812
 - Red LAN con hosts con IPQoS, 811
- dominios lógicos, IPsec, 504

E

- EGP, *Ver* protocolos de enrutamiento
- ejemplo de red de IPQoS, 831
- eliminar
 - opciones DHCP, 414
 - SA IPsec, 521
- encabezado de autenticación (AH)
 - consideraciones de seguridad, 497
 - mecanismo de protección IPsec, 495–499
 - proteger datagrama IP, 496
 - proteger paquetes IP, 489
- encabezado de paquetes
 - encabezado IP, 48
 - funciones de protocolo TCP, 41
- encaminador de reenvío 6to4, topología de túnel, 294

- encaminador predeterminado, ejemplo de configuración, 124
- encaminamiento estático, ejemplo de configuración de host, 134
- encapsulado de datos
 - definición, 45
 - pila de protocolo TCP/IP y, 45, 49
- enlace de movilidad, 705, 707, 708, 710
- enlaces de filtros de paquetes, 649
- enrutador con Diffserv
 - evaluación de puntos de código DS, 878
 - planificar, 815
- enrutador de límite, 119
- enrutador de límite de sistema, en ubicación 6to4, 292
- enrutador de reenvío, configuración de túnel 6to4, 196, 197
- enrutador de reenvío 6to4
 - cuestiones de seguridad, 232, 293–295
 - tareas de configuración de túnel, 196, 197
- enrutador de reenvío de paquetes, 120
- enrutador de relé de 6to4, en un túnel de 6to4, 270
- enrutador predeterminado, definición, 120
- enrutadores
 - agregar, 66, 69
 - archivo /etc/defaultrouter, 235
 - configuración de modo de archivos locales, 106
 - configurar, 253
 - interfaces de red, 123
 - IPv6, 178
 - definición, 115, 121, 253
 - dirección predeterminada, 104
 - direcciones para clientes DHCP, 325
 - enrutador de reenvío de paquetes, 120
 - enrutadores predeterminados, 120
 - enrutamiento dinámico, 135
 - enrutamiento estático, 133
 - función, en topología 6to4, 291
 - límite, 119
 - problemas al actualizar a IPv6, 231
 - protocolos de enrutamiento
 - descripción, 44, 253, 254
 - selección automática, 123
 - topología de red, 66, 67
 - transferencia de paquetes, 68, 69

- enrutamiento
 - configuración de tabla de enrutamiento, 127
 - configurar estático, 132
 - configurar manualmente una tabla de enrutamiento, 126
 - definición, 115
 - en hosts de interfaz única, 132
 - en hosts múltiples, 129
 - enrutamiento dinámico, 126
 - enrutamiento estático, 126
 - IPv6, 284
 - portal, 126
 - ruta directa, 115
 - ruta indirecta, 115
- enrutamiento de datagramas de multidifusión, IP para móviles, 710–711
- enrutamiento de datagramas de unidifusión, IP para móviles, 709–710
- enrutamiento dinámico, 135
 - configurar en un host de interfaz única, 135
 - ejemplo de configuración de host, 136
 - uso recomendado, 127
- enrutamiento estático, 133, 235
 - agregar una ruta estática, 126, 127–129
 - configurar manualmente en un host, 132
 - ejemplo de configuración, 128–129
 - uso recomendado, 127
- entrada /opt/SUNWconn/lib/libpkcs11.so, en archivo ike/config, 633
- enumeración, certificados (IPsec), 599
- enumerar
 - algoritmos (IPsec), 497, 573
 - certificados (IPsec), 612
 - CRL (IPsec), 612
 - hardware (IPsec), 624
 - ID de señal a partir de metarranura, 624–625
 - ID de símbolo (IPsec), 624
- envoltorios, TCP, 141
- envoltorios TCP, activar, 141
- equilibrio de carga, en una red habilitada para IPv6, 282
- equilibrio de la carga
 - en una red con IPQoS, 811
 - entre agregaciones, 163
 - equilibrio de la carga entrante, 282
- equipos, proteger comunicación, 511–515
- ESP, Ver Carga de seguridad encapsuladora (ESP)
- estadísticas
 - por protocolo (netstat), 209
 - transmisión de paquetes (ping), 216, 217
- estadísticas de estado, ver, 679–680
- estadísticas de IPQoS
 - activación de las estadísticas globales, 886
 - activar estadísticas basadas en clases, 886
 - activar estadísticas globales, 835
 - generar, con el comando kstat, 868
- estructura
 - capa de vínculo de datos, 40, 48
 - descripción, 48
- estructura criptográfica de Solaris, IPsec y, 570–571
- estructura del Gestor de coordinación de reconfiguración (RCM), 764–765
- /etc/hostname.archivo *interfaz*, configuración de encaminador, 123
- /etc/inet/hosts, archivo
 - archivo inicial, 236
 - interfaces de red múltiples, 237
- /etc/nsswitch.conf, archivo
 - cambiar, 248
 - plantillas de servicios de nombres, 248
- etiqueta AdvertiseOnBcast, 716, 736
- etiqueta AdvFrequency, 716, 736
- etiqueta AdvInitCount, 736
- etiqueta AdvLifetime, 716, 720, 736
- etiqueta AdvLimitUnsolicited, 736
- etiqueta BaseAddress, 717, 738
- etiqueta Challenge, 716, 737
- etiqueta ForeignAgent, 716, 724, 735
- etiqueta HA-FAauth, 716, 721, 737
- etiqueta HomeAgent, 716, 724, 735
- etiqueta Key, 717, 722, 739
- etiqueta KeyDistribution, 716, 737
- etiqueta MaxClockSkew, 716, 737
- etiqueta MN-FAauth, 716, 737
- etiqueta Pool, 718, 722, 741, 742
- etiqueta PrefixFlags, 716, 735
- etiqueta RegLifetime, 716, 736
- etiqueta ReplayMethod, 717, 739

- etiqueta ReverseTunnel, 716, 736
- etiqueta ReverseTunnelRequired, 716, 736
- etiqueta Size, 717, 738
- etiqueta SPI, 722, 740, 741, 742
- etiqueta Type, 722, 740, 741, 742
- etiqueta Version, 716, 735
- eventos DHCP, 448–451
- evitar falsificación de IP, manifiesto SMF, 563–565
- expansión de carga
 - definición, 750
 - saliente, 753

F

- fallos de grupo, IPMP, 760–761

filtro IP

- activar en versiones anteriores de Solaris, 660–662
- administrar conjuntos de reglas de filtros de paquetes, 667–674
- agrupaciones de direcciones
 - anexar, 677–678
 - eliminar, 677
 - ver, 676–677
- agrupaciones de direcciones y, 647–649
- archivo /etc/ipf/ipf.conf, 686–687
- archivo /etc/ipf/ipf6.conf, 650–651
- archivo /etc/ipf/ipnat.conf, 686–687
- archivo /etc/ipf/ippool.conf, 686–687
- archivo ipf.conf, 643–646
- archivo ipf6.conf, 650–651
- archivo ipnat.conf, 646–647
- archivo ippool.conf, 647–649
- comando ipf, 655–656
 - opción -6, 650–651
- comando ipfstat
 - opción -6, 650–651
- comando ipmon
 - IPv6 y, 650–651
- comando ipnat, 655–656
- comando ippool, 676–677
 - IPv6 y, 650–651
- conjunto de reglas
 - activar otro, 668–670

filtro IP (*Continuación*)

- conjuntos de reglas
 - activos, 668
 - alternar, 672–673
 - anexar a activos, 671
 - anexar a inactivos, 672
 - eliminar, 670
 - eliminar inactivos, 673–674
 - inactivos, 668
- conjuntos de reglas y, 643–649
- crear
 - archivos de registro, 682–683
- crear archivos de configuración, 686–687
- desactivar
 - en una NIC, 664–665
 - NAT, 658
- descripción general, 638–639
- descripción general de filtros de paquetes, 643–646
- deshabilitar, 659
- directrices para utilizar, 642
- ejemplos de archivos de configuración, 642
- eliminar
 - reglas NAT, 675
- enlaces de filtros de paquetes, 649, 654–655
- filtros en bucle de retorno, 656–657
- guardar paquetes registrados en un
 - archivo, 684–685
- IPv6, 650–651
- módulo pfil, 649–650
- NAT y, 646–647
- reglas NAT
 - anexar, 675–676
 - ver, 674–675
- rehabilitar, 655–656
- vaciado de archivo de registro, 684
- ver
 - archivos de registro, 683–684
 - estadísticas de agrupación de direcciones, 681
 - estadísticas de estado, 679–680
 - estadísticas NAT, 680–681
 - estadísticas pfil, 665–666
 - tablas de estado, 679

Filtro IP, código abierto, *Ver* Filtro IP, información de código abierto

filtro IP de Oracle Solaris, especificar una NIC, 662–664
 filtros, 800
 crear, en el archivo de configuración IPQoS, 843, 848
 planificar, en la directiva QoS, 818
 selectores, lista de, 872
 sintaxis de la cláusula *filter*, 887
 filtros de paquete, especificar una NIC, 662–664
 filtros de paquetes
 activar otro conjunto de reglas, 668–670
 administrar conjuntos de reglas, 667–674
 alternar entre conjuntos de reglas, 672–673
 anexar
 reglas a conjunto activo, 671
 reglas a conjunto inactivo, 672
 configurar, 643–646
 desactivar, 657–658
 eliminar
 conjunto de reglas activo, 670
 conjunto de reglas inactivo, 673–674
 volver a cargar tras actualizar conjunto de reglas actual, 668–670
 firmas digitales
 DSA, 634
 RSA, 634
 flujo de paquetes
 a través de túnel, 292
 enrutador de reenvío, 294
 flujo de paquetes, IPv6
 6to4 e IPv6 nativo, 294
 a través de túnel 6to4, 292
 formato de decimales con puntos, 59

G

generar, números aleatorios, 519–520
 grupos de difusión por proximidad, enrutador de reenvío 6to4, 196
 grupos IPMP
 agregar interfaces, mediante DR, 763–764
 agregar una interfaz a un grupo, 782
 configurar, 771–775

grupos IPMP (*Continuación*)
 configurar un grupo para una única interfaz, 779–781
 eliminar interfaces, mediante DR, 764
 eliminar una interfaz de un grupo, 782–783
 fallos de grupo, 760–761
 interfaces que no están presentes durante el inicio, 765
 mostrar pertenencia a un grupo, 781–782
 mover una interfaz entre grupos, 783–784
 planificar tareas, 769–771
 resolución de problemas de configuración de grupo, 775
 velocidad de NIC en un grupo, 751–752

H

hardware
 acelerar cálculos IKE, 580, 622
 almacenar claves IKE, 580, 623–625
 capa de red física (TCP/IP), 39, 40
 capa física (OSI), 39
 hardware para redes con IPQoS, 810
 host, configurar una dirección 6to4, 259
 hostname.*interfaz*, archivo, en IPMP, 778
 hosts
 comprobar conectividad de host con ping, 216
 comprobar conectividad IP, 217
 configurar para IPv6, 181–189
 de recepción
 transferencia del paquete a través de, 48
 direcciones IPv6 temporales, 182–185
 ejemplo de red, 101
 en una topología de encaminamiento IPv4, 120
 en una topología de red IPv4, 101
 envío
 transferencia de paquete a través de, 46, 48
 modos de configuración de TCP/IP, 101
 configuraciones mixtas, 101
 ejemplo de red, 101
 información de configuración, 99
 modo de archivos locales, 99
 modo de cliente de red, 101, 110
 servidores de configuración de red, 100

hosts (*Continuación*)

- modos de configuración TCP/IP
 - modo de archivos locales, 100, 107
 - modo de cliente de red, 101
 - múltiples
 - configurar, 129
 - definición, 120
 - nombre de host
 - administrar, 64
 - archivo `/etc/inet/hosts`, 237
 - recibir
 - transferencia del paquete a través de, 49
 - resolución de problemas generales, 229
 - selección del protocolo de enrutamiento, 123
- hosts**, base de datos
- archivo `/etc/inet/hosts`
 - archivo inicial, 236, 237
 - interfaces de red múltiples, 237
- hosts** base de datos
- archivo `/etc/inet/hosts`
 - agregar subredes, 102
- hosts** con varias direcciones permanentes, habilitar para IPv6, 172–174
- hosts** de envío
- transferencia de paquete a través de, 46, 48
- hosts** de recepción
- transferencia del paquete a través de, 48, 49
- hosts** múltiples
- configuración durante la instalación, 237
 - configurar, 130–132
 - definición, 120, 129
 - ejemplo de configuración, 131
 - en redes con cortafuegos, 130

I

- ID de cliente, 431
- ID de interfaz
 - definición, 80
 - formato, en una dirección IPv6, 77
 - utilizar un token configurado manualmente, 188
- ID de token, del hardware, 635
- identificador de acceso de red, IP para móviles, sección Address, 741

- identificador de acceso de red (NAI), IP para móviles, 739
- `ifconfig`
 - sondear una interfaz, 122, 149
- `ifconfig`, comando, parámetro `standby`, 778
- IGP, *Ver* protocolos de enrutamiento
- IKE
 - aceleración de hardware, 580
 - administración de claves, 576
 - administrar mediante SMF, 528–529
 - agregar certificados autofirmados, 597
 - almacenamiento de hardware de claves, 580
 - archivo `ike.preshared`, 632
 - archivos de configuración, 580–581
 - asociaciones de seguridad, 630
 - asociaciones de seguridad de ISAKMP, 577
 - base de datos `crls`, 636
 - base de datos `ike.privatekeys`, 635
 - base de datos `publickeys`, 635
 - bases de datos, 632–636
 - biblioteca PKCS #11, 634
 - buscar hardware conectado, 622
 - cambiar
 - nivel de privilegios, 590, 632
 - certificados, 579
 - claves precompartidas
 - ver, 589–591
 - claves previamente compartidas, 578
 - comando `ikeadm`, 631–632
 - comando `ikecert`, 632
 - comando `ikecert certdb`, 604
 - comando `ikecert certrldb`, 614
 - comando `ikecert tokens`, 624
 - comprobar validez de directiva, 586
 - confidencialidad directa perfecta (PFS), 576
 - configurar
 - con certificados de autoridad de certificación, 602–608
 - con certificados de clave pública, 595
 - con claves previamente compartidas, 584
 - para sistemas portátiles, 614–621
 - crear certificados autofirmados, 597
 - daemon, 630
 - daemon `in.iked`, 630

IKE (*Continuación*)

- descripción de servicios SMF, 580–581
- descripción general, 576
- descripciones de comandos, 580–581
- generar solicitudes de certificación, 603
- implementar, 583
- intercambio de fase 1, 577
- intercambio de fase 2, 578
- mediante la placa Crypto Accelerator 6000 de Sun, 623–625
- mediante una placa Crypto Accelerator de Sun, 635
- NAT y, 618–619, 620–621
- negociación de claves de fase 1, 625–627
- nivel de privilegio
 - comprobar, 589
- nivel de privilegios
 - cambiar, 590, 632
 - comprobar, 590
 - descripción, 631
- referencia, 629
- resolución de problemas de tiempo de
 - transmisión, 625–627
- RFC, 490
- servicio de SMF, 629–630
- sistemas portátiles, 614–621
- ubicaciones de almacenamiento para
 - claves, 580–581
- utilizar placa Sun Crypto Accelerator 1000, 622–623
- utilizar placa Sun Crypto Accelerator 4000, 623–625
- utilizar procesador UltraSPARC T2, 622
- utilizar una placa Crypto Accelerator de Sun, 633, 634
- ver
 - claves precompartidas, 589–591
 - zona global, 575
- indicador de recursos uniforme (URI), para acceder a
 - CRL, 612
- índice de parámetro de seguridad (SPI), IP para
 - móviles, 707
- índice de parámetros de seguridad (SPI)
 - crear, 520
 - descripción, 494–495
 - IP para móviles, 738
 - tamaño de clave, 520
- información de estado, IP para móviles, 744
- iniciar, protocolos de inicio de servidores de
 - configuración de red, 100
- instrucción *action*, 885
- interfaces
 - comprobar paquetes, 222–223
 - configuración de enrutador, 121, 123
 - configurar
 - como parte de una VLAN, 158–159
 - conectar, 146
 - direcciones temporales, 182–185
 - en agregaciones, 164–166
 - en Solaris 10 1/06, 148–151
 - interfaces lógicas de IPv6, 267–268
 - manualmente, para IPv6, 172–174
 - convenciones de denominación, 145–146
 - eliminar
 - en Solaris 10 1/06, 152
 - fallo, con IPMP, 761
 - hosts múltiples, 129, 237
 - mostrar estado, 208
 - mostrar estado, Solaris 10 1/06, 147–148
 - orden de los módulos STREAMS en una
 - interfaz, 770
 - pseudo-interfaz, para túneles 6to4, 193
 - reserva, en IPMP, 757–758
 - reserva en IPMP, 777–779
 - tipos, en Solaris 10 1/06, 146
 - tipos de interfaces heredadas, 146
 - tipos de interfaces no VLAN, 146
 - tipos de interfaz IPMP, 757–758
 - tipos de NIC, 145
 - tipos que admiten agregaciones, 164
 - verificar exclusividad de dirección MAC, 152–154
 - visualizar estado, 205, 758
 - VLANs, 154–159
- interfaces de red
 - direcciones IP y, 63
 - interfaces de red múltiples
 - archivo */etc/inet/hosts*, 237
 - mostrar estado de DHCP, 440
- interfaces de red múltiples
 - archivo */etc/inet/hosts*, 237
 - configuración de enrutador, 121, 123

- interfaces de redes, supervisar con servicio DHCP, 367
- interfaces dinámicas
 - a través de anuncio de agente, 701
 - anuncios de agente a través de, 735
- interfaces heredadas, 146
- interfaces lógicas
 - definición, 145
 - para dirección IPv6, 267–268
 - para túneles IPv6, 190, 191, 192
 - sistemas cliente DHCP, 441
- interfaces no VLAN, 146
- interfaz, definición, 145
- interfaz de red principal, 145
- interfaz de reserva
 - configurar dirección de prueba en, 778
 - configurar para un grupo IPMP, 777–779
 - definición, 757–758
- interfaz de socket PF_KEY
 - IPsec, 494, 505
- interfaz física, 160–161
 - Ver también* interfaces
 - agregar, tras la instalación, 148
 - convenciones de denominación, 145–146
 - definición, 145, 751
 - detección de fallos, 758
 - detección de reparaciones con IPMP, 761
 - eliminar, 152
 - tarjeta de interfaz de red (NIC), 145
- interfaz lógica, 432
- Internet, registro de nombre de dominio, 38
- InterNIC
 - servicios de registro
 - registro de nombre de dominio, 38
- interoperabilidad, IPsec con otras plataformas
 - utilizando claves previamente compartidas, 588
- interoperatividad, IPsec con otras plataformas en modo túnel, 488
- interredes
 - definición, 67
 - redundancia y fiabilidad, 67
 - topología, 66, 67
 - transferencia de paquetes mediante enrutadores, 68, 69
- IP address, dirección de auxilio, 702
- IP móvil
 - configurar, 714–718
 - ejemplos de archivos de configuración, 731–734
 - formato del archivo de configuración, 731
 - implementar, 713
 - mostrar estado de agente, 725–727
 - RFC admitidos, 729
 - sección Address
 - nodo móvil predeterminado, 718
- IP para móviles
 - anular registro, 700, 705, 706
 - anuncio de agente, 700, 701, 705
 - anuncio de enrutador, 730
 - archivo de configuración
 - sección Address, 738, 739–742
 - sección Advertisements, 735–736
 - sección General, 735
 - sección GlobalSecurityParameters, 736–737
 - sección Pool, 737–738
 - sección SPI, 738–739, 740
 - asociación de seguridad, 707
 - autenticación de mensajes, 707, 711
 - comunicaciones inalámbricas, 697, 702, 711
 - consideraciones de seguridad, 711–712
 - datagrama encapsulado, 698
 - datagramas de multidifusión, 710
 - descubrimiento de agentes, 701–702
 - direcciones privadas, 703–704
 - enrutamiento de datagramas de multidifusión, 710–711
 - enrutamiento de datagramas de unidifusión, 709–710
 - funcionamiento, 698–700
 - funciones no admitidas, 730
 - funciones RFC no admitidas, 730
 - identificador de acceso de red (NAIN), 739
 - índice de parámetro de seguridad (SPI), 707
 - índice de parámetros de seguridad (SPI), 738
 - información de estado, 744
 - mensaje de autenticación, 738
 - mensaje de respuesta de registro, 708
 - mensaje de solicitud de registro, 708
 - mensajes de registro, 705, 706, 707, 730
 - movimiento de datagramas, 697

IP para móviles (*Continuación*)

- registrar, 698, 700, 705
 - indicador de túnel inverso, 707
- sección Address
 - identificador de acceso de red (NAI), 741
 - nodo móvil predeterminado, 742
- secciones del archivo de configuración, 734
- solicitud de agente, 701, 702
- solicitud de agentes, 700
- solicitud de registro, 707
- tipos de encapsulado, 709
- túnel inverso, 701, 703–704
 - consideraciones del agente externo, 708
 - consideraciones del agente interno, 708
 - enrutamiento de datagramas de
 - multidifusión, 711
 - enrutamiento de datagramas de unidifusión, 710
- ip_strict_dst_multihoming, evitar falsificación de IP, 563–565

IPMP

- administrar, 781–784
- archivo de configuración IPMP, 788–790
- archivo hostname.interfaz, 778
- compatibilidad con ATM, 770
- compatibilidad con Ethernet, 770
- compatibilidad con Token ring, 770
- componentes de software, 750
- configuración de grupo
 - planificar un grupo IPMP, 769–771
 - resolución de problemas, 775
 - tareas para configurar, 771–775
- configuración de interfaz
 - activa-activa, 758
 - activa-reserva, 758
 - interfaz de reserva, 757–758, 777–779
 - tipos de configuración de interfaz, 757
- conmutación por error
 - definición, 752
- conservar configuración tras reinicio, 773, 774
- controladores de red admitidos, 759
- definición de grupo de múltiples rutas
 - Ver grupo IPMP
- descripción general, 749–753

IPMP (*Continuación*)

- detección de fallos
 - definición, 752
 - detección de fallos basada en sondeos, 759–760
 - detección de fallos basada en vínculos, 759
 - detección de reparaciones, 752
 - direcciones de datos, 754
 - direcciones de prueba, 754–756
 - expansión de carga, 750
 - mantener la configuración tras el reinicio, 778
 - reconfiguración dinámica, 753, 763–765
 - reemplazar interfaces, DR, 784–786
 - reemplazar una interfaz que no estaba presente al
 - iniciar el sistema, 786–788
 - requisitos básicos, 753–754
 - sistemas de destino, 752
 - configurar manualmente, 776
 - configurar una secuencia, 776–777
 - terminología, 751–753
 - tiempo de detección de fallos, 760
 - tráfico de sondeos, 754
 - vínculos IP, tipos, 751
- IPQoS, 793
- archivo de configuración, 831, 884
 - cláusula class, 835
 - cláusula filter, 837
 - instrucción action de marcador, 838
 - instrucción action inicial, 885
 - instrucción de acción inicial, 834
 - lista de módulos IPQoS, 886
 - sintaxis, 884
 - sintaxis de instrucción action, 885
 - compatibilidad con dispositivos VLAN, 879
 - directrices en redes habilitadas para IPv6, 92
 - distribuciones de red admitidas, 810
 - distribuciones de red compatibles, 811, 812
 - ejemplo de configuración, 826–828
 - ejemplo de red, 831
 - enrutadores en una red IPQoS, 854
 - funciones, 794
 - funciones de administración del tráfico, 797, 798
 - generación de estadísticas, 868
 - implementación del modelo Diffserv, 799
 - mensajes de error, 861

IPQoS (Continuación)

- páginas de comando man, 795
- Peticiones de comentarios relacionadas, 795
- planificar la configuración, 809
- planificar la directiva QoS, 813
- registro de mensajes, 859

ipqosconf, 831

IPsec

- activar, 505
- administración de claves, 494–495
- administrar mediante SMF, 528–529
- agregar asociaciones de seguridad (SA), 513
- algoritmos de autenticación, 498
- algoritmos de cifrado, 498
- archivo /etc/hostname.ip6.tun0
 - configurar VPN, 548, 560
- archivo /etc/hosts, 512
- archivo /etc/inet/ipnodes, 512
- archivo hostname.ip.tun0
 - configurar VPN, 553
- archivo ipsecinit.conf
 - archivo de directiva, 499
 - configurar, 512
 - descripción, 569–570
 - eliminar omisión IPsec de LAN, 544, 556
 - omitir LAN, 538, 553, 573
 - proteger el servidor web, 517
 - proteger servidor web, 516
- archivos de configuración, 505–507
- archivos de directiva, 569–570
- asegurar el registro remoto, 512
- asociaciones de seguridad (SA), 494–495
- base de datos de asociaciones de seguridad (SADB), 489, 571
- base de datos de directivas de seguridad (SPD), 489, 491, 568
- Carga de seguridad encapsuladora (ESP), 495–499
- comando de directiva
 - , 568–569
- comando ifconfig
 - configurar VPN, 540, 549
 - opciones de seguridad, 573–574
- comando ipsecals, 498, 570–571
- comando ipsecconf, 499, 568–569

IPsec (Continuación)

- comando ipseckey, 495, 571–573
- comando route, 539, 541, 549, 550, 554, 555, 561
- comando snoop, 573, 574
- comando ifconfig
 - configurar VPN, 561
- comandos, lista, 505–507
- componentes, 489
- configurar, 499, 568–569
- configurar directiva
 - permanentemente, 569–570
 - temporalmente, 568–569
- crear manualmente SA, 520–525
- daemon in.iked, 495
- datos de encapsulación, 496
- descripción general, 489
- directiva de protección, 499
- dominios lógicos, 504
- especificar
 - algoritmos de autenticación, 573
 - algoritmos de cifrado, 573
- estructura criptográfica de Solaris y, 570–571
- extensiones para utilidades
 - comando ifconfig, 573–574
 - comando snoop, 573, 574
- implementar, 509
- índice de parámetros de seguridad (SPI), 494–495
- interoperatividad con otras plataformas
 - claves previamente compartidas, 519, 588
 - túneles de IP en IP, 488
- mecanismos de protección, 495–499
- mecanismos de seguridad, 489
- modo de transporte, 499–501
- modo de túnel, 499–501
- NAT y, 503
- obtener números aleatorios para claves, 519–520
- omitir, 499, 516, 517
- origen de algoritmo, 570–571
- proceso de paquetes entrantes, 491
- proceso de paquetes salientes, 491
- proteger
 - paquetes, 489
 - servidores web, 515–518
 - sistemas portátiles, 614–621

IPsec, proteger (*Continuación*)

- VPN, 535–545
- proteger tráfico, 511–515
- proteger una VPN, 530–532, 532–565
- protocolo SCTP y, 504, 511
- protocolos de seguridad, 489, 494–495
- RBAC y, 511
- redes privadas virtuales (VPN), 502, 535–545
- reemplazar asociaciones de seguridad (SA), 521
- RFC, 490
- roles de seguridad, 526–528
- servicios
 - manual-key, 506
 - policy, 505
- servicios, lista, 505–507
- servicios de SMF, 487–489, 567–568
- terminología, 490–491
- túneles, 502
- utilidades de claves
 - comando ipseckey, 571–573
 - IKE, 576
- utilizar ssh para inicio de sesión remota seguro, 514
- verificar protección de paquetes, 525–526
- visualizar directivas, 518–519
- VPN IPv4 en modo transporte de túnel y, 551–557
- VPN IPv4 y, 535–545
- VPN IPv6 en modo de transporte de túnel, y, 557–563
- VPN IPv6 y, 545–551
- zonas y, 504
- zones y, 511

IPv6

- admisión de ATM, 298
- agregar
 - compatibilidad con DNS, 198
 - direcciones a NIS, 199
- anuncio de enrutador, 279, 280, 283, 285
- aspectos sobre la seguridad, 94
- campos de encabezado de extensión, 262
- comando nslookup, 200
- comparación con IPv4, 283–284
- comparado con IPv4, 72
- comprobar el estado de in.ndpd, 230
- configuración automática de direcciones, 275, 279

IPv6 (*Continuación*)

- configuración automática de direcciones sin estado, 280
- configuración de direcciones temporales, 182–185
- configuración de túneles, 190–191
- daemon in.ndpd, 275
- daemon in.ripngd, 276
- descripción general de protocolo, 279
- descubrimiento de enrutador, 283
- descubrimiento de enrutadores, 275
- detección de direcciones duplicadas, 83
- detección de inasequibilidad de vecinos, 83, 284
- determinación de salto siguiente, 83
- dirección 6to4, 258
- direcciones locales de sitio, 84
- direcciones locales de vínculo, 280, 284
- direcciones multidifusión, 260–261, 283
- enrutamiento, 284
- extensiones del comando ifconfig, 271
- formato de encabezado de paquetes, 261–262
- habilitar, en un servidor, 188–189
- plan de direcciones, 95–96
- preparación para admitir DNS, 92–93
- protocolo ND (Neighbor Discovery), 278–284
- protocolos de pila doble, 90
- redirección, 279, 283
- redirigir, 83
- registros AAAA de DNS, 200
- resolución de problemas IPv6 comunes, 231
- resolver problemas IPv6 comunes, 231–232
- solicitud de enrutador, 278, 280
- solicitud de vecino, 279
- solicitud e inasequibilidad de vecinos, 281
- subredes, 76
- supervisar tráfico, 224–225
- tabla de directrices de selección de direcciones
 - predeterminada, 269
- túneles, 288–290
- túneles automáticos, 287
- y filtro IP, 650–651

L

lista de visitantes

agente externo, 725

IP para móviles, 744

listas de revocación de certificados, *Ver* CRL

M

macros

DHCP

Ver macros DHCP

macros de DHCP, configuración, 381

macros DHCP

categorías, 314

crear, 403

descripción general, 313

eliminar, 405

inicio de red, 417

límite de tamaño, 315

macro de configuración regional, 335

macro de dirección de red, 314, 336

macro de servidor, 336

macros de clase de cliente, 314

macros de ID de cliente, 314

modificar, 398

orden de procesamiento, 315

predeterminadas, 327

procesamiento automático, 314

Macros DHCP, trabajar con, 395

mapa de `hosts.byaddr`, 199

mapa de `hosts.byname`, 199

mapa de `ipnodes.byaddr`, 199

mapa de `ipnodes.byname`, 199

mapa de tareas

IPQoS

planificar la configuración, 809

mapas de tareas

Cambio de los parámetros de transmisión de IKE
(mapa de tareas), 625

Configuración de IKE (mapa de tareas), 583

Configuración de IKE con certificados de clave
pública (mapa de tareas), 595

Configuración de IKE con claves previamente
compartidas (mapa de tareas), 584

mapas de tareas (*Continuación*)

Configuración de IKE para buscar el hardware
conectado (mapa de tareas), 622

Configuración de IKE para sistemas portátiles (mapa
de tareas), 614

configuración de red, 98–99

DHCP

compatibilidad con clientes BOOTP, 376

compatibilidad con clientes sólo de
información, 418

decisiones sobre la administración de direcciones
IP, 325

eliminación de clientes de inicio y sin disco con
DHCP, 417

modificar opciones de servicio DHCP, 353

preparar red para DHCP, 318

redes DHCP, 366

toma de decisiones para la configuración del
servidor DHCP, 322

transferir datos de configuración de servidores
DHCP, 422

uso de direcciones IP, 379

uso de macros DHCP, 396

uso de opciones DHCP, 407

IP móvil

configuración, 713–714

modificar una configuración, 718–719

IPMP

administración de reconfiguración dinámica
(DR), 768–769

configuración de grupos IPMP, 767–768

IPQoS

configuración de control de flujo, 865

creación de archivo de configuración, 829

planificación de directiva QoS, 814

IPv6

configuración, 177–178

configuración de túnel, 189

planificar, 87–88

Protección de una VPN con IPsec (mapa de
tareas), 532–565

Protección del tráfico con IPsec (mapa de
tareas), 509

- mapas de tareas (*Continuación*)
 - red IPv4
 - agregar subredes, 102–103
 - tareas de administración de red, 204
- marca de clase de servicio (CoS), 801
- marcador dlcsmk, 801
 - etiquetas VLAN, 879
 - planificar el reenvío de datagramas, 823
 - valores de prioridad de usuario, tabla de, 879
- marcador dscpmk, 801
 - comportamientos PHB para el reenvío de paquetes, 877
 - invocar, en una instrucción `action` de
 - marcador, 838, 844, 850, 853
 - planificar el reenvío de paquetes, 823
- marcas de tiempo, 717, 737
- mecanismos de protección, IPsec, 495–499
- medidor tokenmt, 800
 - configuración de presencia de color, 801
 - configuración de reconocimiento de colores, 875
 - medición de tasas, 874
 - medidor de doble tasa, 875
 - medidor de tasa única, 875
 - parámetros de tasas, 874
- medidor tswtclmt, 800, 876
 - medición de tasas, 876
- mensajes, anuncio de enrutador, 286
- mensajes de error de IPQoS, 861
- metarranura
 - almacenamiento de claves, 488, 624–625
- metaslot, almacenamiento de claves, 575
- modelo administrativo, 430
- modelo administrativo de DHCPv6, 431
- modelo de referencia de Interconexión de Sistemas Abiertos (OSI), 39
- modelo de referencia para redes de Interconexión de Sistemas Abiertos (OSI), 38
- modelo Diffserv
 - ejemplo de flujo, 802
 - implementación de IPQoS, 799
 - implementación IPQoS, 800, 801, 802
 - módulo clasificador, 799
 - módulos de marcador, 801
- módulo Diffserv, módulos de medidor, 800
- modificar
 - macros DHCP, 398
 - opciones DHCP, 412
- modo de ahorro de espacio, opción de daemon
 - `in.routed`, 253
- modo de archivos locales
 - configuración de host, 107
 - definición, 99
 - servidores de configuración de red, 100
 - sistemas que necesitan, 99, 100
- modo de cliente de red
 - configuración de host, 110
 - definición, 99
 - descripción general, 101
- modo de transporte
 - datos protegidos con ESP, 500
 - IPsec, 499–501
- modo de túnel, IPsec, 499–501
- modo interactivo, comando `ipseckey`, 521
- modo transporte, proteger datos con AH, 501
- modo túnel, proteger paquete IP interior
 - completo, 501
- modos de configuración de host (TCP/IP), 99, 101
 - configuraciones mixtas, 101
 - ejemplo de red, 101
 - modo de archivos locales, 99, 100
 - modo de cliente de red, 101
 - servidores de configuración de red, 100
 - topología de red IPv4, 101
- módulo clasificador, 799
 - instrucción de acción, 834
- módulo classifier, funciones de classifier, 872
- módulo flowacct, 801, 881
 - atributos de registros de flujo, 882
 - comando `acctadm`, para crear un archivo de control de flujo, 883
 - instrucción `action` de flowacct, 841
 - parámetros, 881
 - registros de flujo, 866
 - tabla de registro de flujo, 882
- módulo pfil, 649–650
 - ver estadísticas, 665–666
- módulo tun, 288

módulos de marcado

Ver también marcador dlcsmk

módulos de marcador, 801

Ver también marcador dlcsmk

Ver también marcador dscpmk

compatibilidad con dispositivos VLAN, 879

especificar un punto de código DS, 879

PHB, para el reenvío de paquetes IP, 804

módulos de medición

Ver también medidor tokenmt

Ver también medidor tswtc1mt

introducción, 800

invocar, en el archivo de configuración IPQoS, 852

resultados de la medición, 800, 874

múltiples rutas de redes IP (IPMP), *Ver* IPMP

N

NAT

compatible con RFC, 488

configurar reglas para, 646–647

desactivar, 658

descripción general, 646–647

eliminar reglas NAT, 675

IPsec admite varios clientes, 487–489

limitaciones con IPsec, 503

reglas NAT

anexar, 675–676

ver, 674–675

uso de IPsec e IKE, 618–619, 620–621

ver estadísticas, 680–681

negociación de claves, IKE, 625–627

netmasks, base de datos, subredes, 240

NIC

Ver tarjeta de interfaz de red (NIC)

especificar para filtro IP, 662–664

NIS

agregar dirección IPv6, 199

bases de datos de red, 64, 245

registro de nombre de dominio, 38

seleccionar como servicio de nombres, 65

NIS+

seleccionar como servicio de nombres, 65

y el almacén de datos DHCP, 453–456

nivel de privilegio, comprobar en IKE, 589

nivel de privilegios

cambiar en IKE, 590

comprobar en IKE, 590

definir en IKE, 595

nodo, IPv6, 75

nodo móvil, 696, 697, 698, 741

definición, 698

sección Address, 717

nodo móvil predeterminado

IP para móviles, sección Address, 742

sección Address de IP móvil, 718

nombre de almacén de claves, *Ver* ID de token

nombre de directorio (DN), para acceder a CRL, 612

nombre de host, activar solicitud de cliente de, 443

nombre de inicio de sesión anónimo, 43

nombre de node, host local, 235

nombre de nodo, host local, 109

nombres/asignar nombre

nombre de nodo

host local, 235

nombres de dominio

archivo /etc/defaultdomain, 106, 109, 235

dominios de nivel superior, 65

registrar, 38

seleccionar, 65

nombres de interfaz de red, 145–146

nombres/denominación

entidades de redes de denominación, 63

entidades de redes de nombres, 66

nombre de host

administrar, 64

archivo /etc/inet/hosts, 237

nombre de nodo

host local, 109

nombres de dominio

dominios de nivel superior, 65

registro, 38

seleccionar, 65

nombres simbólicos para números de red, 243

novedades

comando inetconv, 108

configurar sistemas de destino en IPMP, 775–777

detección de fallos basada en vínculos, 759

novedades (*Continuación*)

- estado de interfaz con comando `dladm`, 147
- mejoras de IKE, 582
- mejoras de IPsec, 507
- protocolo SCTP, 138–141
- Utilidad de gestión de servicios (SMF), 108
- `nsswitch.conf`, archivo
 - cambiar, 248
 - plantillas de servicios de nombres, 248
- nuevas características, DHCP en interfaces lógicas, 441
- nuevas funciones
 - comando `routeadm`, 179
 - configurar manualmente una dirección local de vínculo, 186–187
 - direcciones temporales en IPv6, 182–185
 - prefijo de sitio, en IPv6, 77, 78–79
 - secuencias de eventos DHCP, 448–451
 - selección de direcciones predeterminadas, 225–227
- números aleatorios, generar con comando `od`, 586
- números de red, 37
- números de red de clase A
 - descripción, 254
 - división de espacio de dirección IPv4, 60
 - intervalo de números disponibles, 61
- números de red de clase A, B y C, 56, 60
- números de red de clase B
 - descripción, 255
 - división de espacio de dirección IPv4, 60
 - intervalo de números disponibles, 61
- números de red de clase C
 - descripción, 255
 - división de espacio de dirección IPv4, 60
 - intervalo de números disponibles, 61

O

omitir

- directiva IPsec, 499
- IPsec en LAN, 538, 553

opción -a

- comando `ikecert`, 608
- comando `ikecert certdb`, 599, 604
- comando `ikecert certltdb`, 614

opción -c

- comando `ipseconf`, 488, 568
- comando `ipseckey`, 488, 571
- daemon `in.iked`, 586

opción -D

- comando `ikecert`, 634
- comando `ikecert certlocal`, 597

opción -F, comando `ikecert certlocal`, 597

opción -f

- comando `ipseckey`, 515
- daemon `in.iked`, 586

opción -L, comando `ipseconf`, 519

opción -l

- comando `ikecert certdb`, 599
- comando `ipseconf`, 519

opción -m, comando `ikecert certlocal`, 597opción -q, daemon `in.routed`, 253

opción -S

- comando `ikecert certlocal`, 597
- daemon `in.routed`, 253

opción -s, comando `ping`, 217

opción -T

- comando `ikecert certlocal`, 597

opción -t

- comando `ikecert`, 634
- comando `ikecert certlocal`, 597

opción -a, comando `ipseconf`, 515opción de seguridad `auth_algs`, comando `ifconfig`, 573–574opción de seguridad `encr_algs`, comando `ifconfig`, 574opción de seguridad `encr_auth_algs`, comando `ifconfig`, 574opción `failover`, comando `ifconfig`, 755

opción -kc

- comando `ikecert certlocal`, 597, 603, 633

opción -ks

- comando `ikecert certlocal`, 597, 633

Opciones DHCP, crear, 409

opciones DHCP

- descripción general, 313
- eliminar, 414
- modificar, 412
- propiedades, 407

opciones DHCP (*Continuación*)

trabajar con, 406

OpenSolaris filtro IP, comando `ifconfig`, 642**P**palabra clave `cert_root`

archivo de configuración de IKE, 605, 610

palabra clave `cert_trust`

archivo de configuración de IKE, 600, 610

comando `ikecert`, 634palabra clave `expire_timer`, archivo de configuración de IKE, 626palabra clave `ignore_crls`, archivo de configuración de IKE, 606palabra clave `ldap-list`, archivo de configuración de IKE, 613palabra clave `pkcs11_path`

descripción, 633

comando `ikecert`, 634

utilizar, 608

palabra clave `proxy`, archivo de configuración de IKE, 613palabra clave `retry_limit`, archivo de configuración de IKE, 626palabra clave `retry_timer_init`, archivo de configuración de IKE, 626palabra clave `retry_timer_max`, archivo de configuración de IKE, 626palabra clave `tunnel`

directiva IPsec, 500, 531, 538, 547

palabra clave `use_http`, archivo de configuración de IKE, 613

paquetes

ciclo de vida, 46, 49

capa de aplicación, 46

capa de Internet, 47

capa de red física, 48

capa de transporte, 46, 47

capa de vínculo de datos, 48

capa del vínculo de datos, 48

proceso de host de recepción, 48

proceso del host de recepción, 49

comprobar flujo, 221

paquetes (*Continuación*)

descartados o perdidos, 216

descripción, 45

encabezado

encabezado IP, 48

funciones de protocolo TCP, 41

encapsulado de datos, 46, 47

formato de encabezado de paquetes de IPv6, 261–262

fragmentación, 40

funciones de protocolo IP, 40

proteger

con IKE, 577

con IPsec, 491, 495–499

paquetes entrantes, 491

paquetes salientes, 491

reenviar, 114

soltados o perdidos, 41

transferir

enrutador, 68, 69

pila TCP/IP, 45, 49

UDP, 47

verificar protección, 525–526

visualizar contenido, 222

paquetes descartados o perdidos, 216

paquetes fragmentados, 40

paquetes perdidos o descartados, 216

paquetes perdidos o soltados, 41

paquetes registrados, guardar en un archivo, 684–685

paquetes soltados o perdidos, 41

parámetro `group`comando `ifconfig`, 771, 784parámetro `standby`comando `ifconfig`, 757, 778parámetro `test`, comando `ifconfig`, 771

parámetros de transmisión

ajuste de IKE, 625–627

parámetros globales de IKE, 626

parámetros de transmisión (IKE), cambiar, 625

perfil de derechos de administración de red, 527

perfil de derechos de gestión de red IPsec, 527

perfil de derechos de seguridad de red, 526–528

perfiles de derechos

administración de red, 527

- perfiles de derechos (*Continuación*)
 - gestión de red IPsec, 527
- permiso de DHCP
 - fecha de caducidad, 382
 - tipo, 382
- permiso DHCP
 - dinámico y permanente, 328
 - direcciones IP reservadas, 382
 - directiva, 324
 - negociación, 324
 - tiempo, 324
 - y direcciones IP reservadas, 328
- Petición de comentarios (RFC), IPQoS, 795
- petición de comentarios (RFC), IPv6, 73–74
- peticiones de comentarios (RFC), definición, 50
- PFS, *Ver* confidencialidad directa perfecta (Perfect Forward Secrecy o PFS)
- placa de Sun Crypto Accelerator 1000, 580
- placa de Sun Crypto Accelerator 4000, acelerar cálculos IKE, 580
- placa Sun Crypto Accelerator 1000, utilizar con IKE, 622–623
- placa Sun Crypto Accelerator 4000
 - almacenar claves IKE, 580
 - utilizar con IKE, 623–625
- planificación de la red, 69
 - agregar enrutadores, 66, 69
 - decisiones de diseño, 55
 - decisiones sobre diseño, 55
 - esquema de direcciones IP, 55, 63
- planificación de red, 53
 - registro de red, 58
- planificación de redes
 - asignaciones de nombres, 63, 66
- portal, en una topología de red, 126
- prefijo
 - prefijo de sitio, IPv6, 78–79
 - prefijo de subred, IPv6, 79
 - red, IPv4, 61
- prefijo 6to4, anuncio `/etc/inet/ndpd.conf`, 195
- prefijo de 6to4, explicación de partes, 259
- prefijo de red, IPv4, 61
- prefijo de sitio, IPv6
 - advertir, en el enrutador, 180
 - prefijo de sitio, IPv6 (*Continuación*)
 - definición, 77, 78
 - obtención, 94–95
 - prefijo de subred, IPv6, 79
 - prefijos
 - anuncio de enrutador, 280, 283, 285
 - presencia de color, 801
 - procesador UltraSPARC T2, utilizar con IKE, 622
 - programa `/usr/sbin/in.rdisc`, descripción, 254
 - programa ftp, 42
 - programa FTP anónimo
 - descripción, 43
 - programa FTP anónimo, descripción, 43
 - programa `hostconfig`, 109
 - programa `in.rdisc`, descripción, 254
 - protección de repetición de mensajes, 737
 - Protección de una VPN con IPsec (mapa de tareas), 532–565
 - Protección del tráfico con IPsec (mapa de tareas), 509
 - proteger
 - claves en hardware, 580
 - paquetes entre dos sistemas, 511–515
 - servidor web con IPsec, 515–518
 - sistemas portátiles con IPsec, 614–621
 - tráfico IPsec, 489
 - VPN con túnel IPsec en modo transporte, 551–557
 - VPN con túnel IPsec en modo túnel, 535–545
 - protocolo ARP (Address Resolution Protocol), comparación con protocolo ND (Neighbor Discovery), 283–284
 - protocolo BOOTP
 - compatibilidad con clientes con el servicio DHCP, 376
 - y DHCP, 301
 - protocolo Bootparams, 100
 - protocolo de administración de claves y asociación de seguridad de Internet (ISAKMP) asociaciones de seguridad, descripción, 577
 - Protocolo de configuración dinámica de host, *Ver* protocolo DHCP
 - protocolo de control de agregación de vínculos (LACP)
 - modificar modos de LACP, 167
 - modos, 163

- protocolo de información de enrutamiento (RIP),
 - descripción, 44
- protocolo de Internet (IP), 696
- protocolo de reconocimiento, tres vías, 47
- protocolo de resolución de direcciones (ARP),
 - definición, 41
- protocolo de tres vías, 47
- protocolo DHCP
 - descripción general, 301
 - secuencia de eventos, 303
 - ventajas en la implementación de Oracle Solaris, 302
- protocolo ICMP
 - descripción, 41
 - invocar, con ping, 216
 - mensajes, para protocolo ND, 278–279
 - visualizar estadísticas, 209
- protocolo ICMP Router Discovery (RDISC), 254
- protocolo IP
 - comprobar conectividad de host, 216, 217
 - descripción, 40
 - visualizar estadísticas, 209
- protocolo ND
 - capacidad, 82
 - configuración automática de direcciones, 83
 - descubrimiento de enrutadores, 83
 - descubrimiento de prefijos, 83
 - resolución de direcciones, 83
- protocolo ND (Neighbor Discovery)
 - características principales, 278–284
 - comparación con ARP, 283–284
 - configuración automática de direcciones, 279
 - descubrimiento de enrutador, 280
 - descubrimiento de prefijo, 280
 - detección de direcciones duplicadas, 281
 - solicitud de vecino, 281
- protocolo RARP
 - asignación de direcciones Ethernet, 250
 - comprobar direcciones Ethernet, 230
 - configuración de servidor RARP, 107
 - descripción, 100
- protocolo SCTP
 - agregar servicios activados para SCTP, 138–141
 - descripción, 42

- protocolo SCTP (*Continuación*)
 - IPsec y, 511
 - limitaciones con IPsec, 504
 - servicio del archivo /etc/inet/services, 252
 - visualizar estadísticas, 209
 - visualizar estado, 211
- Protocolo simple de administración de red (SNMP), 44
- protocolo TCP
 - descripción, 41
 - establecer una conexión, 47
 - segmentación, 47
 - servicios del archivo /etc/inet/services, 252
 - visualizar estadísticas, 209
- protocolo Telnet, 43
- protocolo tftp
 - descripción, 43
 - protocolo de inicio de servidor de configuración de red, 100
- protocolo UDP
 - descripción, 42
 - proceso de paquetes UDP, 47
 - servicios del archivo /etc/inet/services, 252
 - visualizar estadísticas, 209
- protocolos de enrutamiento
 - daemons de enrutamiento asociados, 116
 - descripción, 44, 115, 253, 254
 - en Oracle Solaris, 115
 - protocolo de portal de límite (BGP), 119
 - protocolo de portal exterior (EGP), 115
 - protocolo de portal interior (IGP), 115
 - RDISC
 - descripción, 44, 254
 - RIP
 - descripción, 44, 253
 - selección automática, 123
- protocolos de pila doble, 90, 263
- protocolos de seguridad
 - Carga de seguridad encapsuladora (ESP), 496–497
 - consideraciones de seguridad, 497
 - descripción general, 489
 - encabezado de autenticación (AH), 496
 - mecanismos de protección IPsec, 495
- protocolos TCP/IP, servicios estándar, 137
- próximo salto, 284

puertos, números de puerto TCP, UDP y SCTP, 252
 punto de código DS (DSCP), 801, 804
 configuración de reconocimiento de color, 876
 configurar, en un enrutador diffserv, 855, 877
 definir, en el archivo de configuración IPQoS, 839
 parámetro `dscp_map`, 879
 PHB y DSCP, 804
 planificar, en la directiva QoS, 823
 punto de código de reenvío AF, 805, 878
 punto de código de reenvío EF, 877
 punto de código de reenvío EF, 805
 punto de conexión físico (PPA), 156

Q

QoS, directiva
 implementar en archivo de configuración
 IPQoS, 829
 mapa de tareas de planificación, 814

R

ranuras, del hardware, 635
 RBAC
 IPsec y, 511
 y comandos DHCP, 311
 RDISC
 descripción, 44, 254
 reconfiguración dinámica (DR)
 agregar interfaces a un grupo IPMP, 763–764
 definición, 753
 desconectar interfaces de un grupo IPMP, 764
 interfaces que no están presentes durante el
 inicio, 765
 interoperatividad con IPMP, 763–765
 procedimientos de conexión en DR, 785–786
 procedimientos de desconexión en DR, 784–785
 reconectar interfaces en un grupo IPMP, 764–765
 reemplazar interfaces fallidas, 784–786
 reemplazar una interfaz que no estaba presente al
 iniciar, 786–788
 reconocimiento de colores, 875

recuperación tras los errores
 definición, 752
 reconfiguración dinámica (DR), con, 764–765
 red de área extensa (WAN)
 Internet
 registro de nombre de dominio, 38
 red externa, 698, 705, 709
 red permanente, 698
 red principal, 697, 705, 708
 redes DHCP
 agregar a servicio DHCP, 369
 eliminar del servicio DHCP, 374
 modificar, 371
 trabajar con, 366–376
 redes privadas virtuales (VPN)
 configurar con el comando `routeadm`, 556
 configurar con el comando `routeadm`, 536
 construidas con IPsec, 502
 ejemplo de IPv4, 535–545
 ejemplo de IPv6, 545–551
 proteger con IPsec, 535–545
 proteger con IPsec en modo de transporte de
 túnel, 551–557
 redes TCP/IP
 archivos de configuración, 233
 archivo `/etc/defaultdomain`, 235
 archivo `/etc/defaultrouter`, 235
 archivo `/etc/nodename`, 109, 235
 base de datos `hosts`, 235, 238
 base de datos `netmasks`, 240
 `/etc/hostname.interfaz` archivo, 234
 configuración de host, 99
 configurar
 archivo `nsswitch.conf`, 247, 249
 bases de datos de red, 244, 247, 249
 clientes de red, 109
 instalación de servidor de configuración de
 red, 107
 modo de archivos locales, 107
 modos de configuración de host, 99, 101
 requisitos previos, 98
 servicios TCP/IP estándar, 137
 modos de configuración de host, 101
 configuraciones mixtas, 101

redes TCP/IP, modos de configuración de host
(*Continuación*)

- ejemplo de red, 101
- modo de archivos locales, 99, 100
- modo de cliente de red, 101
- servidores de configuración de red, 100
- números de red, 37
- proteger con ESP, 496
- resolución de problemas, 224
 - comando `ifconfig`, 205
 - comando `netstat`, 209
 - comando `ping`, 216, 217
 - comprobaciones de software, 230
 - métodos generales, 229
 - pérdida de paquetes, 216, 217
 - programas de diagnóstico de otros fabricantes, 229
 - visualizar contenido de paquetes, 222
- tareas de configuración de red IPv4, 104
- topología de red IPv4, 101
- redirección
 - IPv6, 279, 283
- redirigir, IPv6, 83
- reemplazar
 - claves manuales (IPsec), 521
 - claves previamente compartidas (IKE), 588–589
 - IPsec SAs, 521
- reenviar tráfico, planificar, en la directiva QoS, 817
- reenvío acelerado (EF), 805, 877
 - definir, en el archivo de configuración IPQoS, 840
- reenvío asegurado (AF), 805, 878
 - para una instrucción `action` de marcador, 839
 - tabla de puntos de código AF, 878
- reenvío de IP
 - en VPN, 502
 - en VPN IPv4, 536, 539, 540, 551, 554
 - en VPN IPv6, 546, 548, 549, 558, 560, 561
- reenvío de tráfico, efecto de comportamientos PHB en el reenvío de tráfico, 877
- reenvío del tráfico
 - flujo del tráfico a través de redes Diffserv, 805
 - reenvío de datagramas, 879
 - reenvío de paquetes IP, con DSCP, 804

- registrar
 - nombres de dominio, 38
 - sistemas autónomos, 120
- registro
 - indicador de túnel inverso, 707
 - IP para móviles, 698, 700, 705
 - mensaje de respuesta, 708
 - mensajes, 705, 708
 - redes, 58
 - solicitud, 707
- registro de archivo `syslog.conf` para IPQoS, 859
- registros AAAA, 200, 295
- regulación del ancho de banda, 797
- regular el ancho de banda, planificar, en la directiva QoS, 817
- Requests for Comments (RFC), 50
- requisitos de IPMP, 753–754
- resolución de direcciones, en IPv6, 83
- resolución de problemas
 - carga útil de IKE, 607
 - comprobar vínculos de PPP
 - flujo de paquetes, 221
- redes TCP/IP
 - comando `ping`, 217
 - comando `traceroute`, 220–221
 - comprobaciones de software, 230
 - comprobar paquetes entre cliente y servidor, 224
 - métodos generales, 229
 - mostrar estado de interfaz con el comando `ifconfig`, 208
 - observar transmisiones de interfaces, 212
 - obtener estadísticas por protocolo, 209–210
 - obtener estado del protocolo de transporte, 211–212
 - pérdida de paquetes, 216, 217
 - programas de diagnóstico de otros fabricantes, 229
 - seguimiento de actividad de `in.ndpd`, 219–220
 - seguimiento de `in.routed`, 218–219
 - sondear hosts remotos con comando `ping`, 216
 - supervisar estado de red con comando `netstat`, 209
 - supervisar transferencia de paquetes con el comando `snoop`, 221

resolución de problemas, redes TCP/IP (*Continuación*)
 visualizar estado de rutas conocidas, 215–216
 redes TCP/IP networks
 visualizar estado de interfaz con comando
 ifconfig, 205
 tiempo de transmisión de IKE, 625–627
 resolver
 problemas IPv6, 231–232
 roles, crear rol de seguridad de red, 526–528
 routeadm, comando, activar enrutamiento
 dinámico, 124
 routeadm command, reenvío de IP, 536
 routers
 configurar
 para redes IPv4, 121
 ejemplo, configurar un encaminador
 predeterminado, 124
 Routing Information Protocol (RIP), descripción, 253

S

salto, en reenvío de paquetes, 115
 saltos, agente de reenvío, 364
 sección Address
 archivo de configuración de IP para móviles, 738,
 739–742
 direcciones privadas, 740
 etiquetas y valores, 740
 etiquetas y valores de nodo predeterminado, 742
 etiquetas y valores NAI, 741
 sección Advertisements
 archivo de configuración de IP para
 móviles, 735–736
 etiquetas y valores, 735
 sección General
 archivo de configuración de IP para móviles, 735
 etiqueta Version, 735
 sección GlobalSecurityParameters
 archivo de configuración de IP para
 móviles, 736–737
 etiquetas y valores, 737
 sección Pool, etiquetas y valores, 738
 sección Pool section, archivo de configuración de IP
 para móviles, 737–738

sección SPI
 archivo de configuración de IP para
 móviles, 738–739, 740
 etiquetas y valores, 739
 segmento ACK, 47
 segmento SYN, 47
 seguridad
 IKE, 630
 IPsec, 489
 seguridad de red, configurar, 485
 selección de direcciones predeterminadas, 269–270
 definición, 225–227
 tabla de directrices de selección de direcciones
 IPv6, 225–227
 selectores, 800
 IPQoS 5-tuple, 799
 planificar, en la directiva QoS, 818
 selectores, lista de, 872
 servicio de manual-key, descripción, 495
 servicio de nombres de archivos locales
 archivo /etc/inet/hosts
 archivo inicial, 236, 237
 ejemplo, 238
 formato, 236
 requisitos, 238
 archivo /etc/inet/ipnodes, 512
 archivo/etc/inet/hosts, 512
 bases de datos de red, 245
 descripción, 65
 modo de archivos locales, 99, 100
 servicio DHCP
 agregar redes, 369
 asignación de direcciones IP, 312
 compatibilidad con clientes BOOTP, 376
 compatibilidad con instalación de inicio WAN, 416
 desconfigurar, 339
 con el Administrador de DHCP, 341
 descripción general de la configuración de red, 312
 direcciones IP
 agregar, 383
 eliminar, 389
 inutilizables, 390
 modificar propiedades, 387

- Servicio DHCP
 - direcciones IP
 - reserva para cliente, 393
- servicio DHCP
 - habilitar e inhabilitar
 - comando `dhcpconfig`, 351–352
 - efectos de, 350
 - habilitar y deshabilitar
 - Administrador de DHCP, 351
 - iniciar y detener
 - Administrador de DHCP, 351
 - efectos de, 350
 - Inicio e instalación en red de Oracle Solaris, 415–416
 - mensajes de error, 457, 464
 - modificar opciones de servicio, 353
 - planificar, 317
 - registro
 - descripción general, 355
 - transacciones, 356
 - supervisión de interfaz de red, 367
 - tiempo de oferta de caché, 364
 - topología de red, 318
 - Utilidad de gestión de servicios, 352–353
- servicio ike
 - descripción, 495, 567
 - utilizar, 513
- servicio `Ipsecalgs`, descripción, 567
- servicio `manual-key`
 - descripción, 567
 - utilizar, 514
- servicio `policy`
 - descripción, 567
 - utilizar, 513
- servicios
 - IPsec
 - `ipsecalgs`, 506
 - red y comando `svcadm`, 537, 546, 552
- servicios de archivos, 44
- servicios de nombres
 - archivos correspondientes a las bases de datos de red, 246
 - archivos locales
 - archivo `/etc/inet/hosts`, 236, 238
- servicios de nombres, archivos locales (*Continuación*)
 - descripción, 65
 - modo de archivos locales, 99, 100
 - base de datos `hosts y`, 237, 238
 - bases de datos de red y, 64, 245
 - especificación de orden de búsqueda de base de datos, 247
 - especificación de orden de búsqueda de bases de datos, 249
 - NIS, 65
 - NIS+, 65
 - plantillas de archivo `nsswitch.conf`, 248
 - registro de clientes DHCP, 363
 - registro de nombre de dominio, 38
 - seleccionar servicio, 64
 - seleccionar un servicio, 66
 - servicios admitidos, 64
 - sistema de nombre de dominio (DNS), 43
 - sistema de nombres de dominio (DNS), 65
 - subdivisiones administrativas, 66
- servicios diferenciados, 793
 - distribuciones de red, 810
 - modelo de servicios diferenciados, 799
 - proporcionar diferentes clases de servicio, 798
- servicios NFS, 44
- servidor, DHCPv6, 430
- servidor de aplicaciones, configurar para IPQoS, 845
- servidor DHCP
 - administrar, 307
 - almacén de datos, 307
 - configuración
 - descripción general, 311
 - información recopilada, 320
 - configurar
 - comando `dhcpconfig`, 342
 - con el Administrador de DHCP, 334
 - cuántos configurar, 319
 - ejecutar en modo de depuración, 461
 - ejemplo de salida, 463–465
 - funciones, 306
 - habilitar para actualizar DNS, 360–361
 - opciones, 353
 - Administrador de DHCP, 364–365
 - comando `dhcpconfig`, 365–366

- servidor DHCP (*Continuación*)
 - planificación de múltiples servidores, 329
 - seleccionar, 322
 - solución de problemas, 453
 - servidores, IPv6
 - habilitar IPv6, 188–189
 - planificar tareas, 91
 - servidores de configuración de red
 - definición, 100
 - instalar, 107
 - protocolos de inicio, 100
 - servidores web
 - configurar para IPQoS, 832, 833, 842, 844
 - proteger con IPsec, 515–518
 - siguiente salto, 115
 - sistema autónomo (SA), *Ver* topología de red
 - sistema de destino, en IPMP
 - configurar en una secuencia de shell, 776–777
 - configurar manualmente, 776
 - definición, 752
 - sistema de nombre de dominio (DNS)
 - bases de datos de red, 64, 245
 - descripción, 43
 - habilitar actualizaciones dinámicas por parte de
 - servidor DHCP, 360–361
 - registro de nombre de dominio, 38
 - seleccionar como servicio de nombres, 65
 - sistema de nombres de dominio (DNS)
 - archivo de zona, 198
 - archivo de zona inversa, 198
 - extensiones para IPv6, 295
 - sistema nombres de dominio (DNS), preparar, para
 - admitir IPv6, 92–93
 - sistemas, proteger comunicación, 511–515
 - sistemas operativos basados en BSD
 - vínculo de archivo `/etc/inet/hosts`, 236
 - vínculo de archivo `/etc/inet/netmasks`, 243
 - SNMP (Protocolo simple de administración de red), 44
 - sockets
 - consideraciones de seguridad, 515
 - seguridad IPsec, 570
 - visualizar estado de sockets con `netstat`, 212
 - solicitud de agente, IP para móviles, 701, 702
 - solicitud de agentes, IP para móviles, 700
 - solicitud de enrutador
 - IPv6, 278, 280
 - solicitud de vecino, IPv6, 279
 - solicitudes de certificados
 - de autoridad de certificación, 603
 - en hardware, 609
 - utilizar, 634
 - solicitudes de comentarios (RFC)
 - IKE, 490
 - IPsec, 490
 - solicitudes de opciones, 433
 - solución de problemas, DHCP, 453
 - sondear una interfaz, 122, 149
 - subdivisiones, administrativas, 66
 - subdivisiones administrativas, 66
 - subredes
 - base de datos netmasks, 240
 - creación de máscara de red, 241, 242
 - editar archivo `/etc/inet/netmasks`, 243
 - descripción general, 240
 - direcciones IPv4 y, 242
 - IPv4
 - configuración de máscara de red, 106
 - direcciones y, 241
 - IPv6
 - configuración 6to4, 292
 - definición, 76
 - sugerencias de numeración, 95
 - máscaras de red
 - aplicar a dirección IPv4, 242
 - crear, 242
 - número de subred, IPv4, 240
 - número de subred en direcciones IPv4, 61
 - prefijo de subred, IPv6, 79
 - servidores de configuración de red, 100
- T**
- opción -T
 - comando `ikecert`, 608, 634, 635
 - t, opción, `daemon inetd`, 137
 - tabla de enlace
 - agente interno, 725, 727
 - IP para móviles, 744

- tabla dhcptab, 335
 - descripción, 480
 - descripción general, 308
 - eliminar al desconfigurar, 340
 - leer automáticamente, 364
- tabla hosts.org_dir, 199
- tabla ipnodes.org_dir, 199
- tablas de enrutamiento
 - configuración manual, 127
 - configurar manualmente, 126
 - creación de daemon de in.routed, 253
 - definición, 115
 - descripción, 68
 - ejemplo de transferencia de paquetes, 69
 - modo de ahorro de espacio, 253
 - mostrar, 229
 - seguimiento de todas las rutas, 221
 - subredes, 240
- tablas de estado, ver, 679
- tablas de red DHCP
 - creadas durante la configuración del servidor, 336
 - descripción, 309
 - eliminar al desconfigurar, 340
- tarjeta de interfaz de red (NIC)
 - administrar NIC que no están durante el inicio, 765
 - conectar NIC con DR, 763–764
 - definición, 751
 - desconectar NIC con DR, 764
 - detección de reparaciones, 752
 - fallos y conmutación por error, 752
 - NIC, tipos de, 145
 - NIC que admiten IPMP, 759
 - reconfiguración dinámica, 753
 - velocidad de NIC en un grupo IPMP, 751–752
- TCP/IP protocol suite, 37
- tiempo de detección de fallos, IPMP, 760
- tipos de encapsulado, IP para móviles, 709
- Token ring, compatibilidad con IPMP para, 770
- topología, 66, 67
- topología de IP para móviles, 696
- topología de red, 66, 67
 - DHCP y, 318
 - sistema autónomo, 118
- topología de sitio, IPv6, 80
- topología pública, IPv6, 80
- traducción de direcciones de red (NAT), *Ver* NAT
- transición a IPv6, mecanismo 6to4, 290
- truncaciones, *Ver* agregaciones
- túnel, 709
- túnel inverso
 - consideraciones del agente externo, 708
 - consideraciones del agente interno, 708
 - enrutamiento de datagramas de multidifusión, 711
 - enrutamiento de datagramas de unidifusión, 710
 - IP para móviles, 701, 703–704
- túneles
 - configuración de IPv6
 - IPv4 a través de IPv6, 192
 - IPv6 a través de IPv4, 190–191
 - IPv6 a través de IPv6, 191
 - configurar IPv6
 - ejemplos, 272–273
 - en enrutador de reenvío 6to4, 196
 - túneles 6to4, 192
 - IPsec, 502
 - IPv6, automático
 - Ver* túneles, túneles 6to4
 - IPv6, configurados manualmente, 288–290
 - mecanismos de colocación en túneles de IPv6, 286
 - modo transporte, 499
 - modo túnel, 500
 - modos en IPsec, 499–501
 - opciones de seguridad de *ifconfig*, 573–574
 - planificar, para IPv6, 93
 - proteger paquetes, 502
 - topología, hasta encaminador de reenvío 6to4, 294
 - túneles 6to4
 - flujo de paquetes, 292, 294
 - topología, 291
 - túneles 6to4
 - definición, 192
 - enrutador de reenvío 6to4, 196
 - flujo de paquetes, 292, 294
 - topología de ejemplo, 291
 - túneles automáticos, transición a IPv6, 287
 - túneles IPsec, sintaxis simplificada, 487–489
 - tunnels, túneles 6to4, 290

U

- unidad de transmisión máxima (MTU), 283
- utilidad de gestión de servicios (SMF)
 - servicio IKE
 - actualizar, 514, 589
 - cambiar propiedad de servicio, 590
- Utilidad de gestión de servicios (SMF)
 - servicio IKE
 - descripción, 629–630
- utilidad de gestión de servicios (SMF)
 - servicio IKE
 - descripción, 575
- Utilidad de gestión de servicios (SMF)
 - servicio IKE
 - habilitar, 630
- utilidad de gestión de servicios (SMF)
 - servicio IKE
 - habilitar, 513, 618, 627
 - ike servicio, 580
- Utilidad de gestión de servicios (SMF)
 - servicio IKE
 - propiedades configurables, 629
- utilidad de gestión de servicios (SMF)
 - servicio IKE
 - reiniciar, 513
 - servicio ike, 495
- servicios de IPsec, 567–568
 - manual-key servicio, 571
 - servicio ipsecalgs, 570
 - servicio policy, 505
- servicios IPsec
 - descripción, 487–489
 - descripción de manual-key, 495
 - lista, 505–507
 - manual-key utilizar, 514
 - utilizar para administrar IKE, 528–529
 - utilizar para administrar IPsec, 528–529
- utilidades de claves
 - comando ipseckey, 495
 - protocolo IKE, 576
 - servicio de manual-key, 495
 - servicio ike, 495
- utilidades de la línea de comandos de DHCP, 310
 - privilegios, 349

V

- opción -V
 - comando snoop, 573, 574
- vaciar, *Ver* eliminar
- valor de prioridad de usuario, 801
- varias interfaces de red, sistemas cliente DHCP, 441
- verificar
 - archivo ipsecinit.conf
 - sintaxis, 538
 - protección de paquetes, 525–526
- vínculo, IPv6, 76
- vínculo IP, en terminología IPMP, 751
- vínculos de PPP
 - resolución de problemas
 - flujo de paquetes, 221
- visualizar
 - configuración de IPsec, 569–570
 - directiva IPsec, 518–519
- visualizar estadísticas de protocolo, 209
- VLAN
 - configuración, 154–159
 - configuración de nodos, 156
 - configuraciones, 154–157
 - definición, 154–159
 - dispositivo virtual, 158
 - escenarios de muestra, 154
 - ID VLAN (VID), 155–157
 - interfaces admitidas en Solaris 10 1/06, 158
 - planificar, 157
 - punto de conexión físico (PPA), 156
- VPN, *Ver* redes privadas virtuales (VPN)

Z

- zona global, IKE, 575
- zonas
 - administración de claves y, 511
 - IPsec y, 504, 511

