

Administración de Oracle® Solaris: servicios IP

Copyright © 1999, 2012, Oracle y/o sus filiales. 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 END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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.

Contenido

Prefacio	19
 Parte I Administración de TCP/IP	 23
 1 Planificación de la implementación de red	 25
Planificación de la red (mapa de tareas)	25
Determinación del hardware de red	26
Cómo decidir el formato de las direcciones IP para la red	27
Direcciones IPv4	27
Direcciones DHCP	28
Direcciones IPv6	29
Direcciones privadas y prefijos de documentación	29
Cómo obtener el número de IP de la red	29
Entidades de denominación en la red	30
Administración de nombres de host	30
Selección de un servicio de nombres y de directorios	31
Uso de subredes	32
Implementación de redes virtuales	32
 2 Consideraciones para el uso de direcciones IPv6	 33
Planificación de IPv6 (mapa de tareas)	33
Situación hipotética de topología de red IPv6	34
Cómo garantizar la compatibilidad de hardware para IPv6	36
Preparación de un plan de direcciones IPv6	37
Obtención de un prefijo de sitio	37
Creación del esquema de numeración de IPv6	37
Configuración de servicios de red para admitir IPv6	39

▼ Cómo preparar servicios de red para admitir IPv6	39
▼ Cómo preparar DNS para admitir IPv6	40
Planificación para el uso de túneles en la red	41
Aspectos relacionados con la seguridad en la implementación de IPv6	41
3 Configuración de una red IPv4	43
Configuración de red (mapa de tareas)	43
Antes de comenzar la configuración de red	44
Configuración de los componentes del sistema en la red	45
Topología de sistemas autónomos IPv4	45
▼ Cómo configurar una interfaz IP	47
Configuración de los modos de configuración del sistema	51
Configuración de un enrutador IPv4	56
▼ Configuración de un enrutador IPv4	57
Tablas y tipos de enrutamiento	59
Configuración de hosts múltiples	62
Configuración del enrutamiento para sistemas de interfaz única	65
Cómo agregar una subred a una red	68
Supervisión y modificación de los servicios de capa de transporte	70
▼ Cómo registrar las direcciones IP de todas las conexiones TCP entrantes	71
▼ Cómo agregar servicios que utilicen el protocolo SCTP	71
▼ Cómo utilizar los envoltorios TCP para controlar el acceso a los servicios TCP	74
4 Habilitación de IPv6 en una red	77
Configuración de una interfaz de IPv6	77
▼ Cómo configurar un sistema para IPv6	78
▼ Cómo desactivar la configuración automática de direcciones IPv6	80
Configuración de un enrutador IPv6	80
▼ Cómo configurar un enrutador habilitado para IPv6	80
Modificación de la configuración de una interfaz de IPv6 para hosts y servidores	82
Uso de direcciones temporales para una interfaz	83
Configuración de un token IPv6	86
Administración de interfaces habilitadas para IPv6 en servidores	88
Configuración de la compatibilidad con el servicio de nombres para IPv6	89
▼ Cómo agregar direcciones IPv6 a DNS	89

▼ Cómo visualizar información sobre servicios de nombres de IPv6	90
▼ Cómo verificar que los registros PTR de DNS IPv6 se actualicen correctamente	91
▼ Cómo visualizar información de IPv6 mediante NIS	91
5 Administración de una red TCP/IP	93
Tareas de administración principales de TCP/IP (mapa de tareas)	94
Supervisión del estado de la red con el comando <code>netstat</code>	95
▼ Cómo visualizar estadísticas por protocolo	95
▼ Cómo visualizar el estado de protocolos de transporte	96
▼ Cómo visualizar el estado de interfaces de red	97
▼ Cómo visualizar el estado de los sockets	98
▼ Cómo visualizar el estado de las transmisiones de paquetes de un determinado tipo de dirección	100
▼ Cómo visualizar el estado de rutas conocidas	100
Sondeo de hosts remotos con el comando <code>ping</code>	101
▼ Cómo determinar si un host remoto está en ejecución	102
▼ Cómo determinar si un host descarta paquetes	102
Administración y registro de la visualización del estado de la red	103
▼ Cómo controlar la salida de visualización de comandos relacionados con IP	103
▼ Cómo registrar acciones del daemon de rutas de IPv4	104
▼ Cómo efectuar el seguimiento de las actividades del daemon de descubrimiento cercano de IPv6	105
Visualización de información de enrutamiento con el comando <code>traceroute</code>	105
▼ Cómo saber la ruta de un host remoto	106
▼ Cómo efectuar el seguimiento de todas las rutas	106
Control de transferencias de paquetes con el comando <code>snoop</code>	107
▼ Cómo comprobar paquetes de todas las interfaces	107
▼ Cómo capturar la salida del comando <code>snoop</code> en un archivo	108
▼ Cómo comprobar paquetes entre un cliente y un servidor IPv4	109
▼ Cómo supervisar tráfico de redes IPv6	109
Supervisión de paquetes mediante dispositivos de capa IP	110
Administración de selección de direcciones predeterminadas	113
▼ Cómo administrar la tabla de directrices de selección de direcciones IPv6	114
▼ Cómo modificar la tabla de selección de direcciones IPv6 sólo para la sesión actual	115

6 Configuración de túneles IP	117
Descripción general de túneles IP	117
Administración de túneles IP en esta versión de Oracle Solaris	117
Tipos de túneles	118
Túneles en los entornos de red IPv6 e IPv4 combinados	118
Túneles 6to4	119
Implementación de túneles	124
Requisitos para crear túneles	124
Requisitos para túneles e interfaces IP	125
Configuración y administración de túneles con el comando <code>dladm</code>	126
Subcomandos <code>dladm</code>	126
Configuración de túneles (mapa de tareas)	126
▼ Cómo crear y configurar un túnel IP	127
▼ Cómo configurar un túnel 6to4	131
▼ Cómo configurar un túnel 6to4 hasta un enrutador de reenvío 6to4	133
▼ Cómo modificar una configuración de túnel IP	135
▼ Cómo visualizar una configuración de túnel IP	136
▼ Cómo visualizar las propiedades de un túnel IP	137
▼ Cómo suprimir un túnel IP	138
7 Resolución de problemas de red	139
Consejos de resolución de problemas de red generales	139
Ejecución de comprobaciones de diagnóstico básicas	139
▼ Cómo realizar comprobaciones de software de red básicas	140
Problemas comunes al utilizar IPv6	140
El enrutador IPv4 no puede actualizarse a IPv6	141
Problemas tras la actualización de servicios a IPv6	141
El ISP actual no admite IPv6	141
Cuestiones de seguridad al transmitir datos mediante túnel a un enrutador de reenvío 6to4	142
8 Referencia de IPv4	143
Archivos de configuración de red	143
Daemon de servicios de Internet <code>inetd</code>	145
El servicio SMF <code>name-service/switch</code>	145

Cómo afectan los servicios de nombres a las bases de datos de red	147
Protocolos de enrutamiento en Oracle Solaris	147
Protocolo de información de enrutamiento (RIP)	147
Protocolo ICMP Router Discovery (RDISC)	148
Tablas de protocolos de enrutamiento en Oracle Solaris	148
9 Referencia de IPv6	151
Implementación de IPv6 en Oracle Solaris	151
Archivos de configuración de IPv6	151
Comandos relacionados con IPv6	155
Daemons relacionados con IPv6	160
Protocolo ND de IPv6	163
Mensajes de ICMP del protocolo ND	164
Proceso de configuración automática	164
Solicitud e inasequibilidad de vecinos	166
Algoritmo de detección de direcciones duplicadas	167
Anuncios de proxy	167
Equilibrio de la carga entrante	167
Cambio de dirección local de vínculo	168
Comparación del protocolo ND con ARP y protocolos relacionados con IPv4	168
Enrutamiento de IPv6	170
Anuncio de enrutador	171
Extensiones de IPv6 para servicios de nombres de Oracle Solaris	172
Extensiones de DNS para IPv6	172
Cambios en los comandos de servicio de nombres	172
Admisión de NFS y RPC IPv6	172
Admisión de IPv6 en ATM	172
Parte II DHCP	173
10 Acerca de DHCP (descripción general)	175
Acerca del protocolo DHCP	175
Ventajas del uso de DHCP	176
Funcionamiento de DHCP	177

Servidor DHCP de ISC	180
Servidor DHCP de Sun antiguo	181
Cliente DHCP	181
11 Administración del servicio DHCP de ISC	183
Configuración del acceso de usuario a los comandos de DHCP	183
▼ Cómo conceder a los usuarios acceso a los comandos de DHCP	184
Tareas del servidor DHCP	184
▼ Cómo configurar un servidor DHCP de ISC	184
▼ Cómo modificar la configuración del servicio DHCP	185
12 Configuración y administración del cliente DHCP	187
Acerca del cliente DHCP	187
Servidor DHCPv6	188
Diferencias entre DHCPv4 y DHCPv6	188
El modelo administrativo de DHCP	188
Detalles del protocolo	190
Interfaces lógicas	190
Negociación de opciones	191
Sintaxis de configuración	191
Inicio de cliente DHCP	192
Comunicación con DHCPv6	192
Cómo gestionan los protocolos del cliente DHCP la información de configuración de red	193
Cierre del cliente DHCP	194
Habilitación y deshabilitación de un cliente DHCP	195
▼ Cómo habilitar un cliente DHCP	195
▼ Cómo deshabilitar un cliente DHCP	196
Administración del cliente DHCP	196
Opciones del comando <code>ipadm</code> usadas con el cliente DHCP	197
Asignación de los parámetros de configuración del cliente DHCP	198
Sistemas cliente DHCP con varias interfaces de red	199
Nombres de host de cliente DHCPv4	199
▼ Cómo habilitar un cliente DHCPv4 para que solicite un nombre de host específico	200
Sistemas cliente DHCP y servicios de nombres	201

Secuencias de eventos de cliente DHCP	203
13 Comandos y archivos DHCP (referencia)	205
Comandos DHCP	205
Archivos que utiliza el servicio DHCP	207
Servicios SMF usados por el servicio DHCP	208
Parte III Seguridad IP	209
14 Arquitectura de seguridad IP (descripción general)	211
Introducción a IPsec	211
RFC IPsec	213
Terminología de IPsec	213
Flujo de paquetes IPsec	214
Asociaciones de seguridad IPsec	217
Gestión de claves en IPsec	217
Mecanismos de protección de IPsec	218
Encabezado de autenticación	218
Carga de seguridad encapsuladora	219
Algoritmos de autenticación y cifrado en IPsec	220
Políticas de protección IPsec	221
Modos de transporte y túnel en IPsec	221
Redes privadas virtuales e IPsec	224
Paso a través de IPsec y NAT	224
IPsec y SCTP	225
IPsec y zonas de Oracle Solaris	226
IPsec y dominios lógicos	226
Archivos y utilidades IPsec	226
15 Configuración de IPsec (tareas)	229
Protección del tráfico con IPsec	229
▼ Cómo proteger el tráfico entre dos sistemas con IPsec	230
▼ Cómo utilizar IPsec para proteger un servidor web del tráfico que no procede de Internet	233

▼ Cómo visualizar las políticas de IPsec	235
Protección de una VPN con IPsec	236
Ejemplos de protección de una VPN con IPsec mediante el uso del modo de túnel	236
Descripción de la topología de red para la protección de una VPN por parte de las tareas de IPsec	237
▼ Cómo proteger una VPN con IPsec en modo de túnel	239
Gestión de IPsec e IKE	243
▼ Cómo crear manualmente claves IPsec	243
▼ Cómo configurar una función para la seguridad de la red	245
▼ Cómo gestionar servicios IPsec e IKE	247
▼ Cómo verificar que los paquetes estén protegidos con IPsec	248
16 Arquitectura de seguridad IP (referencia)	251
Servicios IPsec	251
Comando ipsecconf	252
Archivo ipsecinit.conf	252
Archivo ipsecinit.conf de ejemplo	253
Consideraciones de seguridad para ipsecinit.conf e ipsecconf	253
Comando ipsecalgs	254
Base de datos de asociaciones de seguridad para IPsec	255
Utilidades para la generación de SA en IPsec	255
Consideraciones de seguridad para ipseckey	256
Comando snoop e IPsec	257
17 Intercambio de claves de Internet (descripción general)	259
Gestión de claves con IKE	259
Negociación de claves IKE	260
Terminología de claves IKE	260
Intercambio de IKE de fase 1	260
Intercambio de IKE de fase 2	261
Opciones de configuración de IKE	261
IKE con autenticación de claves previamente compartidas	262
IKE con certificados de claves públicas	262
Archivos y utilidades IKE	263

18 Configuración de IKE (tareas)	265
Visualización de información IKE	265
▼ Cómo visualizar grupos y algoritmos disponibles para intercambios IKE de fase 1	265
Configuración de IKE (mapa de tareas)	267
Configuración de IKE con claves previamente compartidas (mapa de tareas)	268
Configuración de IKE con claves previamente compartidas	268
▼ Cómo configurar IKE con claves previamente compartidas	268
▼ Cómo actualizar IKE para un sistema equivalente nuevo	271
Configuración de IKE con certificados de clave pública (mapa de tareas)	273
Configuración de IKE con certificados de clave pública	274
▼ Cómo configurar IKE con certificados de clave pública autofirmados	274
▼ Cómo configurar IKE con certificados firmados por una autoridad de certificación	279
▼ Cómo generar y almacenar certificados de clave pública en el hardware	284
▼ Cómo administrar una lista de revocación de certificados	288
Configuración de IKE para sistemas portátiles (mapa de tareas)	290
Configuración de IKE para sistemas portátiles	291
▼ Cómo configurar IKE para sistemas remotos	291
Configuración de IKE para buscar el hardware conectado	298
▼ Cómo configurar IKE para buscar la placa Sun Crypto Accelerator 6000	298
19 Intercambio de claves de Internet (referencia)	301
Servicio IKE	301
Daemon IKE	302
Archivo de configuración IKE	303
Comando ikeadm	303
Archivos de claves IKE previamente compartidas	304
Comandos y bases de datos de claves públicas IKE	304
Comando ikecert tokens	305
Comando ikecert certlocal	305
Comando ikecert certdb	306
Comando ikecert certrldb	307
Directorio /etc/inet/ike/publickeys	307
Directorio /etc/inet/secret/ike.privatekeys	307
Directorio /etc/inet/ike/crls	307

20 Filtro IP en Oracle Solaris (descripción general)	309
Introducción al filtro IP	309
Fuentes de información para el filtro IP de código abierto	310
Procesamiento de paquetes del filtro IP	310
Directrices para utilizar el filtro IP	313
Uso de archivos de configuración del filtro IP	314
Uso de conjuntos de reglas de filtro IP	314
Uso de la función de filtros de paquetes del filtro IP	314
Uso de la función NAT del filtro IP	317
Uso de la función de agrupaciones de direcciones del filtro IP	318
Enlaces de filtros de paquetes	320
IPv6 para filtro IP	320
Páginas del comando man del filtro IP	321
21 Filtro IP (tareas)	323
Configuración de filtro IP	323
▼ Cómo habilitar el filtro IP	324
▼ Cómo rehabilitar el filtro IP	325
▼ Cómo activar los filtros en bucle	326
Desactivación y deshabilitación de filtro IP	327
▼ Cómo desactivar los filtros de paquetes	327
▼ Cómo desactivar NAT	328
▼ Cómo desactivar los filtros de paquetes	328
Cómo trabajar con conjuntos de reglas del filtro IP	329
Gestión de conjunto de reglas de filtro de paquetes para filtro IP	330
Gestión de reglas NAT para filtro IP	337
Gestión de agrupaciones de direcciones para el filtro IP	339
Cómo visualizar las estadísticas e información sobre el filtro IP	341
▼ Cómo ver las tablas de estado para el filtro IP	342
▼ Cómo ver las tablas de estado para el filtro IP	342
▼ Cómo visualizar las estadísticas de NAT para el filtro IP	343
▼ Cómo visualizar las estadísticas de la agrupación de direcciones para el filtro IP	344
Cómo trabajar con archivos de registro para el filtro IP	344
▼ Cómo configurar un archivo de registro para el filtro IP	345
▼ Cómo visualizar los archivos de registro del filtro IP	346

▼ Cómo vaciar el archivo de registro de paquetes	347
▼ Cómo guardar paquetes registrados en un archivo	347
Creación y edición de archivos de configuración del filtro IP	348
▼ Cómo crear un archivo de configuración para el filtro IP	349
Ejemplos de archivos de configuración del filtro IP	350
Parte IV Rendimiento de redes	355
22 Descripción general del equilibrador de carga integrado	357
Terminología del ILB	358
Funciones del ILB	360
Modos de funcionamiento del ILB	360
Algoritmos del ILB	361
Interfaz de línea de comandos del ILB	361
Función de supervisión de servidores del ILB	362
Funciones adicionales del ILB	363
Procesos del ILB	365
Directrices para utilizar el ILB	366
ILB y la utilidad de gestión de servicios	366
Comandos y subcomandos del ILB	366
23 Configuración del equilibrador de carga integrado (tareas)	369
Instalación del equilibrador de carga integrado	369
Habilitación y deshabilitación del ILB	370
▼ Cómo habilitar el ILB	370
▼ Cómo deshabilitar el ILB	371
Configuración del ILB	371
Topologías DSR, NAT parcial y NAT completa	371
Topología NAT parcial de equilibrio de carga	373
Topología NAT completa de equilibrio de carga	374
Configuración del ILB de alta disponibilidad (únicamente modo activo-pasivo)	375
Configuración del ILB de alta disponibilidad mediante la topología DSR	375
Configuración del ILB de alta disponibilidad mediante la topología NAT parcial	377
Configuración de la autorización del usuario para los subcomandos de configuración del ILB	380

Administración de grupos de servidores del ILB	381
▼ Cómo crear un grupo de servidores	381
▼ Cómo suprimir un grupo de servidores	381
Visualización de un grupo de servidores	382
Administración de servidores back-end en el ILB	382
▼ Cómo agregar un servidor back-end a un grupo de servidores	382
▼ Cómo eliminar un servidor back-end de un grupo de servidores	383
▼ Cómo volver a habilitar o deshabilitar un servidor back-end	384
Administración de comprobaciones de estado en el ILB	385
Creación de una comprobación de estado	385
Detalles de la prueba proporcionada por el usuario	386
Supresión de una comprobación de estado	387
Enumeración de comprobaciones de estado	387
Visualización de resultados de comprobaciones de estado	387
Administración de reglas del ILB	388
▼ Cómo crear una regla	388
Supresión de una regla	389
Enumeración de reglas	389
Visualización de estadísticas del ILB	389
Obtención de información estadística mediante el subcomando <code>show-statistics</code>	390
Visualización de la tabla de conexiones NAT	390
Visualización de la tabla de asignación de persistencia de sesión	391
Uso de los subcomandos <code>import</code> y <code>export</code>	391
 24 Protocolo de redundancia de enrutador virtual (descripción general)	393
Terminología de VRRP	394
Descripción general de la arquitectura de VRRP	395
Enrutador VRRP	395
Procesos de VRRP	395
Limitaciones de VRRP	397
Compatibilidad con zonas de IP exclusiva	397
Funcionamiento junto con otras funciones de red	398
 25 Configuración VRRP (tareas)	399
Creación de una VNIC de VRRP	400

Configuración vrrpadm	400
Subcomando vrrpadm create-router	400
Subcomando vrrpadm modify-router	401
Subcomando vrrpadm delete-router	401
Subcomando vrrpadm disable-router	401
Subcomando vrrpadm enable-router	401
Subcomando vrrpadm show-router	401
Consideraciones de seguridad	403
26 Implementación del control de congestión	405
Control de congestión y congestión de red	405
▼ Cómo implementar el control de congestión de redes TCP y SCTP	406
Parte V Calidad de servicio IP (IPQoS)	409
27 Introducción a IPQoS (descripción general)	411
Conceptos básicos de IPQoS	411
¿Qué son los servicios diferenciados?	411
Funciones de IPQoS	412
Dónde obtener más información sobre la teoría y práctica de la calidad del servicio	412
Ofrecimiento de calidad de servicio con IPQoS	414
Utilización de acuerdos de nivel de servicio	414
Garantía de calidad de servicio para una organización específica	414
Introducción a la política de calidad de servicio	414
Mejoramiento de la eficacia de la red con IPQoS	415
Cómo afecta el ancho de banda al tráfico de red	415
Utilización de clases de servicio para priorizar el tráfico	416
Modelo de servicios diferenciados	417
Descripción general del clasificador (ipgpc)	417
Descripción general de medidor (tokenmt y tswtclmt)	418
Descripción general de marcadores (dscpmk y dlcosmk)	419
Descripción general del control de flujo (flowacct)	419
Cómo fluye el tráfico a través de los módulos IPQoS	420
Reenvío del tráfico en una red con IPQoS	422

Punto de código DS	422
Comportamientos por salto	422
28 Planificación para una red con IPQoS (tareas)	427
Planificación de configuración IPQoS general (mapa de tareas)	427
Planificación de la distribución de la red Diffserv	428
Estrategias de hardware para la red Diffserv	428
Distribuciones de red IPQoS	429
Planificación de la política de calidad de servicio	431
Ayudas para planificar la política QoS	431
Planificación de la política QoS (mapa de tareas)	432
▼ Cómo preparar una red para IPQoS	433
▼ Cómo definir las clases de la política QoS	434
Definición de filtros	436
▼ Cómo definir filtros en la política QoS	437
▼ Cómo planificar el control de flujo	438
▼ Cómo planificar el comportamiento de reenvío	441
▼ Cómo planificar la recopilación de datos de flujo	443
Introducción al ejemplo de configuración IPQoS	444
Distribución IPQoS	444
29 Creación del archivo de configuración IPQoS (tareas)	447
Definición de una política QoS en el archivo de configuración IPQoS (mapa de tareas)	447
Herramientas para crear una política QoS	449
Archivo de configuración IPQoS básico	449
Creación de archivos de configuración IPQoS para servidores web	450
▼ Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico	452
▼ Cómo definir filtros en el archivo de configuración IPQoS	454
▼ Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS	456
▼ Cómo activar el control para una clase en el archivo de configuración IPQoS	459
▼ Cómo crear un archivo de configuración IPQoS para un servidor web "best-effort"	460
Creación un archivo de configuración IPQoS para un servidor de aplicaciones	463
▼ Cómo definir el archivo de configuración IPQoS para un servidor de aplicaciones	465
▼ Cómo configurar el reenvío para el tráfico de aplicaciones en el archivo de configuración IPQoS	467

▼ Cómo configurar el control de flujo en el archivo de configuración IPQoS	469
Suministro de servicios diferenciados en un enrutador	472
▼ Cómo configurar un enrutador en una red con IPQoS	473
30 Inicio y mantenimiento de IPQoS (tareas)	475
Administración IPQoS (mapa de tareas)	475
Aplicación de una configuración IPQoS	476
▼ Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS	476
▼ Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia	477
Activación del registro sys log para mensajes IPQoS	477
▼ Cómo activar el registro de mensajes IPQoS durante el inicio	477
Resolución de problemas con mensajes de error IPQoS	478
31 Uso de control de flujo y recopilación de estadísticas (tareas)	483
Establecimiento del control de flujo (mapa de tareas)	483
Registro de información sobre flujos de tráfico	484
▼ Cómo crear un archivo para datos de control de flujo	484
Recopilación de estadísticas	486
32 IPQoS detallado (referencia)	489
Arquitectura IPQoS y el modelo Diffserv	489
Módulo clasificador	489
Módulo medidor	492
Módulo marcador	495
Módulo flowacct	499
Archivo de configuración IPQoS	502
Instrucción action	503
Definiciones de módulo	504
Cláusula class	504
Cláusula filter	505
Cláusula params	505
Herramienta de configuración ipqosconf	506

Glosario 507

Índice 517

Prefacio

Bienvenido a Administración de Oracle Solaris: servicios IP para Oracle Solaris. Este manual forma parte de un conjunto de 14 volúmenes que abarca una gran cantidad de información sobre la administración de sistemas Oracle Solaris. En este manual, se da por sentado que ya instaló Oracle Solaris. Debe estar listo para configurar la red o para configurar el software de red que se necesite.

Nota – Esta versión de Oracle Solaris admite sistemas que utilizan las familias de arquitecturas de procesadores SPARC y x86. Los sistemas admitidos se muestran en las [Listas de compatibilidad de hardware del sistema operativo Oracle Solaris](#). Este documento indica las diferencias de implementación entre los tipos de plataforma.

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>Inicio y cierre de Oracle Solaris en plataformas SPARC</i>	Inicio y cierre de un sistema, gestión de servicios de inicio, modificación del comportamiento de inicio, inicio desde ZFS, gestión del archivo de inicio y resolución de problemas de inicio en plataformas SPARC
<i>Inicio y cierre de Oracle Solaris en plataformas x86</i>	Inicio y cierre de un sistema, gestión de servicios de inicio, modificación del comportamiento de inicio, inicio desde ZFS, gestión del archivo de inicio y resolución de problemas de inicio en plataformas x86
<i>Administración de Oracle Solaris: tareas comunes</i>	Uso de los comandos de Oracle Solaris, inicio y cierre de un sistema, gestión de grupos y cuentas de usuario, gestión de servicios, errores de hardware, información del sistema, recursos del sistema y rendimiento del sistema, gestión de software, impresión, consola y terminales, y resolución de problemas del sistema y de software
<i>Administración de Oracle Solaris: dispositivos y sistemas de archivos</i>	Medios extraíbles, discos y dispositivos, sistemas de archivos y copias de seguridad y restauración de datos

Título de manual	Temas
<i>Administración de Oracle Solaris: servicios IP</i>	Administración de redes TCP/IP, administración de direcciones IPv4 e IPv6, DHCP, IPsec, IKE, IP Filter e IPQoS
<i>Oracle Solaris Administration: Naming and Directory Services</i>	Servicios de directorios y nombres DNS, NIS y LDAP, incluida la transición de NIS a LDAP
<i>Administración de Oracle Solaris: interfaces y virtualización de redes</i>	Configuración automática y manual de interfaz IP, incluida la inalámbrica WiFi; administración de puentes, VLAN, agregaciones, LLDP e IPMP; gestión de recursos y NIC virtuales
<i>Oracle Administración Solaris: 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>Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos</i>	Funciones de gestión de recursos, que permiten controlar la manera en que las aplicaciones utilizan los recursos disponibles del sistema; tecnología de partición del software Oracle Solaris Zones, que virtualiza los servicios del sistema operativo para crear un entorno aislado para ejecutar aplicaciones; y Oracle Solaris 10 Zones, que aloja entornos de Oracle Solaris 10 que se ejecutan en el núcleo de Oracle Solaris 11
<i>Administración de Oracle Solaris: servicios de seguridad</i>	Auditoría, gestión de dispositivos, seguridad de archivos, BART, servicios Kerberos, PAM, estructura criptográfica, gestión de claves, privilegios, RBAC, SASL, Secure Shell y análisis de virus
<i>Oracle Solaris Administration: SMB and Windows Interoperability</i>	Servicio SMB, que permite configurar un sistema Oracle Solaris para que los recursos compartidos de SMB estén disponibles para clientes SMB; cliente SMB, que permite acceder a recursos compartidos de SMB; y servicios nativos de asignación de identidad, que permiten asignar identidades de grupos y usuarios entre sistemas Oracle Solaris y sistemas Windows
<i>Administración de Oracle Solaris: sistemas de archivos 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
<i>Configuración y administración de Trusted Extensions</i>	Tareas de instalación, configuración y administración del sistema específicas de Trusted Extensions
<i>Directrices de seguridad de Oracle Solaris 11</i>	Protección de un sistema Oracle Solaris, además de escenarios de uso para funciones de seguridad, como zonas, ZFS y Trusted Extensions

Título de manual	Temas
<i>Transición de Oracle Solaris 10 a Oracle Solaris 11</i>	Proporciona información sobre la administración del sistema y ejemplos para la transición de Oracle Solaris 10 a Oracle Solaris 11 en las áreas de instalación y gestión de dispositivos, discos y sistemas de archivos, gestión de software, redes, gestión de sistemas, seguridad, virtualización, funciones de escritorio, gestión de cuentas de usuario y entornos de usuarios

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>machine_name% 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

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 implementación de red

En este capítulo, se describen brevemente las distintas consideraciones que debe tener en cuenta al planificar la configuración de red. Estas cuestiones lo ayudarán a implementar la red de una manera organizada y rentable. Tenga en cuenta que los detalles sobre la planificación de la red están fuera del alcance de este manual. Únicamente se proporcionan instrucciones generales.

En este manual, se da por sentado que usted está familiarizado con los conceptos y la terminología básicos. Consulte los siguientes recursos para ver una introducción a estos conceptos básicos:

- Para obtener una descripción general del conjunto de protocolos TCP/IP y su implementación del modelo de interconexión de sistemas abiertos (OSI), consulte el [Capítulo 1, “Conjunto de protocolos TCP/IP de Oracle Solaris \(descripción general\)” de *Guía de administración del sistema: servicios IP*](#).
- Para obtener una descripción breve de cómo se implementa el conjunto de protocolos TCP/IP en esta versión de Oracle Solaris, consulte el [Capítulo 1, “Descripción general de la pila de red” de *Administración de Oracle Solaris: interfaces y virtualización de redes*](#).

En las secciones pertinentes que siguen, se proporcionan más referencias a introducciones y descripciones generales.

Planificación de la red (mapa de tareas)

En la siguiente tabla, se enumeran las distintas tareas para planificar la configuración de red.

Tarea	Descripción	Para obtener información
Identificar los requisitos de hardware de la topología de red planificada.	Determine los tipos de equipo que necesita para el sitio de red.	“Determinación del hardware de red” en la página 26 Para obtener información sobre un tipo de equipo específico, consulte la documentación del fabricante del equipo.
Determinar el tipo de direcciones IP que se utilizarán y obtener direcciones IP registradas.	Seleccione si está implementando una red puramente IPv4, una red IPv6 o una red que utiliza ambos tipos de direcciones IP. Obtenga direcciones IP exclusivas para comunicarse con redes públicas en Internet.	“Cómo decidir el formato de las direcciones IP para la red” en la página 27 “Cómo obtener el número de IP de la red” en la página 29
Determinar un esquema de nomenclatura para identificar los hosts de la red y también el servicio de nombres que se utilizará.	Cree una lista de nombres para asignar a los sistemas de la red y decida si se utilizarán NIS, LDAP, DNS o las bases de datos de red en el directorio /etc local.	“Administración de nombres de host” en la página 30 “Selección de un servicio de nombres y de directorios” en la página 31
Si es necesario, establecer subdivisiones administrativas y diseñar una estrategia para subredes.	Decida si el sitio requiere la división de la red en subredes para prestar servicio a subdivisiones administrativas.	“Uso de subredes” en la página 32
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.	“Planificación de enrutadores en la red” de Guía de administración del sistema: servicios IP
Decidir si se deben crear redes virtuales en el esquema de configuración de red general.	Es posible que deba crear redes virtuales dentro de un sistema para reducir el espacio utilizado por el hardware en la red.	Parte III, “Virtualización de la red y gestión de los recursos” de <i>Administración de Oracle Solaris: interfaces y virtualización de redes</i> .

Determinación del hardware de red

El número de sistemas que espera admitir afecta 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*.

A continuación, se presentan algunas de las decisiones de planificación que debe tomar relacionadas con el hardware:

- La topología de red, el diseño y las conexiones del hardware de red
- El tipo y número de sistemas host que admite la red, incluidos los servidores que pueden ser necesarios
- Los dispositivos de red que se instalarán en estos sistemas
- El tipo de medios de red que se utilizarán, como Ethernet, etc.
- Si necesita puentes o enrutadores que extiendan este medio o conecten la red local a redes externas

Nota – Para obtener una descripción de cómo funcionan los enrutadores, consulte “Planificación de enrutadores en la red” de *Guía de administración del sistema: servicios IP*. Para obtener una descripción general de los puentes, consulte “Descripción general sobre puentes” de *Administración de Oracle Solaris: interfaces y virtualización de redes*.

Cómo decidir el formato de las direcciones IP para la red

Al planificar el esquema de direcciones de la red, debe tener 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 varias tarjetas de interfaz de red (NIC) con sus propias direcciones IP individuales
- Si se utilizarán direcciones privadas en la red
- Si habrá un servidor DHCP que administre las agrupaciones de direcciones IPv4

Brevemente, los tipos de direcciones IP incluyen los siguientes:

Direcciones IPv4

Estas direcciones de 32 bits son el formato original de direcciones IP para TCP/IP.

Para obtener una descripción general de las direcciones IPv4 basadas en clase, consulte los siguientes recursos:

- “Cómo diseñar un esquema de direcciones IPv4” de *Guía de administración del sistema: servicios IP*
- Internet Protocol DARPA Internet Program Protocol Specification (<http://tools.ietf.org/html/rfc791>) (Especificación del protocolo de Internet de DARPA Internet Program)

IETF desarrolló direcciones de *enrutamiento entre dominios sin clase (CIDR)* como una solución de corto a mediano plazo para la escasez de direcciones IPv4 y la capacidad limitada de las tablas de enrutamiento de Internet globales.

Para obtener más información, consulte los siguientes recursos:

- “Cómo diseñar un esquema de direcciones IPv4 CIDR” de *Guía de administración del sistema: servicios IP*
- Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan (<http://tools.ietf.org/html/rfc4632>) (Enrutamiento entre dominios sin clase [CIDR]: plan de agregación y asignación de direcciones de Internet)

En la siguiente tabla, se proporcionan las subredes en formato de notación CIDR y en formato decimal con punto.

TABLA 1-1 Prefijos CIDR y sus equivalentes decimales

Prefijo de red CIDR	Equivalente de subred decimal con punto	Direcciones IP disponibles
/19	255.255.224.0	8,192
/20	255.255.240.0	4,096
/21	255.255.248.0	2,048
/22	255.255.252.0	1,024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32

Direcciones DHCP

El protocolo de configuración dinámica de sistemas (DHCP, Dynamic Host Configuration Protocol) 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 obtener más información, consulte el [Capítulo 10, “Acerca de DHCP \(descripción general\)”](#).

Direcciones IPv6

Las direcciones IPv6 de 128 bits proporcionan un espacio de direcciones más grande que el que está disponible con IPv4. Al igual que con las direcciones IPv4 en formato CIDR, las direcciones IPv6 no tienen clase y utilizan prefijos para designar la parte de la dirección que define la red del sitio.

Para obtener más información sobre las direcciones IPv6, consulte los siguientes recursos:

- “Descripción general de las direcciones IPv6” de *Guía de administración del sistema: servicios IP*
- [Internet Protocol, Version 6 \(IPv6\) Specification \(http://tools.ietf.org/html/rc2460\)](http://tools.ietf.org/html/rc2460) (Especificación del protocolo de Internet, versión 6 [IPv6])

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. Las direcciones privadas se utilizan para tráfico de red dentro de una red privada. Estas direcciones también se utilizan en la documentación.

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

Rango 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

Para las direcciones IPv6, el prefijo `2001:db8::/32` es un prefijo IPv6 especial que se utiliza específicamente para ejemplos 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*.

Para habilitar la red privada para que se comunique con redes externas en Internet, debe obtener un número de IP registrado para su red de la organización pertinente. 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).

Entidades de denominación en la red

Los protocolos TCP/IP localizan un sistema en una red utilizando su dirección IP. Sin embargo, un nombre de host le permite identificar sistemas más fácilmente que las direcciones IP. Los protocolos TCP/IP (y Oracle Solaris) requieren tanto la dirección IP como el nombre de host para identificar un sistema de forma exclusiva.

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

Planifique un esquema de nomenclatura para los sistemas que compondrán la red. Para los sistemas que funcionan como servidores y que tienen varias NIC, se debe proporcionar al menos un nombre de host asociado con la dirección IP de su interfaz de red principal.

No puede haber dos máquinas en la red que tengan el mismo nombre de host. Por lo tanto, cada nombre de host debe ser exclusivo para cada sistema. Sin embargo, un host o un sistema con un nombre exclusivo asignado pueden tener varias 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

En Oracle Solaris, puede seleccionar entre tres tipos de servicios de nombres: archivos locales, NIS y DNS. Los servicios de nombres conservan información crítica sobre las máquinas de una red, como los nombres de host, las direcciones IP, las direcciones Ethernet, etc. También puede utilizar el servicio de directorios LDAP además del servicio de nombres o en lugar de él. Para ver una introducción a los servicios de nombres en Oracle Solaris, consulte la [Parte I, “About Naming and Directory Services”](#) de *Oracle Solaris Administration: Naming and Directory Services*.

Durante la instalación del sistema operativo, proporcione el nombre de host y la dirección IP del sistema autónomo, cliente o de servidor. El programa de instalación agrega esta información a la base de datos `hosts` para que el servicio de red la utilice al prestar servicio a la red.

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.

Para un servicio de nombres, puede seleccionar una de las opciones siguientes:

- NIS o DNS. Los servicios de nombres NIS y DNS conservan bases de datos de red en varios servidores de la red. En *Oracle Solaris Administration: Naming and Directory Services* se describen estos servicios de nombres y se explica cómo configurar las bases de datos. Asimismo, la guía explica de forma pormenorizada los conceptos de "espacio de nombres" y "dominio administrativo".
- Archivos locales. Si no desea implementar 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 en InterNIC. Si tiene previsto utilizar DNS, también debe registrar su propio nombre de dominio en 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 existentes de nivel superior, como .com, .org, .edu, .gov, etc.

Uso de subredes

El uso de subredes está relacionado con la necesidad de contar con subdivisiones administrativas para abordar cuestiones de tamaño y control. Cuantos mas hosts y servidores haya en una red, más compleja será la tarea de administración. Al crear divisiones administrativas y utilizar subredes, la gestión de una red compleja resulta más fácil. La decisión de configurar subdivisiones administrativas para su red la determinan los factores siguientes:

- **Tamaño de la red**

Las subredes también son útiles incluso en una red relativamente pequeña cuyas subdivisiones están ubicadas a lo largo de una amplia área geográfica.

- **Necesidades comunes compartidas por grupos de usuarios**

Por ejemplo, posiblemente tenga una red que esté limitada a un único edificio y que admita un número relativamente pequeño de máquinas. 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.

Para obtener una descripción general, consulte “¿Qué son las subredes?” de *Guía de administración del sistema: servicios IP*.

Implementación de redes virtuales

Esta versión de Oracle Solaris admite la creación de redes virtuales en una única red al configurar zonas y tarjetas de red virtual (VNIC). Las VNIC son interfaces de red que se crean además de las NIC. La combinación de zonas y VNIC es una manera eficaz de consolidar un centro de datos enorme que contiene un gran número de sistemas físicos en menos sistemas. Para obtener más información sobre la red virtual, consulte la [Parte III, “Virtualización de la red y gestión de los recursos” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

Consideraciones para el uso de direcciones IPv6

Este capítulo complementa al [Capítulo 1, “Planificación de la implementación de red”](#) y describe consideraciones adicionales que deben tenerse en cuenta al decidir utilizar direcciones IPv6 en la red.

Si tiene previsto utilizar direcciones IPv6 además de direcciones IPv4, asegúrese de que el ISP actual admita ambos tipos de direcciones. De lo contrario, deberá encontrar un ISP independiente para admitir direcciones IPv6.

Para ver una introducción a los conceptos relativos a IPv6, consulte los recursos siguientes:

- “Descripción general de las direcciones IPv6” de *Guía de administración del sistema: servicios IP*
- [Internet Protocol, Version 6 \(IPv6\) Specification \(http://tools.ietf.org/html/rc2460\)](http://tools.ietf.org/html/rc2460) (Especificación del protocolo de Internet, versión 6 [IPv6])

Planificación de IPv6 (mapa de tareas)

En la tabla siguiente, se enumeran diferentes consideraciones que deben tenerse en cuenta al implementar IPv6 en la red.

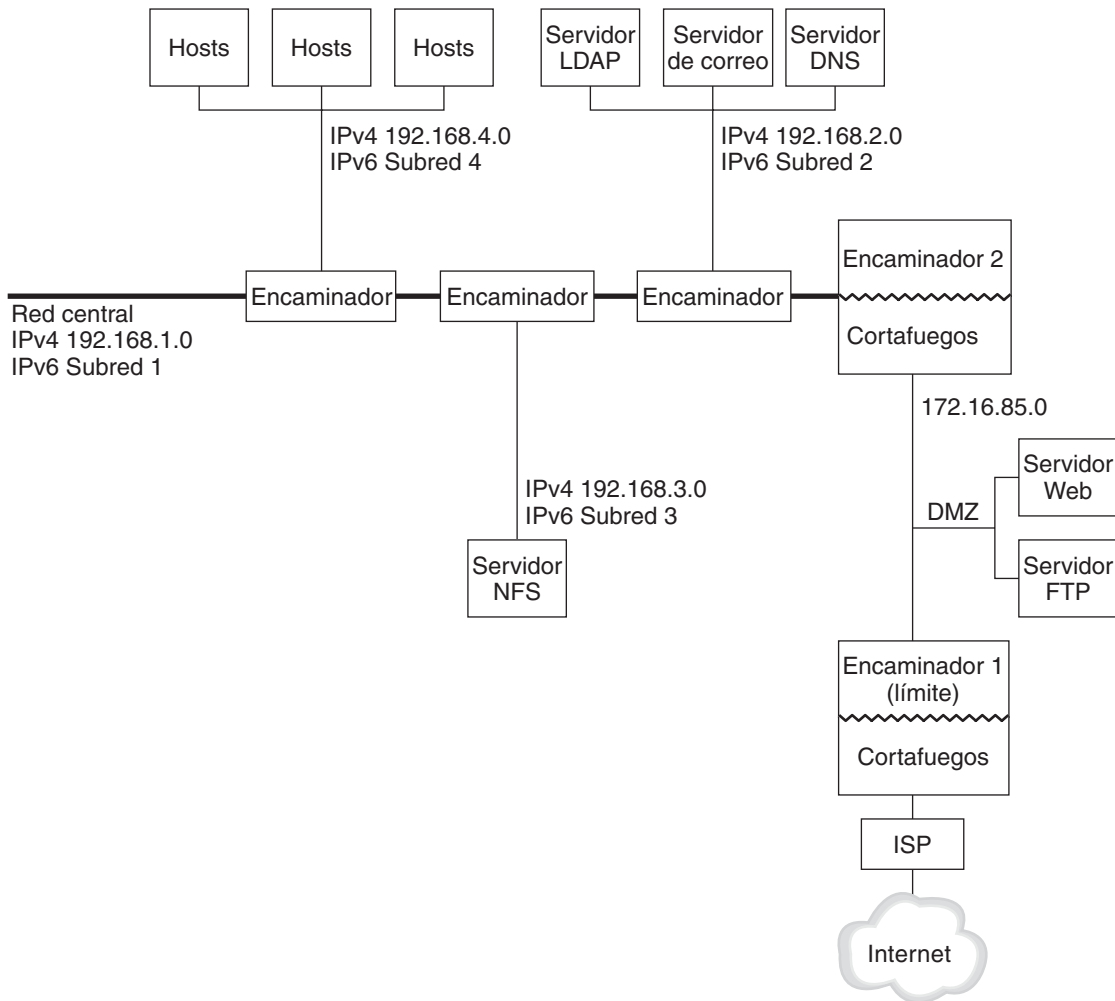
Tarea	Descripción	Para obtener instrucciones
Preparar el hardware para admitir IPv6.	Compruebe que el hardware se pueda actualizar a IPv6.	“Cómo garantizar la compatibilidad de hardware para IPv6” en la página 36
Asegurarse de que las aplicaciones estén preparadas para funcionar con IPv6.	Verifique que las aplicaciones puedan funcionar en un entorno IPv6.	“Configuración de servicios de red para admitir IPv6” en la página 39

Tarea	Descripción	Para obtener instrucciones
Diseñar un plan para el uso de túneles.	Establezca los enrutadores que deben ejecutar túneles a otras subredes o redes externas.	“Planificación para el uso de túneles en la red” en la página 41
Planificar cómo proteger las redes y desarrollar una política de seguridad IPv6.	Por motivos de seguridad, se precisa un plan de direcciones para la DMZ y sus entidades antes de configurar IPv6. Decida cómo implementará la seguridad, por ejemplo, con un filtro IP, una arquitectura de seguridad IP (IPsec), el intercambio de claves de Internet (IKE) y otras funciones de seguridad de esta versión.	“Aspectos relacionados con la seguridad en la implementación de IPv6” en la página 41 Parte III
Crear un plan de direcciones para sistemas de la red.	Se debe planificar la dirección de servidores, enrutadores y hosts antes de configurar IPv6. Este paso implica obtener un prefijo de sitio para la red, además de planificar subredes IPv6, si es necesario.	“Creación de un plan de direcciones IPv6 para nodos” en la página 37

Situación hipotética de topología de red IPv6

Por lo general, IPv6 se utiliza en una topología de red mixta que también utiliza IPv4, como se muestra en la figura siguiente. Esta figura se utiliza como referencia en la descripción de las tareas de configuración de IPv6 de las secciones siguientes.

FIGURA 2-1 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 2–1](#), 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.

La pila doble de protocolos de Oracle Solaris permite operaciones simultáneas de IPv4 e IPv6. Puede ejecutar correctamente operaciones relacionadas con IPv4 durante la implementación de IPv6 en la red y después de esta implementación. Al implementar IPv6 en una red operativa que ya utiliza IPv4, asegúrese de no interrumpir las operaciones en curso.

En las secciones siguientes, se describen las áreas que debe tener en cuenta al prepararse para implementar IPv6.

Cómo garantizar la compatibilidad de hardware para IPv6

Consulte la documentación de los fabricantes para conocer la compatibilidad de IPv6 con los siguientes tipos de hardware:

- Enrutadores
- Cortafuegos
- Servidores
- Conmutadores

Nota – Todos los procedimientos de este manual suponen que los equipos, 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 141](#).

Para cada NIC de los servidores IPv6, configure manualmente la parte del ID de interfaz de la dirección IPv6, en lugar de obtener automáticamente el ID con el protocolo de descubrimiento de vecinos. De esta forma, si se reemplaza una NIC, se puede aplicar el mismo ID de interfaz a la

NIC de reemplazo. Es posible que un ID diferente generado automáticamente por el protocolo de descubrimiento de vecinos cause un comportamiento inesperado en el servidor.

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 37
- “Creación del esquema de numeración de IPv6” en la página 37

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. Para ver una introducción a los prefijos de sitio, consulte “Prefijos de IPv6” de *Guía de administración del sistema: servicios IP*.

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 141.

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>).

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 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 en la [Figura 2-1](#) 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 2-1](#), 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.

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 2-1](#). 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

Para ver una descripción más detallada de las subredes, consulte “¿Qué son las subredes?” de [Guía de administración del sistema: servicios IP](#)

Configuración 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 141](#).

▼ 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:

- Cortafuegos

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 41.](#)

- 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 40.](#)

- IPQoS

En un host, emplee las mismas directrices DiffServ que se usaban en IPv4. Para obtener más información, consulte [“Módulo clasificador” en la página 489.](#)

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 [Oracle Solaris Administration: Naming and Directory Services.](#)

- 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 para el uso de túneles en la 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 2–1](#) 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 conocer los procedimientos para la configuración de túneles, consulte “[Configuración de túneles \(mapa de tareas\)](#)” en la [página 126](#). Para obtener información conceptual relativa a los túneles, consulte “[Descripción general de túneles IP](#)” en la [página 117](#).

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 política 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 14, “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 17, “Intercambio de claves de Internet \(descripción general\)”](#).

Configuración de una red IPv4

La configuración de red se compone de dos etapas: ensamblado del hardware y configuración de los daemons, los archivos y los servicios que implementan el protocolo TCP/IP.

En este capítulo, se explica cómo configurar una red que implementa servicios y direcciones IPv4.

Muchas de las tareas de este capítulo se aplican a redes habilitadas tanto para IPv4 como para IPv6. Las tareas que son específicas para las redes IPv6, se incluyen en el [Capítulo 4](#), “Habilitación de IPv6 en una red”.

Nota – Antes de configurar TCP/IP, revise las distintas tareas de planificación que se enumeran en el [Capítulo 1](#), “Planificación de la implementación de red”. Si planea utilizar direcciones IPv6, consulte también el [Capítulo 2](#), “Consideraciones para el uso de direcciones IPv6”.

Este capítulo contiene la información siguiente:

- “Configuración de red (mapa de tareas)” en la página 43
- “Antes de comenzar la configuración de red” en la página 44
- “Configuración de los componentes del sistema en la red” en la página 45
- “Cómo agregar una subred a una red” en la página 68
- “Supervisión y modificación de los servicios de capa de transporte” en la página 70

Configuración de red (mapa de tareas)

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 las interfaces IP del sistema.	Asigna direcciones IP a las interfaces IP del sistema.	“Cómo configurar una interfaz IP” en la página 47
Configurar un sistema para el modo de archivos locales.	Edita archivos de configuración específicos en el directorio /etc del sistema y configura el servicio SMF nis/domain.	“Cómo configurar un sistema para el modo de archivos locales” en la página 53
Configurar un servidor de configuración de red.	Habilita el daemon in.tftp y edita otros archivos de configuración en el directorio /etc del sistema.	“Cómo instalar un servidor de configuración de red” en la página 55
Configurar un sistema para el modo de cliente de red.	Edita archivos de configuración en el directorio /etc del sistema.	“Cómo configurar un sistema para el modo de cliente de red” en la página 54
Especificar una estrategia de enrutamiento para el cliente de red.	Configura sistemas para que utilicen el enrutamiento estático o el enrutamiento dinámico.	“Cómo activar el enrutamiento estático en un host de interfaz única” en la página 65 y “Cómo habilitar el enrutamiento dinámico en un sistema de interfaz única” en la página 67

Antes de comenzar la configuración de red

En esta versión de Oracle Solaris, la configuración de red de un sistema se gestiona mediante un *perfil de configuración de red (NCP)* activo. Si el NCP activo del sistema es `automatic`, el sistema operativo gestiona automáticamente la configuración de red. Si el NCP activo es `DefaultFixed`, la configuración de red se realiza de forma manual con los comandos `dladm` y `ipadm`.

Nota – Los comandos `dladm` y `ipadm` no funcionan si el NCP activo es `Automatic`.

Para conocer los procedimientos para determinar el perfil activo del sistema y para cambiar a un NCP fijo, consulte [“Herramientas de configuración y perfiles” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

Para obtener más información sobre los NCP, consulte la [Parte I, “Conexión automática a la red \(NWAM, Network Auto-Magic\)” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

En este documento, los procedimientos suponen que el NCP activo de todos los sistemas de la red es `DefaultFixed`.

Configuración de los componentes del sistema en la red

Al configurar sistemas de red, necesita la siguiente información de configuración:

- Nombre de host de cada sistema.
- Dirección IP y máscara de red de cada sistema. Si la red está subdividida en subredes, debe contar con los números de subred y el esquema de direcciones IP que se aplicarán a los sistemas en cada subred, incluidas sus respectivas máscaras de red.
- Nombre de dominio al que pertenece cada sistema.
- Dirección del enrutador predeterminado.

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 obtener más información sobre los enrutadores y una lista de los protocolos de enrutamiento admitidos por Oracle Solaris, consulte [“Reenvío de paquetes y rutas en redes IPv4” de Guía de administración del sistema: servicios IP](#).

Nota – Puede configurar la red durante la instalación de Oracle Solaris. Para obtener instrucciones, consulte [Instalación de sistemas Oracle Solaris 11](#).

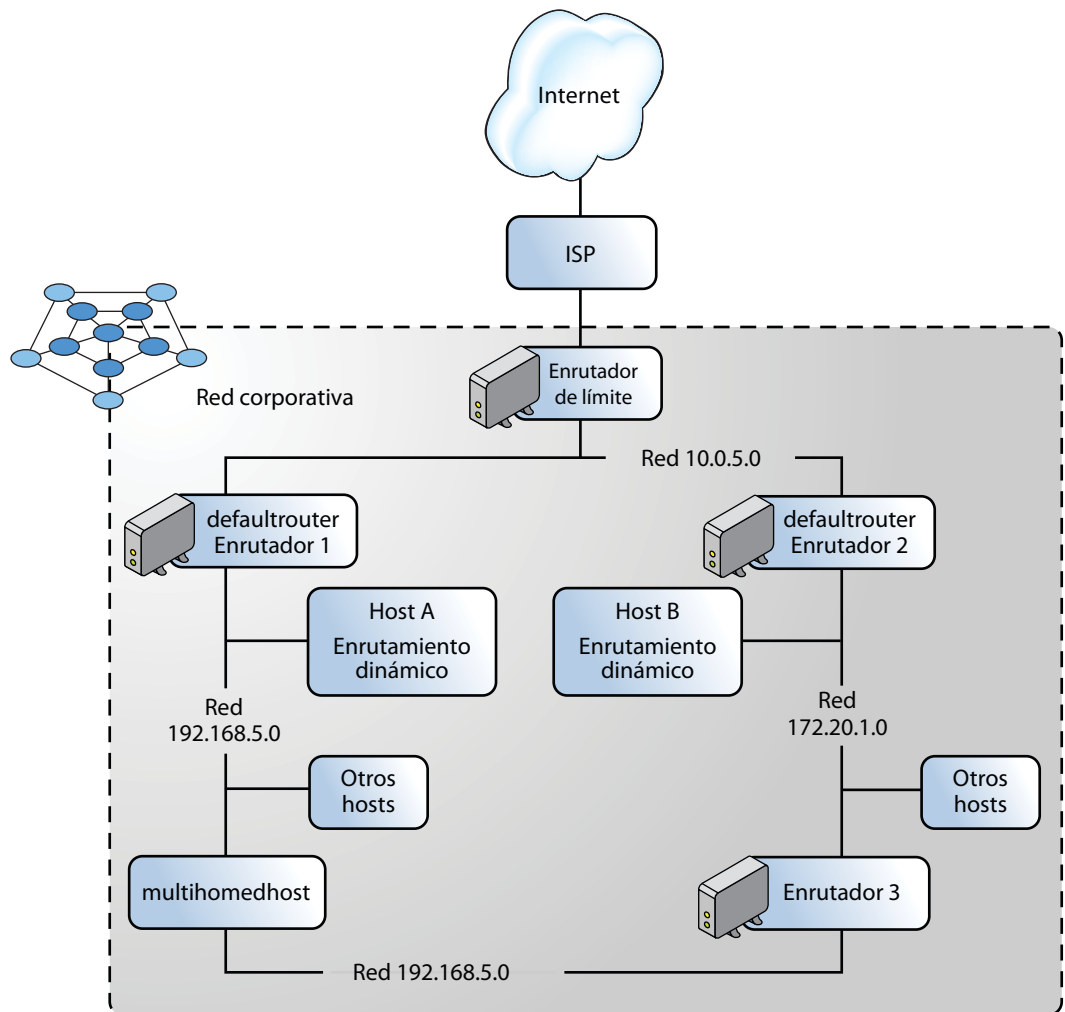
En este documento, los procedimientos suponen que la red se configura después de haber instalado el sistema operativo.

Utilice la [Figura 3–1](#) que se incluye en la siguiente sección como referencia para configurar los componentes del sistema de la red.

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)*.

FIGURA 3-1 Sistema autónomo con varios enrutadores IPv4



La [Figura 3-1](#) muestra un SA que está dividido en tres redes locales: 10.0.5.0, 172.20.1.0 y 192.168.5.0. La red se compone de los siguientes tipos de sistemas:

- Los enrutadores utilizan protocolos de enrutamiento para gestionar la forma en que los paquetes de red se dirigen o se enrutan desde el origen hasta los destinos dentro de la red local o en redes externas. Para obtener información sobre los protocolos de enrutamiento admitidos en Oracle Solaris, consulte [“Tablas de protocolos de enrutamiento en Oracle Solaris”](#) en la página 148.

A continuación, se describen los tipos de enrutadores:

- El *enrutador de límite* conecta la red local, como 10.0.5.0, externamente a un proveedor de servicios.
- Los *enrutadores predeterminados* gestionan el enrutamiento de paquetes en la red local, que, a su vez, puede incluir varias redes locales. Por ejemplo, en la [Figura 3-1](#), el enrutador 1 actúa como enrutador predeterminado para 192.168.5. En el mismo momento, el enrutador 1 también está conectado a la red interna 10.0.5.0. Las interfaces del enrutador 2 se conectan a las redes internas 10.0.5.0 y 172.20.1.0.
- Los *enrutadores de reenvío de paquetes* reenvían paquetes entre redes internas, pero no ejecutan protocolos de enrutamiento. En la [Figura 3-1](#), el enrutador 3 es un enrutador de reenvío de paquetes con conexiones a las redes 172.20.1 y 192.168.5.
- Sistemas cliente
 - Sistemas de host múltiple o sistemas que tienen varias NIC. En Oracle Solaris, de manera predeterminada, estos sistemas pueden reenviar paquetes a otros sistemas del mismo segmento de red.
 - Los sistemas de interfaz única confían en los enrutadores locales para reenviar paquetes y para recibir información de configuración.

▼ Cómo configurar una interfaz IP

El siguiente procedimiento proporciona un ejemplo de configuración básica de una interfaz IP.

Antes de empezar

Determine si desea renombrar los vínculos de datos en el sistema. Por lo general, se utilizan nombres genéricos que fueron asignados de manera predeterminada a los vínculos de datos. Para cambiar nombres de enlace, consulte [“Cómo cambiar el nombre de un enlace de datos” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#).

2 (Opcional) Muestre información acerca de los atributos físicos de los vínculos de datos en el sistema.

```
# dladm show-phys
```

Este comando muestra las tarjetas de red físicas instaladas en el sistema, además de algunas de sus propiedades. Para obtener más información sobre este comando, consulte [“Cómo visualizar información sobre atributos físicos de enlaces de datos” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

3 Muestre información acerca de los vínculos de datos en el sistema.

```
# dladm show-link
```

Este comando muestra los vínculos de datos y ciertas propiedades que fueron configuradas para ellas, incluidas las tarjetas físicas a partir de las cuales se crearon los vínculos.

4 Cree la interfaz IP.

ipadm create-interface-class interface

clase_interfaz Hace referencia a una de las tres clases de interfaces que puede crear:

- Interfaz IP. Esta clase de interfaz es la más común que puede crear al realizar la configuración de red. Para crear esta clase de interfaz, utilice el subcomando **create-ip**.
- Controlador de interfaz de red virtual STREAMS (interfaz VNI). Para crear esta clase de interfaz, utilice el subcomando **create-vni**. Para obtener información acerca de los dispositivos o interfaces de VNI, consulte la página del comando **man vni(7d)**.
- Interfaz IPMP. Esta interfaz se utiliza cuando configura grupos IPMP. Para crear esta clase de interfaz, utilice el subcomando **create-ipmp**. Para obtener más información acerca de los grupos IPMP, consulte el [Capítulo 14, “Introducción a IPMP” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

interfaz Hace referencia al nombre de la interfaz. El nombre es idéntico al nombre del vínculo desde el cual se está creando la interfaz.

Nota – Debe crear la interfaz IP antes de poder asignarle la dirección IP.

5 Configure la interfaz IP con una dirección IP válida.

La siguiente sintaxis asigna una dirección estática a una interfaz. Consulte la página del comando **man ipadm(1M)** para conocer otras opciones para la asignación de direcciones de IP.

ipadm create-addr -T address-type -a address/prefixlen addrobj

-T tipo_dirección Especifica el tipo de dirección IP que se asigna a la interfaz, que es uno de los siguientes: **static**, **dhcp** o **addrconf**. **Addrconf** hace referencia a direcciones IPv6 generadas automáticamente.

-a Especifica la dirección IP que se debe configurar en la interfaz. Puede especificar sólo una dirección local o una dirección local y una remota en el caso de la configuración de túnel. Por lo general, sólo asigna direcciones locales. En este caso, especifica la dirección directamente con la opción **-a**, como: **-a dirección**. La dirección se considera automáticamente una dirección local.

Si está configurando túneles, quizás deba proporcionar la dirección local del sistema y la dirección remota del sistema de destino. En este caso, debe especificar **local** y **remote** para distinguir las dos direcciones, de la

siguiente manera: `-a local=dir_local, remote=dir_remota`. Para obtener más información sobre la configuración de túneles, consulte el [Chapter 6, Configuración de túneles IP](#).

Si está usando una dirección IP numérica, use el formato *dirección/prefijo_largo* para direcciones en notación CIDR, por ejemplo, `1.2.3.4/24`. Vea la explicación para la opción *prefijo_largo*.

Opcionalmente, puede especificar un nombre de host para *dirección* en lugar de una dirección IP numérica. Es válido usar un nombre de host si hay una dirección IP numérica correspondiente definida para ese nombre de host en el archivo `/etc/hosts`. Si no hay ninguna dirección IP definida, entonces, el valor numérico se obtiene de modo exclusivo al usar el orden de resolución especificado para `host` en el servicio `name-service/switch`. Si existen varias entradas para un nombre de host determinado, se genera un error.

Nota – Durante el proceso de inicio, la creación de direcciones IP precede los servicios de nombres que se producen en línea. Por lo tanto debe asegurarse de que cualquier nombre de host que se use en la configuración de red debe estar definido en el archivo `/etc/hosts`.

/prefijo_largo

Especifica el largo del ID de red que es parte de la dirección IPv4 al usar la notación CIDR. En la dirección `12.34.56.78/24`, 24 es el *prefijo_largo*. Si no incluye *prefijo_largo*, la máscara de red se computa de acuerdo con la secuencia mostrada para `netmask` en el servicio `name-service/switch` o mediante la semántica de dirección con clases.

dir_obj

Especifica un identificador para la dirección IP única o el conjunto de direcciones que se usan en el sistema. La dirección puede ser de los tipos IPv4 o IPv6. El identificador usa el formato *interfaz/cadena_especificada por usuario*.

interfaz hace referencia a la interfaz IP a la que se asigna la dirección. La variable *interfaz* debe reflejar el nombre del vínculo de datos en el que está configurada la interfaz IP.

cadena_especificada por usuario hace referencia a una cadena de caracteres alfanuméricos que comienza con una letra del alfabeto y que tiene una longitud máxima de 32 caracteres. Además, puede hacer referencia a *dir_obj* en lugar de la dirección IP numérica cuando usa cualquier subcomando `ipadm` que gestiona direcciones en el sistema, como `ipadm show-addr` o `ipadm delete-addr`.

6 (Opcional) Muestre información acerca de la interfaz IP recientemente configurada.

Puede usar los siguientes comandos, según la información que quiera controlar:

- Muestre el estado general de la interfaz.

```
# ipadm show-if [interface]
```

Si no especifica la interfaz, entonces se muestra la información para todas las interfaces en el sistema.

- Muestre la información de dirección de la interfaz.

```
# ipadm show-addr [addrobj]
```

Si no especifica *dir_obj*, entonces se muestra la información para todos los objetos en la dirección en el sistema.

Para obtener más información acerca de la salida del subcomando `ipadm show-*`, consulte [“Supervisión de direcciones e interfaces IP” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

7 (Opcional) Agregue entradas para las direcciones IP en el archivo `/etc/hosts`.

Las entradas en este archivo están formadas por direcciones IP y los nombres de host correspondientes.

Nota – Este paso se aplica solamente si está configurando direcciones IP estáticas que usan nombres de host. Si está configurando direcciones DHCP, no es necesario que actualice el archivo `/etc/hosts`.

Ejemplo 3–1 Configuración de una interfaz de red con una dirección estática

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net3      Ethernet   up         100Mb      full        bge3

# dladm show-link
LINK      CLASS      MTU        STATE      BRIDGE      OVER
net3      phys       1500       up         --          --

# ipadm create-ip net3
# ipadm create-addr -T static -a 192.168.84.3/24 net3/v4static

# ipadm show-if
IFNAME    CLASS      STATE      ACTIVE      OVER
lo0       loopback   ok         yes         --
net3      ip         ok         yes         --

# ipadm show-addr
ADDROBJ    TYPE      STATE      ADDR
lo0/?      static    ok         127.0.0.1/8
net3/v4     static    ok         192.168.84.3/24
```

```
# vi /etc/hosts
# Internet host table
# 127.0.0.1      localhost
10.0.0.14       myhost
192.168.84.3    campus01
```

Tenga en cuenta que si `campus01` ya está definido en el archivo `/etc/hosts`, puede usar ese nombre de host al asignar la siguiente dirección:

```
# ipadm create-addr -T static -a campus01 net3/v4static
```

Ejemplo 3-2 Configuración automática de una interfaz de red con una dirección IP

Este ejemplo usa el mismo dispositivo de red que el ejemplo anterior pero configura la interfaz IP para recibir su dirección desde un servidor DHCP.

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net3      Ethernet   up         100Mb      full        bge3

# dladm show-link
LINK      CLASS      MTU        STATE      BRIDGE      OVER
net3      phys      1500       up         --          --

# ipadm create-ip net3

# ipadm create-addr -T dhcp net3/dhcp

# ipadm show-if
IFNAME    CLASS      STATE      ACTIVE      OVER
lo0       loopback   ok         yes         --
net3      ip         ok         yes         --

# ipadm show-addr net3/dhcp
ADDROBJ   TYPE      STATE      ADDR
net3/dhcp dhcp       ok         10.8.48.242/24

# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/?     static    ok         127.0.0.1/8
net3/dhcp dhcp       ok         10.8.48.242/24
```

Configuración de los modos de configuración del sistema

En esta sección, se describen los procedimientos para configurar un sistema para que se ejecute en *modo de archivos locales* o en *modo de cliente de red*. Al ejecutar el sistema en modo de archivos locales, el sistema obtiene toda la información de configuración TCP/IP de los

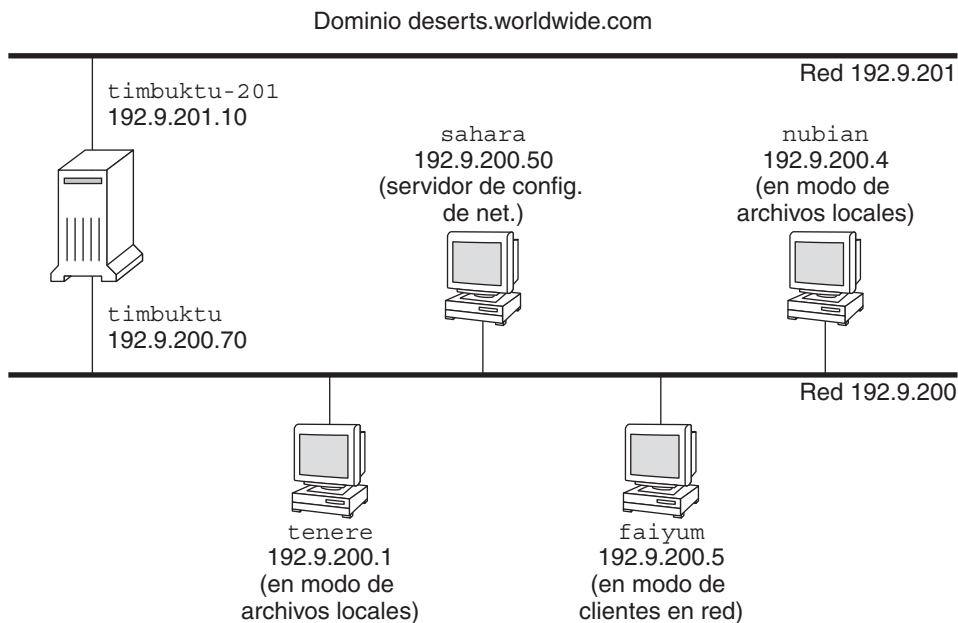
archivos que se encuentran en el directorio local. En el modo de cliente de red, la información de configuración se proporciona para todos los sistemas de la red mediante un servidor de configuración de red remota.

Por lo general, los servidores de la red se ejecutan en modo de archivos locales, como los siguientes:

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

Los clientes se pueden ejecutar en cualquiera de los dos modos. Por lo tanto, en la red puede existir una combinación de estos modos con los cuales se configuran distintos sistemas, como se muestran en la figura siguiente.

FIGURA 3-2 Sistemas en un escenario de topología de red IPv4



La [Figura 3-2](#) muestra los sistemas en una red 192.9.200.

- Todos los sistemas pertenecen al dominio organizativo `deserts.worldwide.com`.

- `sahara` es un servidor de configuración. Como servidor, se ejecuta en modo de archivos locales, donde la información de configuración TCP/IP se obtiene del disco local del sistema.

Nota – Si los clientes se configuran para ejecutarse en modo de cliente de red, se debe configurar al menos un servidor de configuración de red que proporcionará la información de configuración a esos clientes.

- `tenere`, `nubian` y `faiyum` son clientes en la red. `tenere` y `nubian` se ejecutan en modo de archivos locales. Independientemente del disco local de `faiyum`, el sistema se configura para funcionar en modo de cliente de red.
- `timbuktu` está configurado como enrutador y, por lo tanto, funciona en modo de archivos locales. El sistema incluye dos NIC, cada una con sus propias interfaces IP configuradas. La primera interfaz IP se denomina `timbuktu` y se conecta a la red 192.9.200. La segunda interfaz IP se denomina `timbuktu-201` y se conecta a la red 192.9.201.

Para obtener una descripción general más detallada de los dos modos de configuración, consulte [“Cómo determinar los modos de configuración de host” de Guía de administración del sistema: servicios IP](#).

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

Utilice este procedimiento para configurar cualquier sistema para que se ejecute en modo de archivos locales, como los que se enumeran en [“Sistemas que deben ejecutarse en modo de archivos locales” de Guía de administración del sistema: servicios IP](#).

1 Configure las interfaces IP del sistema con las direcciones IP asignadas.

Consulte [“Cómo configurar una interfaz IP” en la página 47](#) para conocer el procedimiento.

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

3 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.

Este archivo también debe incluir el nombre del enrutador predeterminado y la dirección IP del enrutador.

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

- b. (Optional) Si el sistema de archivos `/usr` está montado en NFS, agregue la dirección o las direcciones IP del servidor de archivos.
- 4 Especifique el dominio completo del sistema como una propiedad del servicio SMF `nis/domain`.
Por ejemplo, debe especificar `deserts.worldwide.com` como el valor para la propiedad `domainname` del servicio SMF `nis/domain`.
- 5 Escriba el nombre de enrutador en el archivo `/etc/defaultrouter`.
- 6 Agregue la información de la máscara de red, si corresponde.

Nota – Si está usando servicios DHCP, omita este paso.

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

Para crear entradas, utilice el formato *número_red, máscara_red*. 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 1–1](#). 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 consulta para las máscaras de red en la propiedad SMF del conmutador de modo que primero se busque en los archivos locales y, luego, refresque la instancia.

```
# svccfg -s name-service/switch setprop config/host = astring: "files nis"
# svccfg -s name-service/switch:default refresh
```

- 7 Reinicie el sistema.

▼ **Cómo configurar un sistema para el modo de cliente de red**

Realice el procedimiento siguiente en cada host que desee configurar en modo de cliente de red.

Antes de empezar

Los clientes de red reciben la información de configuración de los servidores de configuración de red. Por lo tanto, antes de configurar un sistema como un cliente de red, debe asegurarse de que haya como mínimo un servidor de configuración de red para la red.

- 1 **Conviértase en administrador.**

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#).

2 Configure las interfaces IP del sistema con las direcciones IP asignadas.

Consulte [“Cómo configurar una interfaz IP” en la página 47](#) para conocer el procedimiento.

3 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 de retorno.

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

4 Elimine los valores asignados a la propiedad `domainname` del servicio `SMF nis/domain`.**5 Asegúrese de que las rutas de búsqueda en el servicio `name-service/switch` del cliente reflejen los mismos requisitos de servicio para su red.****▼ Cómo instalar un servidor de configuración de red**

Puede encontrar información sobre cómo configurar servidores de instalación y servidores de inicio en [Instalación de sistemas Oracle Solaris 11](#).

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#).

2 Active el daemon `in.tftpd` de la siguiente manera:

a. Navegue hasta el directorio raíz (`/`) del servidor de configuración de red designado.

b. Cree el directorio `/tftpboot`:

```
# mkdir /tftpboot
```

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

c. Cree un vínculo simbólico al directorio.

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

3 Agregue la línea `tftp` en el archivo `/etc/inetd.conf`.

La línea debe decir lo 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`.

4 En la base de datos `/etc/hosts`, agregue los nombres de host y las direcciones IP de todos los clientes de la red.

- 5 En la base de datos `/etc/ethers`, cree entradas para cada sistema de la red que se ejecuta en modo de cliente de red.

Las entradas en esta base de datos tienen el formato siguiente:

```
MAC Address      host name      #comment
```

Para obtener más información, consulte la página del comando `man ethers(4)`.

- 6 En la base de datos `/etc/bootparams`, cree una entrada para cada sistema de la red que se ejecuta en modo de cliente de red.

Para obtener información sobre cómo editar esta base de datos, consulte la página del comando `man bootparams(4)`.

- 7 Convierta la entrada `/etc/inetd.conf` en un manifiesto de servicios de la utilidad de gestión de servicios (SMF) y habilite el servicio resultante.

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

- 8 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 6, “Gestión de servicios \(descripción general\)” de Administración de Oracle Solaris: tareas comunes](#).

Configuración de un enrutador IPv4

Un enrutador proporciona la interfaz entre dos o más redes. Por lo tanto, debe asignar un nombre y una dirección IP exclusivos 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 de interfaz única como enrutador si el sistema actúa como punto final en un enlace PPP, como se explica en [“Planificación de un enlace de PPP por marcación telefónica” de Oracle Administración Solaris: Servicios de red](#).

▼ Configuración de un enrutador IPv4

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

Antes de empezar

Después de que el enrutador se haya instalado físicamente en la red, configure el enrutador para que funcione en el modo de archivos locales, como se describe en [“Cómo configurar un sistema para el modo de archivos locales” en la página 53](#). Con esta configuración, los enrutadores se reiniciarán si el servidor de configuración de red no funciona.

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#).

2 Para cada NIC instalada en el sistema, configure las interfaces IP como se describe en [“Cómo configurar una interfaz IP” en la página 47](#).

Asegúrese de que cada interfaz IP esté configurada con la dirección IP de la red para la cual el sistema enrutará los paquetes. De esta manera, si el sistema presta servicio a las redes 192.168.5.0 y 10.0.5.0, se debe configurar una NIC para cada red.



Precaución – Si desea configurar enrutadores IPv4 para que utilicen DHCP, debe tener amplios conocimientos sobre la administración DHCP.

3 Agregue el nombre de host y la dirección IP de cada interfaz al archivo `/etc/inet/hosts`.

Por ejemplo, suponga que los nombres que asignó a las dos interfaces del enrutador 1 son `krakatoa` y `krakatoa-1`, respectivamente. Las entradas del archivo `/etc/inet/hosts` serían las siguientes:

```
192.168.5.1    krakatoa        #interface for network 192.168.5.0
10.0.5.1      krakatoa-1     #interface for network 10.0.5.0
```

4 Siga el resto de los pasos para configurar este enrutador para que se ejecute en modo de archivos locales.

Consulte [“Cómo configurar un sistema para el modo de archivos locales” en la página 53](#).

5 Si el enrutador está conectado a cualquier red con subredes, agregue el número de red y la máscara de red al archivo `/etc/inet/netmasks`.

Por ejemplo, para la notación de direcciones IPv4 tradicional, como `192.168.5.0`, debe escribir:

```
192.168.5.0    255.255.255.0
```

6 Habilite el reenvío de paquetes IPv4 en el enrutador.

```
# ipadm set-prop -p forwarding=on ipv4
```

7 (Opcional) Inicie un protocolo de enrutamiento.

Utilice una de las siguientes sintaxis del comando:

- `# routeadm -e ipv4-routing -u`
- `# svcadm enable route:default`

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

Cuando inicia 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*. Para obtener más información sobre los tipos de enrutamiento, consulte “[Tablas y tipos de enrutamiento](#)” en la [página 59](#). Para obtener información sobre el comando `routeadm`, consulte la [página del comando man routeadm\(1M\)](#).

Ejemplo 3–3 Configuración del enrutador predeterminado para una red

Este ejemplo se basa en la [Figura 3–1](#). El enrutador 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 muestra cómo configurar el enrutador 2 para que se convierta en el enrutador predeterminado de la red `172.20.1.0`. El ejemplo también supone que el enrutador 2 se configuró para funcionar en modo de archivos locales, como se describe en “[Cómo configurar un sistema para el modo de archivos locales](#)” en la [página 53](#).

Una vez se haya convertido en superusuario o haya asumido un rol equivalente, debe determinar el estado de las interfaces del sistema.

```
# dladm show-link
LINK    CLASS    MTU    STATE    BRIDGE    OVER
net0    phys     1500   up       --        --
net1    phys     1500   up       --        --
net2    phys     1500   up       --        --
# ipadm show-addr
ADDROBJ  TYPE    STATE    ADDR
lo0/v4   static  ok       127.0.0.1/8
net0/v4   static  ok       172.20.1.10/24
```

Únicamente `net0` se configuró con una dirección IP. Para convertir el enrutador 2 en el enrutador predeterminado, debe conectar físicamente la interfaz `net1` a la red `10.0.5.0`.

```
# ipadm create-ip net1
# ipadm create-addr -T static -a 10.0.5.10/24 net1/v4
# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4       static    ok         127.0.0.1/8
net0/v4       static    ok         172.20.1.10/24
net1/v4       static    ok         10.0.5.10/24
```

A continuación, deberá actualizar las siguientes bases de datos de red con información sobre la interfaz recientemente configurada 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     255.255.255.0
10.0.5.0       255.255.255.0
```

Por último, habilite el reenvío de paquetes y el daemon de enrutamiento `in.routed`.

```
# ipadm set-prop -p forwarding=on ipv4
# 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:

- Modifique cada host de la red 172.20.1.0 de modo que obtenga la 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 65](#).
- 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 59](#).

Tablas y tipos de enrutamiento

Tanto los enrutadores como los hosts mantienen una *tabla de enrutamiento*. 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. La *puerta de enlace* es un sistema que puede recibir paquetes salientes y reenviarlos un salto más allá de la red local.

La siguiente es una tabla de enrutamiento simple para un sistema en una red de sólo IPv4:

Routing Table: IPv4					
Destination	Gateway	Flags	Ref	Use	Interface

default	172.20.1.10	UG	1	532	net0
224.0.0.0	10.0.5.100	U	1	0	net1
10.0.0.0	10.0.5.100	U	1	0	net1
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 el *enrutamiento dinámico* se basa en protocolos de enrutamiento, como RIP para redes IPv4 y RIPng para redes IPv6, para enrutar el tráfico de red y actualizar información de enrutamiento en la tabla. Con el *enrutamiento estático*, la información de enrutamiento se mantiene de forma manual 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 3–1](#) combina el enrutamiento estático y el dinámico.

Nota – Dos rutas al mismo destino no hacen que el sistema ejecute automáticamente la función de equilibrio de carga o fallos. Si necesita estas capacidades, utilice IPMP, como se explica en el [Capítulo 14, “Introducción a IPMP”](#) de *Administración de Oracle Solaris: interfaces y virtualización de redes*.

▼ 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 la forma siguiente del 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   net0
224.0.0.0        198.168.5.10    U      1      0   net0
default          192.168.5.10    UG     1   91908
127.0.0.1        127.0.0.1       UH     1  811302   lo0
```

2 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#).

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`.

`-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 3-4 Cómo agregar una ruta estática a la tabla de enrutamiento

En el siguiente ejemplo, se muestra cómo agregar una ruta estática al enrutador 2 de la [Figura 3-1](#). La ruta estática es necesaria para el 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
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*. Las interfaces de un host múltiple se conectan a distintas subredes, ya sea en redes físicas diferentes o en la misma red física.

En un sistema cuyas múltiples interfaces se conectan a la misma subred, es necesario configurar primero las interfaces en un grupo IPMP. De lo contrario, el sistema no puede ser un host múltiple. Para obtener más información acerca de IPMP, consulte el [Capítulo 14, “Introducción a IPMP” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

Un host múltiple no reenvía paquetes IP, pero se puede configurar para ejecutar 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 distintos tipos de cortafuegos en cualquiera de sus interfaces, procure evitar la interrupción involuntaria de los paquetes del host. Este problema sucede especialmente con los cortafuegos con estado. Una solución podría ser configurar los cortafuegos sin estado. Para obtener más información sobre los cortafuegos, consulte [“Sistemas de cortafuegos” de Administración de Oracle Solaris: servicios de seguridad](#) o la documentación del cortafuegos si es de otro proveedor.

▼ Cómo crear un host múltiple

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#).

2 Configure cada interfaz de red adicional que no haya sido configurada como parte de la instalación de Oracle Solaris.

Consulte [“Cómo configurar una interfaz IP” en la página 47](#).

3 Si el reenvío de paquetes está habilitado, deshabilite este servicio.

```
# ipadm show-prop -p forwarding ipv4
PROTO PROPERTY  PERM CURRENT    PERSISTENT  DEFAULT  POSSIBLE
ipv4 forwarding  rw   on           --          off      on,off
```

```
ipadm set-prop -p forwarding=off ipv4
```

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

Utilice una de las siguientes sintaxis del comando:

- `# routeadm -e ipv4-routing -u`
- `# svcadm enable route:default`

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

Ejemplo 3-5 Configuración de un host múltiple

En el siguiente ejemplo, se muestra cómo configurar el host múltiple que aparece en la [Figura 3-1](#). 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
LINK      CLASS      MTU      STATE    BRIDGE    OVER
net0      phys       1500     up       --        --
net1      phys       1500     up       --        --

# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/v4    static    ok         127.0.0.1/8
net0/v4    static    ok         192.168.5.82/24
```

El comando `dladm show-link` informa que `hostc` tiene dos enlaces de datos. Sin embargo, únicamente `net0` se configuró con una dirección IP. Para configurar `hostc` como host múltiple, debe configurar `net1` con una dirección IP en la misma red `192.168.5.0`. Asegúrese de que la NIC física subyacente de `net1` esté conectada físicamente a la red.

```
# ipadm create-ip net1
# ipadm create-addr -T static -a 192.168.5.85/24 bge0/v4
# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/v4    static    ok         127.0.0.1/8
net0/v4    static    ok         192.168.5.82/24
net1/v4    static    ok         192.168.5.85/24
```

A continuación, debe agregar la interfaz `net1` a la base de datos `/etc/hosts`:

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

Luego, debe desactivar el reenvío de paquetes si este servicio se está ejecutando en `hostc`:

```
# ipadm show-prop -p forwarding ipv4
PROTO PROPERTY  PERM CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4 forwarding rw on -- off on,off

# ipadm set-prop -p forwarding=off ipv4

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



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

El comando `routeadm` informa que el enrutamiento dinámico a través del daemon `in.routed` está actualmente deshabilitado.

Configuración del enrutamiento para sistemas de interfaz única

Los sistemas de interfaz única se pueden configurar con enrutamiento estático o enrutamiento dinámico. Con el enrutamiento estático, el host debe confiar en los servicios de un enrutador predeterminado para obtener información de enrutamiento. Los procedimientos siguientes contienen las instrucciones para activar ambos tipos de enrutamiento.

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

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

- 1 **Conviértase en administrador.**
Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#).
- 2 **Configure las interfaces IP del sistema con una dirección IP para la red a la que pertenece el sistema.**
Para obtener instrucciones, consulte [“Cómo configurar una interfaz IP” en la página 47](#).
- 3 **Con un editor de textos, cree o modifique el archivo `/etc/defaultrouter` agregando la dirección IP del enrutador que utilizará el sistema.**
- 4 **Agregue una entrada para el enrutador predeterminado en el archivo `/etc/inet/hosts` local.**
- 5 **Asegúrese de que el enrutamiento esté desactivado.**

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

Routing services   "route:default ripng:default"

# svcadm disable route:default
```

6 Asegúrese de que el reenvío de paquetes esté desactivado.

```
# # ipadm show-prop -p forwarding ipv4
PROTO PROPERTY   PERM CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4 forwarding  rw  on      --         off      on,off

# ipadm set-prop -p forwarding=off ipv4
```

Ejemplo 3-6 Configuración del enrutamiento estático en un sistema de interfaz única

En el ejemplo siguiente, se muestra cómo configurar el enrutamiento estático para hostb, un sistema de interfaz única en la red 172.20.1.0, como se muestra en la [Figura 3-1](#). hostb debe utilizar el enrutador 2 como enrutador predeterminado. El ejemplo supone que ya se configuró la interfaz IP del sistema.

Primero, debe iniciar sesión en hostb con derechos de administrador. A continuación, debe determinar si el archivo /etc/defaultrouter está presente en el sistema:

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

# vi /etc/defaultrouter
172.20.1.10
```

La dirección IP 172.20.1.10 pertenece al enrutador 2.

```
# 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

# ipadm show-prop -p forwarding ipv4
PROTO PROPERTY   PERM CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4 forwarding  rw  on      --         off      on,off

# ipadm set-prop -p forwarding=off ipv4

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

                   Routing services "route:default ripng:default"

# svcadm disable route:default
```

▼ **Cómo habilitar el enrutamiento dinámico en un sistema de interfaz única**

El enrutamiento dinámico que utiliza un protocolo de enrutamiento es la manera más sencilla de gestionar el enrutamiento en un sistema.

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#).

2 Configure las interfaces IP del sistema con una dirección IP para la red a la que pertenece el sistema.

Para obtener instrucciones, consulte [“Cómo configurar una interfaz IP” en la página 47](#).

3 Suprima las entradas en el archivo `/etc/defaultrouter`.

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

4 Asegúrese de que el reenvío de paquetes esté deshabilitado.

```
# ipadm set-prop -p forwarding=off ipv4
```

5 Habilite los protocolos de enrutamiento en el sistema.

Utilice uno de los siguientes comandos:

- `# routeadm -e ipv4-routing -u`
- `# svcadm enable route:default`

Ejemplo 3–7 Ejecución del enrutamiento dinámico en un sistema de interfaz única

En el ejemplo siguiente, se muestra cómo configurar el enrutamiento dinámico para el comando `hosta`, un sistema de interfaz única en la red `192.168.5.0` que se muestra en la [Figura 3–1](#). El sistema utiliza el enrutador 1 como enrutador predeterminado. El ejemplo supone que ya se configuró la interfaz IP del sistema.

Primero, debe iniciar sesión en `hosta` con derechos de administrador. A continuación, debe determinar si el archivo `/etc/defaultrouter` está presente en el sistema:

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

# cat defaultrouter
192.168.5.10
```

El archivo incluye correctamente la entrada `192.168.5.10`, que es la dirección IP del enrutador 1.

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

              Routing services "route:default ripng:default"

# svcadm enable route:default

# ipadm show-prop -p forwarding ipv4
PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE
ipv4 forwarding rw on -- off on,off

# ipadm set-prop -p forwarding=off ipv4
```

Cómo agregar una subred a una red

Si está cambiando de una red que no utiliza una subred a una red que utiliza una subred, realice las tareas de la siguiente lista. Esta lista supone que ya se ha preparado un esquema de subred. Para obtener una descripción general, consulte “¿Qué son las subredes?” de *Guía de administración del sistema: servicios IP*.

- Asigne las direcciones IP con el nuevo número de subred a los sistemas que pertenecen a esa subred.
Para obtener información de referencia, consulte “Cómo configurar una interfaz IP” en la página 47.
- Agregue la dirección IP y la máscara de red correctas al archivo /etc/netmasks de cada sistema.
- Revise el archivo /etc/inet/hosts de cada sistema con la dirección IP correcta que corresponde a los nombres de host.
- Reinicie todos los sistemas de la subred.

El siguiente procedimiento está estrechamente relacionado con las subredes. Si implementa subredes mucho tiempo después de haber configurado originalmente la red sin subredes, realice el siguiente procedimiento para implementar los cambios.

▼ 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 IP” en la página 47.](#)

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” de Guía de administración del sistema: servicios IP.](#)

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad.](#)

2 Modifique la dirección IP con el comando `ipadm`.

Con el comando `ipadm`, no puede modificar una dirección de IP directamente. Primero suprima 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
```

3 Si corresponde, modifique el nombre de host en el archivo `/etc/inet/hosts` o la base de datos `hosts` equivalente.

4 Si corresponde, modifique la entrada de nombre de host en el servicio SMF `system/identity:node`:

```
# svccfg -s svc:/system/identity:node setprop config/nodename = astring: hostname
```

5 Si la máscara de subred ha cambiado, modifique las entradas de subred en el archivo `/etc/netmasks`.

6 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.

7 Reinicie el sistema.

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

Ejemplo 3–8 Cambio de la dirección IP y el nombre de host

En este ejemplo, se muestra cómo cambiar el nombre de un host, la dirección IP de la interfaz de red principal y la máscara de subred. La dirección IP de la interfaz de red principal bge0 cambia de 10.0.0.14 a 192.168.34.100.

```
# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4        static    ok         127.0.0.1/8
bge0/v4        static    ok         10.0.0.14/24

# ipadm delete-addr bge0/v4
# ipadm create-addr -T static -a 192.168.34.100/24 bge0/v4
# svccfg -s svc:/system/identity:node setprop config/nodename = astring: mynewhostname

# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4        static    ok         127.0.0.1/8
bge0/v4new    static    ok         192.168.34.100/24

# hostname
mynewhostname
```

Véase también Para cambiar la dirección IP de una interfaz que no sea la interfaz de red principal, consulte [Administración de Oracle Solaris: tareas comunes](#) y “Cómo configurar una interfaz IP” en la página 47.

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 6, “Gestión de servicios \(descripción general\)”](#) de *Administración de Oracle Solaris: tareas comunes*.

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 145.

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 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: 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 SMF, consulte “[Utilidades administrativas de la línea de comandos de la SMF](#)” de *Administración de Oracle Solaris: tareas comunes*.
- 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 3–9 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, como se describe en [“Compatibilidad con envoltorios TCP de la versión 8.12 de sendmail” de Oracle Administración Solaris: Servicios de red](#).

1 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

2 Active los envoltorios TCP.

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

3 Configure la política 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 puede encontrar en el directorio `/usr/sfw/man`.

Habilitación de IPv6 en una red

En este capítulo, se presentan las tareas para habilitar IPv6 en una red. Se tratan los temas principales siguientes:

- “Configuración de una interfaz de IPv6” en la página 77
- “Cómo configurar un sistema para IPv6” en la página 78
- “Configuración de un enrutador IPv6” en la página 80
- “Modificación de la configuración de una interfaz de IPv6 para hosts y servidores” en la página 82
- “Configuración de túneles (mapa de tareas)” en la página 126
- “Configuración de la compatibilidad con el servicio de nombres para IPv6” en la página 89

Para obtener distintos tipos de información sobre IPv6, consulte los siguientes recursos:

- Para obtener una descripción general de conceptos de IPv6: [Capítulo 3, “Introducción a IPv6 \(descripción general\)” de *Guía de administración del sistema: servicios IP*](#)
- Para conocer las tareas de planificación de IPv6: [Capítulo 2, “Consideraciones para el uso de direcciones IPv6”](#)
- Para conocer la preparación para el uso de túneles IP: [“Planificación para el uso de túneles en la red” en la página 41](#)
- Para obtener información de referencia: [Capítulo 9, “Referencia de IPv6”](#)

Configuración de una interfaz de IPv6

Como paso inicial para usar IPv6 en una red, configure IPv6 en la interfaz IP del sistema.

En el proceso de instalación de Oracle Solaris, IPv6 se puede habilitar en una o varias interfaces del sistema. Si habilitó la compatibilidad con IPv6 durante la instalación, una vez que se completa la instalación, se crean los siguientes archivos y tablas relacionados con IPv6:

- El servicio SMF `name-service/switch` se modificó para permitir consultas 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 describe cómo activar IPv6 en las interfaces después de que se completa la instalación de Oracle Solaris.

▼ Cómo configurar un sistema para IPv6

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. Inicialmente, la interfaz obtiene sus direcciones IPv6 mediante el proceso de configuración automática, como se describe en [“Configuración automática de direcciones IPv6” de Guía de administración del sistema: servicios IP](#). 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 80](#).

En el procedimiento siguiente se explica cómo habilitar IPv6 para una interfaz incorporada después de instalar Oracle Solaris.

1 Configure la interfaz IP con los comandos adecuados.

Consulte [“Cómo configurar una interfaz IP” en la página 47](#).

Nota – Al asignar la dirección IP, asegúrese de utilizar la opción correcta para asignar una dirección IPv6:

```
# ipadm create-addr -T addrconf addrobj
```

Para agregar más direcciones, utilice la sintaxis siguiente:

```
# ipadm create-addr -T static ipv6-address addrobj
```

2 Inicie el daemon de IPv6 `in.ndpd`.

```
# /usr/lib/inet/in.ndpd
```

3 (Opcional) 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 83](#). Para obtener más información sobre `/etc/inet/ndpd.conf`, consulte la página del comando `man ndpd.conf(4)` y [“Archivo de configuración ndpd.conf” en la página 152](#).

- 5 (Opcional) Para visualizar el estado de las interfaces IP con sus configuraciones IPv6, escriba el comando siguiente:

```
# ipadm show-addr
```

Ejemplo 4–1 Habilitación de una interfaz para IPv6 tras la instalación

En este ejemplo, se muestra cómo habilitar IPv6 en la interfaz `net0`. Antes de comenzar, compruebe el estado de todas las interfaces configuradas en el sistema.

```
# ipadm show-addr
ADDROBJ  TYPE    STATE  ADDR
lo0/v4   static  ok     127.0.0.1/8
net0/v4   static  ok     172.16.27.74/24
```

Para este sistema, únicamente está configurada la interfaz `net0`. Habilite IPv6 en esta interfaz de la forma que se indica a continuación:

```
# ipadm create-addr -T addrconf net0/v6
# ipadm create-addr -T static -a 2001:db8:3c4d:15:203/64 net0/v6add
# /usr/lib/inet/in.ndpd

# ipadm show-addr
ADDROBJ  TYPE        STATE  ADDR
lo0/v4   static      ok     127.0.0.1/8
net0/v4   static      ok     172.16.27.74/24
net0/v6   addrconf    ok     fe80::203:baff:fe13:14e1/10
lo0/v6   static      ok     ::1/128
net0/v6add static      ok     2001:db8:3c4d:15:203/64

# route -p add -inet6 default fe80::203:baff:fe13:14e1
```

- Pasos siguientes**
- Para configurar el nodo de IPv6 como enrutador, consulte [“Configuración de un enrutador IPv6” en la página 80](#).
 - Para anular la configuración automática de direcciones en el nodo, consulte [“Cómo desactivar la configuración automática de direcciones IPv6” en la página 80](#).
 - Para adaptar el nodo como servidor, tenga en cuenta las sugerencias de [“Administración de interfaces habilitadas para IPv6 en servidores” en la página 88](#).

▼ 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 86](#).

1 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 del comando `man ndpd.conf(4)` y [“Archivo de configuración `ndpd.conf`” en la página 152](#).

2 Actualice el daemon de IPv6 con los cambios.

```
# pkill -HUP in.ndpd
```

Configuración de un enrutador IPv6

En esta sección, se describen las tareas para configurar un enrutador IPv6. Según los requisitos del sitio, es posible que deba realizar únicamente tareas seleccionadas.

▼ Cómo configurar un enrutador habilitado para IPv6

En el siguiente procedimiento, se asume que ya se configuró el sistema para IPv6. Para conocer los procedimientos, consulte [“Configuración de una interfaz de IPv6” en la página 77](#).

1 Configure el reenvío de paquetes IPv6 en todas las interfaces del enrutador.

```
# ipadm set-prop -p forwarding=on ipv6
```

2 Inicie el daemon de enrutamiento.

El daemon `in.ripngd` se encarga del enrutamiento de IPv6. Active el enrutamiento de IPv6 mediante cualquiera de las opciones siguientes:

- Utilice el comando `routeadm`:

```
# routeadm -e ipv6-routing -u
```
- Utilice el comando SMF adecuado:

```
# svcadm enable ripng:default
```


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

3 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 152](#) y la página del comando `man ndpd.conf(4)`.

4 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.

5 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
```

En el siguiente archivo de ejemplo `/etc/inet/ndpd.conf`, se configura el enrutador para que anuncie el prefijo de sitio `2001:0db8:3c4d::/48` en las interfaces `net0` y `net1`.

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on

if net0 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:15::0/64 net0

if net1 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:16::0/64 net1
```

6 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 4-2 Salida de `ipadm show-addr` que muestra interfaces IPv6

En el ejemplo siguiente, se muestra la salida del comando `ipadm show-addr` después de finalizar el procedimiento de [“Configuración de un enrutador IPv6” en la página 80](#).

ADDROBJ	TYPE	STATE	ADDR
lo0/v4	static	ok	127.0.0.1/8
net0/v4	static	ok	172.16.15.232/24
net1/v4	static	ok	172.16.16.220/24

net0/v6	addrconf	ok	fe80::203:baff:fe11:b115/10
lo0/v6	static	ok	::1/128
net0/v6add	static	ok	2001:db8:3c4d:15:203:baff:fe11:b115/64
net1/v6	addrconf	ok	fe80::203:baff:fe11:b116/10
net1/v6add	static	ok	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 objeto de dirección, como *interfaz/v6*, muestra la dirección de enlace local de esa interfaz. La entrada con el nombre de objeto de dirección, como *interfaz/v6add* muestra una dirección IPv6 global. Esta dirección incluye el prefijo de sitio configurado en el archivo `/etc/ndpd.conf`, además del ID de interfaz. Tenga en cuenta que la designación `v6add` es una cadena definida de forma aleatoria. Puede definir otras cadenas para la segunda parte del nombre de objeto de dirección, siempre que la *interface* refleje la interfaz donde se están creando las direcciones IPv6, por ejemplo `net0/mystring`, `net0/ipv6addr`, etc.

- Véase también**
- Para configurar túneles desde los enrutadores identificados en la topología de red IPv6, consulte [“Configuración y administración de túneles con el comando `dladm`” en la página 126](#).
 - 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 82](#).
 - Para mejorar la compatibilidad de IPv6 en los servidores, consulte [“Administración de interfaces habilitadas para IPv6 en servidores” en la página 88](#).
 - Para obtener más información sobre comandos, archivos y daemons de IPv6, consulte [“Implementación de IPv6 en Oracle Solaris” en la página 151](#).

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, debe utilizar la configuración automática de direcciones para interfaces activadas para IPv6, como se explica en [“Descripción general de configuración automática sin estado” de *Guía de administración del sistema: servicios IP*](#). Sin embargo, la dirección IPv6 de una interfaz se puede modificar, si hace falta, como se explica en las tareas de la presente sección.

Debe realizar tres tareas generales en el siguiente orden:

1. Desactivar la configuración automática de direcciones IPv6. Consulte [“Cómo desactivar la configuración automática de direcciones IPv6” en la página 80](#).
2. Crear una dirección temporal para un host. Consulte [“Cómo configurar una dirección temporal” en la página 84](#).

3. Configurar un token IPv6 para el ID de interfaz. Consulte “[Cómo configurar un token IPv6 especificado por el usuario](#)” en la página 86.

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 las interfaces de un nodo IPv6 que desee mantener anónimas. 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>).

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 h</i>	<i>n</i> cantidad de horas (h)
<i>n d</i>	<i>n</i> cantidad de días (d)

▼ **Cómo configurar una dirección temporal**

1 Si es preciso, habilite IPv6 en las interfaces del host.

Consulte [“Cómo configurar un sistema para IPv6”](#) en la página 78.

2 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
```

3 (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.

4 (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 113.

- 5 (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.

- 6 Cambie la configuración del daemon `in.ndpd`.

```
# pkill -HUP in.ndpd
# /usr/lib/inet/in.ndpd
```

- 7 Verifique que las direcciones temporales se hayan creado con el comando `ipadm show-addr`, como se muestra en el [Ejemplo 4–4](#).

La salida del comando muestra el indicador `t` en el campo `CURRENT` de las direcciones temporales.

Ejemplo 4–3 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 4–4 Salida del comando `ipadm show-addr` con direcciones temporales habilitadas

En este ejemplo, se muestra la salida del comando `ipadm show-addr` después de crear direcciones temporales. Tenga en cuenta que en la salida de ejemplo únicamente se incluye información relacionada con IPv6.

```
# ipadm show-addr -o all
ADDROBJ  TYPE      STATE  CURRENT  PERSISTENT  ADDR
lo0/v6    static    ok     U----    ---         ::1/128
net0/v6    addrconf  ok     U----    ---         fe80::a00:20ff:feb9:4c54/10
net0/v6a   static    ok     U----    ---         2001:db8:3c4d:15:a00:20ff:feb9:4c54/64
net0/?     addrconf  ok     U--t-    ---         2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64
```

Tenga en cuenta que para el objeto de dirección `net0/?`, el indicador `t` se configura en el campo `CURRENT`. El indicador señala que la dirección correspondiente 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 89](#).

- Para configurar direcciones IPv6 para un servidor, consulte [“Cómo configurar un token IPv6 especificado por el usuario” en la página 86](#).
- Para supervisar actividades en nodos de IPv6, consulte el [Capítulo 5, “Administración de una red TCP/IP”](#).

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” de Guía de administración del sistema: servicios IP](#). 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 exista y que no haya direcciones IPv6 configuradas en la interfaz.**

Nota – Asegúrese de que la interfaz no tenga configurada ninguna dirección IPv6.

```
# ipadm show-if
IFNAME  CLASS  STATE  ACTIVE  OVER
lo0     loopback ok      yes     ---
net0    ip      ok      yes     ---
```

```
# ipadm show-addr
ADDROBJ  TYPE      STATE  ADDR
lo0/v4   static   ok     127.0.0.1/8
```

En esta salida, se muestra que la interfaz de red `net0` existe y no que tiene configurada ninguna dirección IPv6.

- 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” de Guía de administración del sistema: servicios IP](#).

- 3 Configure cada interfaz con un token.

Utilice la forma siguiente del comando `ipadm` para cada interfaz que deba tener un ID de interfaz especificado por el usuario (token):

```
# ipadm create-addr -T addrconf -i interface-ID addrobj
```

Por ejemplo, utilice el comando siguiente para configurar la interfaz `net0` con un token:

```
# ipadm create-addr -T addrconf -i ::1a:2b:3c:4d/64 net0/v6add
```

Nota – Después de crear el objeto de dirección con el token, no se puede modificar el token.

- 4 Actualice el daemon de IPv6 con los cambios.

```
# pkill -HUP in.ndpd
```

Ejemplo 4–5 Configuración de un token especificado por el usuario en una interfaz de IPv6

En el ejemplo siguiente, se muestra que `net0` se configura con una dirección IPv6 y un token.

```
# ipadm show-if
IFNAME  CLASS  STATE  ACTIVE  OVER
lo0     loopback ok      yes     ---
net0    ip      ok      yes     ---

# ipadm show-addr
ADDROBJ  TYPE      STATE  ADDR
lo0/v4   static   ok     127.0.0.1/8

# ipadm create-addr -T addrconf -i ::1a:2b:3c:4d/64 net0/v6
# pkill -HUP in.ndpd
# ipadm show-addr
ADDROBJ  TYPE      STATE  ADDR
lo0/v6   static   ok     ::1/128
net0/v6  addrconf ok     fe80::1a:2b:3c:4d/10
```

```
net0/v6      addrconf  ok      2002:a08:39f0:1:1a:2b:3c:4d/64
```

Después de configurar el token, el objeto de dirección `net0/v6` tiene una dirección de enlace local y una dirección con `1a:2b:3c:4d` configurado para este ID de interfaz. Tenga en cuenta que este token no puede ser modificado para esta interfaz después de la creación de `net0/v6`.

- 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 89](#).
 - Para supervisar el rendimiento del servidor, consulte el [Capítulo 5, “Administración de una red TCP/IP”](#).

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

Este procedimiento proporciona pasos generales para habilitar IPv6 en los servidores de la red. Algunos de los pasos pueden variar según cómo desea implementar IPv6.

1 Habilite IPv6 en las interfaces IP del servidor.

Para conocer los procedimientos, consulte [“Configuración de una interfaz de IPv6” en la página 77](#).

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 80](#).

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.

- Para una interfaz activada para IPv6 que no tenga previsto reemplazar, utilice la dirección IPv6 configurada automáticamente, como se menciona en [“Configuración automática de direcciones IPv6”](#) de *Guía de administración del sistema: servicios IP*.
- 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 84.
- 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 86.

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 [Oracle Solaris Administration: Naming and Directory Services](#).

▼ Cómo agregar direcciones IPv6 a DNS

- 1 **Edite el pertinente archivo de zona de DNS agregando registros de AAAA por cada nodo habilitado para IPv6:**

```
hostname IN AAAA host-address
```

- 2 **Edite el archivo de zona inversa de DNS y agregue registros PTR:**

```
hostaddress IN PTR hostname
```

Para obtener información detallada sobre la administración de DNS, consulte la [Oracle Solaris Administration: Naming and Directory Services](#).

Ejemplo 4–6 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.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.
```

▼ 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  
>hostname
```

3 Escriba el comando siguiente para ver sólo registros AAAA:

```
>set q=AAAA  
hostname
```

4 Salga del comando `nslookup`. Para ello, escriba `exit`.

Ejemplo 4-7 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 4–8 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 .byname
```

Aparece la información relativa al *nombre_host* especificado.

Administración de una red TCP/IP

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 94
- “Supervisión de direcciones e interfaces IP” de *Administración de Oracle Solaris: interfaces y virtualización de redes*
- “Supervisión del estado de la red con el comando `netstat`” en la página 95
- “Sondeo de hosts remotos con el comando `ping`” en la página 101
- “Administración y registro de la visualización del estado de la red” en la página 103
- “Visualización de información de enrutamiento con el comando `traceroute`” en la página 105
- “Control de transferencias de paquetes con el comando `snoop`” en la página 107
- “Administración de selección de direcciones predeterminadas” en la página 113

Nota – Para supervisar las interfaces de red, consulte “Supervisión de direcciones e interfaces IP” de *Administración de Oracle Solaris: interfaces y virtualización de redes*.

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 2, “Consideraciones para el uso de direcciones IPv6”](#).
- Para configurar IPv6 y crear un entorno de red de pila doble, consulte el [Capítulo 4, “Habilitación de IPv6 en una red”](#).

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 estadísticas según el protocolo.	Supervisar el rendimiento de los protocolos de red en un determinado sistema.	“Cómo visualizar estadísticas por protocolo” en la página 95
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 98
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 97
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 100
Controlar la salida en pantalla de los comandos relacionados con IPv6.	Controla la salida de los comandos ping, netstat 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 103
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 109
Efectuar el seguimiento de todas las rutas conocidas en los enrutadores de la red.	Se utiliza el comando traceroute para mostrar todas las rutas.	“Cómo efectuar el seguimiento de todas las rutas” en la página 106

Nota – Para supervisar las interfaces de red, consulte [“Supervisión de direcciones e interfaces IP” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

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 del 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 5–1 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
	rawipInChecksumErrs	=	0
	rawipOutErrors	=	0
	rawipInErrors	=	0
	rawipOutDatagrams	=	4
UDP			
	udpInDatagrams	=	10091
	udpOutDatagrams	=	15772
	udpInErrors	=	0
	udpOutErrors	=	0
TCP			
	tcpRtoAlgorithm	=	4
	tcpRtoMax	=	60000
	tcpRtoMin	=	400
	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
      icmp6InDestUnreachs =      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 del 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 5–2 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 5–3 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 5-4 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 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
net0	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
net0	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 5-5 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						
.						
.						
.	0	0	49152	0	LISTEN	

*TCP: IPv6

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 5-6 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 5-7 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 5-8 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
host15	myhost	U	1	31059	net0
10.0.0.14	myhost	U	1	0	net0
default	distantrouter	UG	1	2	net0
localhost	localhost	UH	42019361		lo0

Routing Table: IPv6						
Destination/Mask	Gateway	Flags	Ref	Use	If	
2002:0a00:3010:2::/64	2002:0a00:3010:2:1b2b:3c4c:5e6e:abcd	U	1	0	net0:1	
fe80::/10	fe80::1a2b:3c4d:5e6f:12a2	U	1	23	net0	
ff00::/8	fe80::1a2b:3c4d:5e6f:12a2	U	1	0	net0	
default	fe80::1a2b:3c4d:5e6f:12a2	UG	1	0	net0	
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 del 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 5-9 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 tiene paquetes descartados. Si falla el comando ping, compruebe el estado de la red indicado por los comandos `ipadm` y `netstat`.

Consulte “Supervisión de direcciones e interfaces IP” de *Administración de Oracle Solaris: interfaces y virtualización de redes* y “Supervisión del estado de la red con el comando `netstat`” en la página 95.

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 del comando `netstat` para visualizar información de IPv4 únicamente, o información de IPv4 y de 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 del comando `man inet_type(4)`.

Nota – El indicador `-f` del comando `netstat` sustituye los valores establecidos en el archivo `inet_type`.

Ejemplo 5–10 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 la salida siguiente:

```
% ipadm show-addr
ADDROBJ      TYPE      STATE  ADDR
lo0/v4       static    ok     127.0.0.1/8
net0/v4       static    ok     10.46.86.54/24
lo0/v6       static    ok     ::1/128
net0/v6       addrconf  ok     fe80::a00:fe73:56a8/10
net0/v6add    static    ok     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:

```
% ipadm show-addr
ADDROBJ      TYPE      STATE  ADDR
lo0/v4       static    ok     127.0.0.1/8
net0/v4       static    ok     10.46.86.54/24
```

▼ 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`.

- 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 5–11 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 104](#).

```
-- 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 net0 #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 net0 <NET_SYN>
Add 10.10.48.85/25 -->10.10.48.112 metric=0 net0 <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 **Inicie el seguimiento del daemon `in.ndpd`.**
`/usr/lib/inet/in.ndpd -t`
- 2 **Concluya el seguimiento a su conveniencia. Para ello, pulse las teclas Control+C.**

Ejemplo 5-12 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 net0
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 net0
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 del 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 5–13 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 5–14 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 del comando [man snoop\(1M\)](#).

▼ Cómo comprobar paquetes de todas las interfaces

1 Imprima la información relativa a las interfaces conectadas al sistema.

```
# ipadm show-if
```

El comando snoop suele utilizar el primer dispositivo que no es de bucle de retorno, en general la interfaz de red principal.

2 Comience a capturar paquetes escribiendo el comando snoop sin argumentos, como se muestra en el [Ejemplo 5–15](#).

3 Para detener el proceso, pulse Control+C.

Ejemplo 5-15 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/net (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)
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 la salida del comando snoop en un archivo

1 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.

2 Inspeccione el archivo de capturas de la salida del comando snoop.

```
# snoop -i filename
```

Ejemplo 5-16 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 refleja lo que sucede realmente en la conexión.

- 2 Escriba el comando snoop con opciones y guarde la salida que se genere en un archivo.

- 3 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.

- Capture paquetes de IPv6.

```
# snoop ip6
```

Para obtener más información sobre el comando snoop, consulte la página del comando [man snoop\(1M\)](#).

Ejemplo 5-17 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:fe9:2d27 -> fe80::a00:20ff:fe9:2d27 ICMPv6 Neighbor
solicitation
fe80::a00:20ff:fe9:2d27 -> fe80::a00:20ff:fe9:2d27 ICMPv6 Neighbor
solicitation
fe80::a00:20ff:fe9:2d27 -> ff02::9 RIPng R (11 destinations)
fe80::a00:20ff:fe9:2d27 -> ff02::1:ffcd:4375 ICMPv6 Neighbor solicitation
```

Supervisión de paquetes mediante dispositivos de capa IP

Los dispositivos de capa IP se agregan en Oracle Solaris para mejorar la observabilidad IP. Estos dispositivos ofrecen acceso a todos los paquetes con direcciones que están asociadas con la interfaz de red del sistema. Las direcciones incluyen direcciones locales y direcciones que están alojadas en interfaces que no son de bucle de retorno o interfaces lógicas. El tráfico observable puede incluir tanto direcciones IPv4 como direcciones IPv6. Por lo tanto, se puede supervisar todo el tráfico destinado al sistema. El tráfico puede incluir tráfico IP en bucle de retorno, paquetes de máquinas remotas, paquetes que se envían desde el sistema o todo el tráfico reenviado.

Con los dispositivos de capa IP, un administrador de una zona global puede supervisar el tráfico entre zonas y dentro de una zona. Un administrador de una zona no global también puede observar el tráfico que envía y recibe esa zona.

Para supervisar el tráfico en la capa IP, se agrega una nueva opción, `-I`, al comando `snoop`. Esta opción especifica que el comando debe utilizar los dispositivos de capa IP nuevos, en lugar del dispositivo subyacente de capa de enlace, para visualizar los datos de tráfico.

Nota – Para comprender las diferencias entre las capas, consulte [“Encapsulado de datos y la pila de protocolo TCP/IP” de Guía de administración del sistema: servicios IP](#).

▼ Cómo comprobar paquetes en la capa IP

- 1 Si es necesario, imprima la información relativa a las interfaces conectadas al sistema.

```
# ipadm show-if
```

- 2 Capture el tráfico IP en una interfaz específica.

```
# snoop -I interface [-v | -v]
```

Ejemplos de comprobación de paquetes

Todos los ejemplos se basan en la siguiente configuración del sistema:

```
# ipadm show-addr
ADDROBJ      TYPE      STATE  ADDR
lo0/v4        static    ok      127.0.0.1/8
net0/v4        static    ok      192.68.25.5/24
lo0/?         static    ok      127.0.0.1/8
net0/?        static    ok      172.0.0.3/24
net0/?        static    ok      172.0.0.1/24
lo0/?         static    ok      127.0.0.1/8
```

Suponga que dos zonas, sandbox y toybox, están utilizando las siguientes direcciones IP:

- sandbox – 172.0.0.3
- toybox – 172.0.0.1

Puede emitir el comando `snoop -I` en las distintas interfaces del sistema. La información de paquetes que se visualiza depende de si usted es administrador de la zona global o de la zona no global.

EJEMPLO 5-18 Tráfico en la interfaz en bucle de retorno

```
# snoop -I lo0
Using device ipnet/lo0 (promiscuous mode)
localhost -> localhost    ICMP Echo request (ID: 5550 Sequence number: 0)
localhost -> localhost    ICMP Echo reply (ID: 5550 Sequence number: 0)
```

Para generar una salida detallada, utilice la opción `-v`.

```
# snoop -v -I lo0
Using device ipnet/lo0 (promiscuous mode)
IPNET: ----- IPNET Header -----
IPNET:
IPNET: Packet 1 arrived at 10:40:33.68506
IPNET: Packet size = 108 bytes
IPNET: dli_version = 1
IPNET: dli_type = 4
IPNET: dli_srczone = 0
IPNET: dli_dstzone = 0
IPNET:
IP: ----- IP Header -----
IP:
IP: Version = 4
IP: Header length = 20 bytes
...
```

La compatibilidad para la observación de paquetes en la capa IP implementa un encabezado `ipnet` nuevo que precede a los paquetes que se están observando. Se indican los ID de origen y de destino. El ID '0' indica que el tráfico se genera en la zona global.

EJEMPLO 5-19 Flujo de paquetes en el dispositivo net0 en las zonas locales

```
# snoop -I net0
Using device ipnet/net0 (promiscuous mode)
toybox -> sandbox TCP D=22 S=62117 Syn Seq=195630514 Len=0 Win=49152 Options=<mss
```

EJEMPLO 5-19 Flujo de paquetes en el dispositivo net0 en las zonas locales (Continuación)

```
sandbox -> toybox TCP D=62117 S=22 Syn Ack=195630515 Seq=195794440 Len=0 Win=49152
toybox -> sandbox TCP D=22 S=62117 Ack=195794441 Seq=195630515 Len=0 Win=49152
sandbox -> toybox TCP D=62117 S=22 Push Ack=195630515 Seq=195794441 Len=20 Win=491
```

La salida muestra el tráfico que se produce en las distintas zonas dentro del sistema. Puede ver todos los paquetes que están asociados con las direcciones IP net0, incluidos los paquetes que se transfieren localmente a otras zonas. Si genera una salida detallada, puede ver las zonas que forman parte del flujo de paquetes.

```
# snoop -I net0 -v port 22
IPNET: ----- IPNET Header -----
IPNET:
IPNET: Packet 5 arrived at 15:16:50.85262
IPNET: Packet size = 64 bytes
IPNET: dli_version = 1
IPNET: dli_type = 0
IPNET: dli_srczone = 0
IPNET: dli_dstzone = 1
IPNET:
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:     .... ..0. = not ECN capable transport
IP:     .... ...0 = no ECN congestion experienced
IP: Total length = 40 bytes
IP: Identification = 22629
IP: Flags = 0x4
IP:     .1.. .... = do not fragment
IP:     ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 64 seconds/hops
IP: Protocol = 6 (TCP)
IP: Header checksum = 0000
IP: Source address = 172.0.0.1, 172.0.0.1
IP: Destination address = 172.0.0.3, 172.0.0.3
IP: No options
IP:
TCP: ----- TCP Header -----
TCP:
TCP: Source port = 46919
TCP: Destination port = 22
TCP: Sequence number = 3295338550
TCP: Acknowledgement number = 3295417957
TCP: Data offset = 20 bytes
TCP: Flags = 0x10
TCP:     0... .... = No ECN congestion window reduced
TCP:     .0.. .... = No ECN echo
TCP:     ..0. .... = No urgent pointer
```


EJEMPLO 5-19 Flujo de paquetes en el dispositivo net0 en las zonas locales (Continuación)

```

TCP:      ...1 .... = Acknowledgement
TCP:      .... 0... = No push
TCP:      .... .0.. = No reset
TCP:      .... ..0. = No Syn
TCP:      .... ...0 = No Fin
TCP: Window = 49152
TCP: Checksum = 0x0014
TCP: Urgent pointer = 0
TCP: No options
TCP:

```

El encabezado ipnet indica que el paquete proviene de la zonal global (ID 0) y se dirige a Sandbox (ID 1).

EJEMPLO 5-20 Observación del tráfico mediante la identificación de la zona

```

# snoop -I hme0 sandbox snoop -I net0 sandbox
Using device ipnet/hme0 (promiscuous mode)
toybox -> sandbox TCP D=22 S=61658 Syn Seq=374055417 Len=0 Win=49152 Options=<mss
sandbox -> toybox TCP D=61658 S=22 Syn Ack=374055418 Seq=374124525 Len=0 Win=49152
toybox -> sandbox TCP D=22 S=61658 Ack=374124526 Seq=374055418 Len=0 Win=49152
#

```

La capacidad de observar paquetes identificando la zona es útil en sistemas que tienen varias zonas. En la actualidad, únicamente se puede identificar la zona con el ID de zona. No se admite el uso de snoop con nombres de zonas.

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 del 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 156](#).



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 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
```

2 Efectúe una copia de seguridad de la tabla de directrices de direcciones predeterminadas.

```
# cp /etc/inet/ipaddrsel.conf /etc/inet/ipaddrsel.conf.orig
```

3 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.

4 Cargue en el núcleo la tabla de directrices modificada.

```
ipaddrsel -f /etc/inet/ipaddrsel.conf
```

5 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 Copie el contenido de `/etc/inet/ipaddrsel` en *nombre_archivo*; *nombre_archivo* es el archivo que haya seleccionado.

```
# cp /etc/inet/ipaddrsel filename
```

2 Modifique la tabla de directrices de *nombre_archivo* a su conveniencia.

3 Cargue 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.

Configuración de túneles IP

En este capítulo, se presentan descripciones de túneles IP y procedimientos para configurar y mantener túneles en Oracle Solaris.

Descripción general de túneles IP

Los túneles IP proporcionan un medio para transportar paquetes de datos entre dominios cuando el protocolo en esos dominios no está admitido por redes intermediarias. Por ejemplo, con la introducción del protocolo IPv6, las redes IPv6 requieren una manera de comunicarse más allá de sus límites en un entorno donde la mayoría de las redes utilizan el protocolo IPv4. La comunicación es posible gracias al uso de túneles. El túnel IP proporciona un enlace virtual entre dos nodos a los que se puede acceder mediante IP. De esta forma, el enlace se puede utilizar para transportar paquetes IPv6 en redes IPv4 para permitir la comunicación IPv6 entre los dos sitios IPv6.

Administración de túneles IP en esta versión de Oracle Solaris

En esta versión de Oracle Solaris, se revisó la administración de túneles para que sea coherente con el nuevo modelo de administración de enlaces de datos de red. Ahora, los túneles se crean y se configuran con nuevos subcomandos `dladm`. Los túneles ahora también pueden utilizar otras funciones de enlaces de datos del modelo de administración nuevo. Por ejemplo, la compatibilidad con nombres elegidos administrativamente permite que se asignen nombres significativos a los túneles. Para obtener más información sobre los subcomandos `dladm`, consulte la página del comando `man dladm(1M)`.

Tipos de túneles

La creación de túneles implica la encapsulación de un paquete IP dentro de otro paquete. Esta encapsulación permite que el paquete llegue a destino a través de redes intermediarias que no admiten el protocolo del paquete.

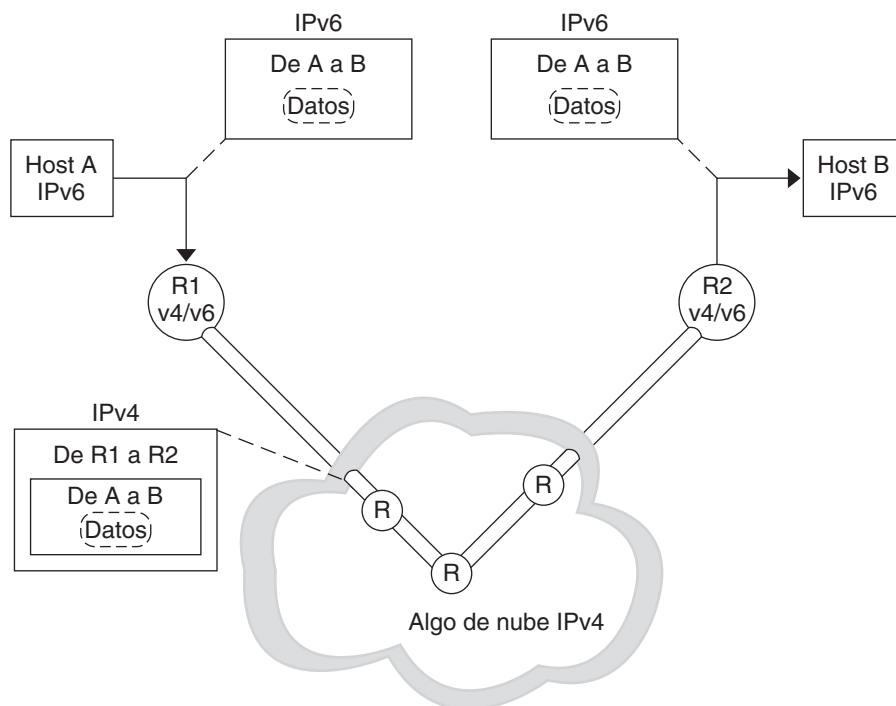
Los túneles varían según el tipo de encapsulación de paquetes. En Oracle Solaris, se admiten los siguientes tipos de paquetes:

- *Túneles IPv4*: los paquetes IPv4 o IPv6 se encapsulan en un encabezado IPv4 y se envían a un destino IPv4 de unidifusión preconfigurado. Para indicar más específicamente los paquetes que pasan por el túnel, los túneles IPv4 también se denominan *IPv4 en túneles IPv4* o *IPv6 en túneles IPv4*.
- *Túneles IPv6*: los paquetes IPv4 o IPv6 se encapsulan en un encabezado IPv6 y se envían a un destino IPv6 de unidifusión preconfigurado. Para indicar más específicamente los paquetes que pasan por el tunnel, los túneles IPv6 también se denominan *IPv4 en túneles IPv6* o *IPv6 en túneles IPv6*.
- *Túneles 6to4*: los paquetes IPv6 se encapsulan en un encabezado IPv4 y se envían a un destino IPv4 que se determina automáticamente según cada paquete. La determinación se basa en un algoritmo definido en el protocolo 6to4.

Túneles en los entornos de red IPv6 e IPv4 combinados

La mayoría de los sitios tienen dominios IPv6 que se comunican con otros dominios IPv6 atravesando redes IPv4, que son más prevalentes que las redes de sólo IPv6. En la figura siguiente, se ilustra el mecanismo de creación de túneles entre dos hosts IPv6 a través de enrutadores IPv4; esto se indica con una “R.”

FIGURA 6-1 Mecanismo de creación de túneles IPv6



En la figura, el túnel está compuesto por dos enrutadores configurados para tener un enlace de punto a punto virtual entre los dos enrutadores en la red IPv4.

Un paquete IPv6 está encapsulado dentro de un paquete 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 es transportado por el túnel hasta el enrutador de límite de destino, donde se desencapsula. A continuación, el enrutador reenvía el paquete IPv6 separado al nodo de destino.

Túneles 6to4

Oracle Solaris incluye túneles 6to4 como método provisional preferido para realizar la transición de direcciones IPv4 a IPv6. Los túneles 6to4 permiten que los sitios IPv6 aislados se comuniquen a través de un túnel automático en 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
- 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

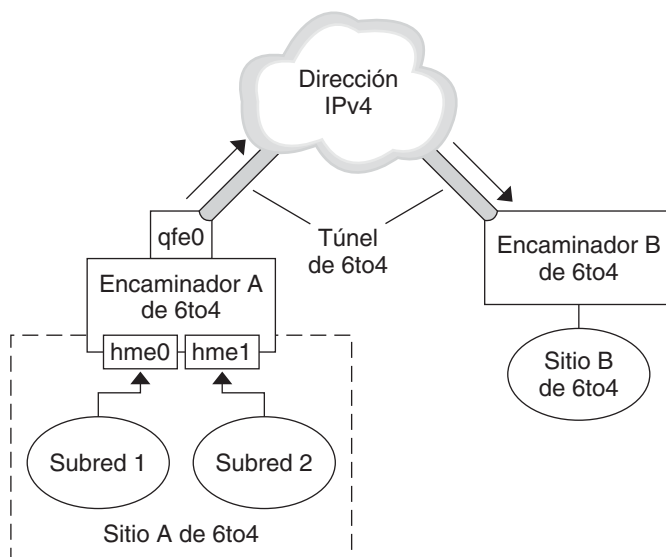
La tabla siguiente describe tareas adicionales para configurar túneles 6to4 y los recursos para obtener información adicional útil.

Tarea o detalle	Para obtener información
Tareas para configurar un túnel 6to4	“Cómo configurar un túnel 6to4” en la página 131
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 6-2 Túnel entre dos ubicaciones 6to4



En la figura, se muestran dos redes 6to4 aisladas: sitio A y sitio B. Cada sitio 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 encaminador A conecta la ubicación de sitio 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, sitio A 6to4 está compuesto por dos subredes conectadas a las interfaces `hme0` y `hme1` en el enrutador A. Todos los hosts IPv6 de la subredes del sitio A se reconfiguran automáticamente con direcciones derivadas de 6to4 al recibir el anuncio del enrutador A.

La ubicación de sitio B es otra ubicación 6to4 aislada. Para recibir correctamente tráfico de la ubicación de sitio A, se debe configurar un enrutador de límite en la ubicación sitio B para admitir 6to4. De no ser así, los paquetes que recibe el enrutador de sitio A no se reconocen y se descartan.

Flujo de paquetes a través del túnel 6to4

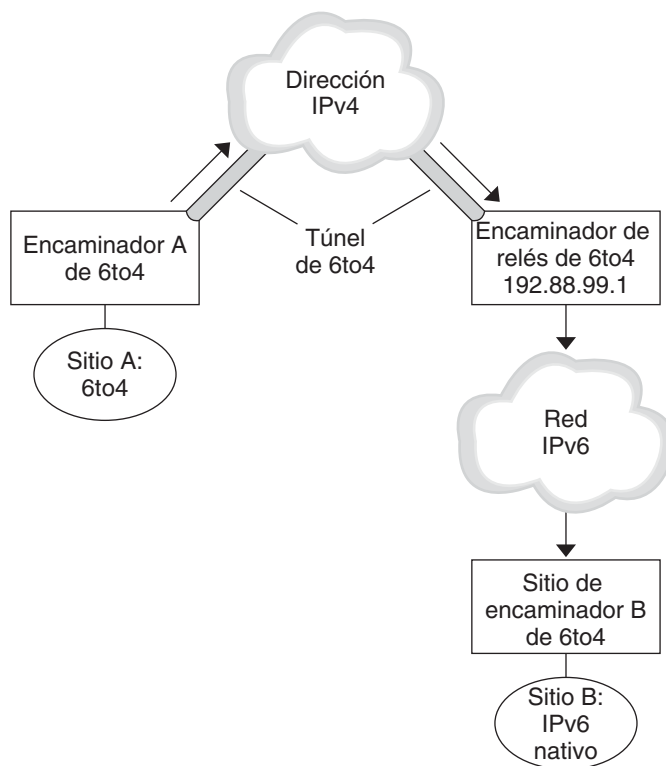
Esta sección describe el flujo de paquetes entre un hosts en una ubicación 6to4 y un host en una ubicación 6to4 remota. Esta situación hipotética utiliza la topología de la [Figura 6-2](#). En el ejemplo se considera que los enrutadores y hosts 6to4 ya están configurados.

1. Un host en la subred 1 de la ubicación de sitio A de 6to4 envía una transmisión, con un host de la ubicación sitio B de 6to4 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 sitio 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 de sitio 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 encaminador B, que también funciona como pseudointerfaz 6to4.
4. Los paquetes de sitio A llegan al encaminador B, que desencapsula los paquetes IPv6 del encabezado IPv4.
5. A continuación, el encaminador B utiliza la dirección de destino del paquete IPv6 para reenviar los paquetes al receptor en el sitio 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 6-3 Túnel desde una ubicación 6to4 hasta un enrutador de reenvío 6to4



En la [Figura 6-3](#), el sitio A 6to4 necesita comunicarse con un nodo en el sitio B IPv6 nativo. En la figura, se muestra la ruta de tráfico del sitio A al túnel 6to4 a través de una red IPv4. Los puntos finales del túnel son el encaminador A de 6to4 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 de sitio B IPv6.

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 6-3](#).

1. Un host en el sitio A 6to4 envía una transmisión que especifica como destino un host en el sitio B IPv6 nativo. El encabezado de cada paquete tiene una dirección derivada de 6to4 como dirección de origen. La dirección de destino es una dirección IPv6 estándar.

2. El enrutador 6to4 de la ubicación de sitio 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 de sitio 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 relé envía los paquetes que ahora son de sólo IPv6 a la red IPv6, donde, en última instancia, un enrutador del sitio B recupera los paquetes. Luego, el enrutador reenvía los paquetes al nodo IPv6 de destino.

Implementación de túneles

Para implementar adecuadamente los túneles IP, debe realizar dos tareas principales. Primero, debe crear el enlace de túnel. Luego, debe configurar una interfaz IP en el túnel. En esta sección, se describen brevemente los requisitos para crear túneles y sus correspondientes interfaces IP.

Requisitos para crear túneles

Para crear túneles correctamente, debe tener cumplir los siguientes requisitos:

- Si utiliza nombres de host en lugar de direcciones IP literales, estos nombres deben remitir a direcciones IP válidas compatibles con el tipo de túnel.
- El túnel IPv4 o IPv6 que cree no debe compartir la misma dirección de origen ni la misma dirección de destino con otro túnel configurado.
- El túnel IPv4 o IPv6 que cree no debe compartir la misma dirección de origen con un túnel 6to4 existente.
- Si crea un túnel 6to4, ese túnel no debe compartir la misma dirección de origen con otro túnel configurado.

Para obtener información sobre la configuración de túneles en la red, consulte [“Planificación para el uso de túneles en la red” en la página 41](#).

Requisitos para túneles e interfaces IP

Cada tipo de túnel tiene requisitos de direcciones IP específicos en la interfaz IP que se configure en el túnel. Los requisitos se resumen en la tabla siguiente.

TABLA 6–1 Requisitos de túneles e interfaces IP

Tipo de túnel	Interfaz IP permitida en el túnel	Requisito de interfaz IP
Túnel IPv4	Interfaz IPv4	Las direcciones locales y remotas se especifican manualmente.
	Interfaz IPv6	Las direcciones locales y remotas de enlace local se configuran automáticamente al emitir el comando <code>ipadm create-addr -T addrconf</code> . Para obtener detalles, consulte la página del comando <code>man ipadm(1M)</code> .
Túnel IPv6	Interfaz IPv4	Las direcciones locales y remotas se especifican manualmente.
	Interfaz IPv6	Las direcciones locales y remotas de enlace local se configuran automáticamente al emitir el comando <code>ipadm create-addr -T addrconf</code> . Para obtener detalles, consulte la página del comando <code>man ipadm(1M)</code> .
Túnel 6to4	Interfaz IPv6 únicamente	La dirección IPv6 predeterminada se selecciona automáticamente al emitir el comando <code>ipadm create-if</code> . Para obtener detalles, consulte la página del comando <code>man ipadm(1M)</code> .

Para sustituir la dirección de interfaz IPv6 predeterminada de los túneles 6to4, puede especificar una dirección IPv6 diferente con el comando `ipadm`.

De manera similar, para sustituir las direcciones de enlace local configuradas automáticamente para las interfaces IPv6 en túneles IPv4 o IPv6, puede especificar distintas direcciones de origen y de destino en el archivo `host` del túnel.

Configuración y administración de túneles con el comando `dladm`

En esta sección, se describen los procedimientos que utiliza el comando `dladm` para configurar túneles.

Subcomandos `dladm`

A partir de esta versión de Oracle Solaris, la administración de túneles es independiente de la configuración de la interfaz IP. El aspecto de enlace de datos de los túneles IP ahora se administra con el comando `dladm`. Además, la configuración de la interfaz IP, incluida la interfaz de túnel IP, se realiza con el comando `ipadm`.

Para configurar túneles IP se utilizan los siguientes subcomandos de `dladm`:

- `create-iptun`
- `modify-iptun`
- `show-iptun`
- `delete-iptun`
- `set-linkprop`

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

Nota – La administración de túneles IP está estrechamente relacionada con la configuración de IPsec. Por ejemplo, las redes privadas virtuales (VPN) IPsec constituyen uno de los principales usos de la creación de túneles IP. Para obtener más información sobre la seguridad en Oracle Solaris, consulte la [Parte III](#). Para configurar IPsec, consulte el [Capítulo 15](#), “Configuración de IPsec (tareas)”.

Configuración de túneles (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Crear un túnel IP.	Configure el túnel que se utilizará para las comunicaciones entre redes.	“Cómo crear y configurar un túnel IP” en la página 127
Modificar la configuración de un túnel.	Cambie los parámetros originales del túnel, como la dirección de origen o de destino del túnel.	“Cómo modificar una configuración de túnel IP” en la página 135

Tarea	Descripción	Para obtener instrucciones
Visualizar la configuración de un túnel.	Muestre la información de configuración de un túnel específico o de todos los túneles IP del sistema.	“Cómo visualizar una configuración de túnel IP” en la página 136
Suprimir un túnel.	Suprima la configuración de un túnel.	“Cómo suprimir un túnel IP” en la página 138

▼ Cómo crear y configurar un túnel IP

1 Cree el túnel.

`dladm create-iptun [-t] -T type -a [local|remote]=addr,... tunnel-link`

Para este comando, están disponibles las opciones o los argumentos siguientes:

-t	Crea un túnel temporal. De manera predeterminada, el comando crea un túnel persistente.
<hr/>	
Nota – Si desea configurar una interfaz IP persistente en el túnel, debe crear un túnel persistente y no utilizar la opción <code>-t</code> .	
<hr/>	
-T <i>tipo</i>	Especifica el tipo de túnel que desea crear. Este argumento es necesario para crear todos los tipos de túneles.
-a [local remote]= <i>dirección</i> ,...	Especifica los nombres de host o las direcciones IP literales que corresponden a la dirección local y a la dirección de túnel remota. Las direcciones deben ser válidas y ya deben estar creadas en el sistema. Según el tipo de túnel, debe especificar una sola dirección o ambas direcciones (locales y remotas). Si especifica direcciones locales y remotas, debe separarlas con una coma. <ul style="list-style-type: none">■ Los túneles IPv4 requieren direcciones IPv4 locales y remotas para funcionar.■ Los túneles IPv6 requieren direcciones IPv6 locales y remotas para funcionar.■ Los túneles 6to4 requieren una dirección IPv4 local para funcionar.

Nota – Para configuraciones de enlace de datos de túneles IP, si está utilizando nombres de host para las direcciones, estos nombres de host se guardan en el almacenamiento de la configuración. Durante un inicio posterior del sistema, si el nombre remite a direcciones IP distintas de las direcciones IP utilizadas cuando se creó el túnel, el túnel adquiere una nueva configuración.

enlace_túnel

Especifica el enlace de túnel IP. Al admitir nombres significativos en una administración de enlace de red, los nombres de los túneles ya no se restringen al tipo de túnel que se está creando. En cambio, se puede asignar a un túnel cualquier nombre elegido administrativamente. Los nombres de túneles está formados por una cadena y el número de punto físico de conexión (PPA), por ejemplo, *mitúnel0*. Para conocer las reglas que rigen la asignación de nombres significativos, consulte [“Reglas para nombres de enlace válidos” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

Si no especifica el enlace de túnel, el nombre se proporciona automáticamente según las convenciones de denominación siguientes:

- Para túneles IPv4: `ip.tun#`
- Para túneles IPv6: `ip6.tun#`
- Para túneles 6to4: `ip.6to4tun#`

corresponde al número de PPA más bajo disponible para el tipo de túnel que se está creando.

2 (Opcional) Configure valores para el límite de salto o el límite de encapsulación.

```
# dladm set-linkprop -p [hoplimit=value] [encaplimit=value] tunnel-link
```

hoplimit Especifica el límite de salto de la interfaz de túnel para la creación de túneles en IPv6. El valor de *hoplimit* es equivalente al campo de tiempo de vida (TTL) de IPv4 para la creación de túneles en IPv4.

encaplimit Especifica el número de niveles de creación de túneles anidados permitidos para un paquete. Esta opción se aplica únicamente a túneles IPv6.

Especifica el número de niveles de creación de túneles anidados permitidos para un paquete. Esta opción se aplica únicamente a túneles IPv6.

Nota – Los valores establecidos para `hoplimit` y `encaplimit` deben estar dentro de rangos aceptables. `hoplimit` y `encaplimit` son propiedades de enlace de túnel. Por lo tanto, estas propiedades se administran con los mismos subcomandos `dladm` que otras propiedades de enlace. Los subcomandos son `dladm set-linkprop`, `dladm reset-linkprop` y `dladm show-linkprop`. Consulte la página del comando [man dladm\(1M\)](#) para conocer los distintos subcomandos que se utilizan con el comando `dladm` para administrar enlaces.

3 Cree una interfaz IP en el túnel.

```
# ipadm create-ip tunnel-interface
```

Donde *interfaz_túnel* utiliza el mismo nombre que el enlace de túnel.

4 Asigne direcciones IP locales y remotas a la interfaz de túnel.

```
# ipadm create-addr [-t] -T static -a local=address,remote=address addrobj
```

<code>-t</code>	Indica una configuración IP temporal en lugar de una configuración IP persistente en el túnel. Si no utiliza esta opción, la configuración de la interfaz IP es persistente.
<code>-T static</code>	Indica que se utilizan direcciones IP estáticas en lugar de los procedimientos IP dinámicos.
<code>-a local=dirección,remote=dirección</code>	Especifica las direcciones IP de la interfaz de túnel. Se requieren direcciones IP de origen y de destino, representadas por <code>local</code> y <code>remote</code> . Las direcciones locales y remotas pueden ser direcciones IPv4 o IPv6.
<i>objeto_dirección</i>	Especifica el objeto de dirección que es propietario de las direcciones locales y remotas. <i>objeto_dirección</i> debe usar el formato <i>interfaz/cadena_especificada_usuario</i> . La <i>cadena_especificada_usuario</i> se refiere a una cadena de caracteres alfanuméricos que comienza con un carácter alfabético y tiene una longitud máxima de 32 caracteres.

Para obtener más información sobre el comando `ipadm` y las diferentes opciones para configurar interfaces IP, incluidos los túneles de interfaces, consulte la página del comando [man ipadm\(1M\)](#) y la Parte II, “Configuración de interfaz y enlace de datos” de *Administración de Oracle Solaris: interfaces y virtualización de redes*.

5 Agregue la información sobre la configuración del túnel al archivo `/etc/hosts`.

6 (Opcional) Verifique el estado de la configuración de la interfaz IP del túnel.

```
# ipadm show-addr interface
```

Ejemplo 6-1 Creación de una interfaz IPv6 en un túnel IPv4

En este ejemplo, se muestra cómo crear una IPv6 persistente en un túnel IPv4.

```
# dladm create-iptun -T ipv4 -a local=63.1.2.3,remote=192.4.5.6 private0
# dladm set-linkprop -p hoplimit=200 private0
# ipadm create-ip private0
# ipadm create-addr -T addrconf private0/v6
# ipadm show-addr private/
```

ADDROBJ	TYPE	STATE	ADDR
private0/v6	static	ok	fe80::a08:392e/10 --> fe80::8191:9a56

Para agregar direcciones alternativas, utilice la misma sintaxis y una *cadena_especificada_usuario* distinta para *objeto_dirección*. Por ejemplo, puede agregar una dirección global de la siguiente manera:

```
# ipadm create-addr -T static -a local=2001:db8:4728::1, \
remote=2001:db8:4728::2 private0/global
# ipadm show-addr private0/
```

ADDROBJ	TYPE	STATE	ADDR
private0/v6	addrconf	ok	fe80::a08:392e/10 --> fe80::8191:9a56
private0/global	static	ok	2001:db8:4728::1 --> 2001:db8:4728::2

Tenga en cuenta que el prefijo `2001:db8` para las direcciones IPv6 es un prefijo IPv6 especial que se utiliza específicamente para ejemplos de documentación. Para obtener una descripción del formato y las direcciones IPv6, consulte [“Descripción general de las direcciones IPv6” de Guía de administración del sistema: servicios IP](#).

Ejemplo 6-2 Creación de una interfaz IPv4 en un túnel IPv4

En este ejemplo, se muestra cómo crear una IPv4 persistente en un túnel IPv4.

```
# dladm create-iptun -T ipv4 -a local=63.1.2.3,remote=192.4.5.6 vpn0
# ipadm create-ip vpn0
# ipadm create-addr -T static -a local=10.0.0.1,remote=10.0.0.2 vpn0/v4
# ipadm show-addr
```

ADDROBJ	TYPE	STATE	ADDR
lo0/v4	static	ok	127.0.0.1
vpn0/v4	static	ok	10.0.0.1-->10.0.0.2

Puede configurar, además, una política IPsec para proporcionar conexiones seguras para los paquetes que pasan por este túnel. Para obtener información sobre la configuración de IPsec, consulte el [Capítulo 15, “Configuración de IPsec \(tareas\)”](#).

Ejemplo 6-3 Creación de una interfaz IPv6 en un túnel IPv6

En este ejemplo, se muestra cómo crear una IPv6 persistente en un túnel IPv6.

```
# dladm create-iptun -T ipv6 -a local=2001:db8:feed::1234,remote=2001:db8:beef::4321 \
tun0
# ipadm create-ip tun0
# ipadm create-addr -T addrconf tun0/v6
# ipadm show-addr
ADDROBJ    TYPE      STATE    ADDR
lo0/v6     static    ok       ::1/128
tun0/v6    addrconf  ok       2001:db8:feed::1234 --> 2001:db8:beef::4321
```

Par agregar direcciones, como una dirección global o direcciones locales y remotas alternativas, utilice el comando `ipadm` de la siguiente manera:

```
# ipadm create-addr -T static \
-a local=2001:db8::4728:56bc,remote=2001:db8::1428:57ab tun0/alt
# ipadm show-addr tun0/
ADDROBJ    TYPE      STATE    ADDR
tun0/v6    addrconf  ok       2001:db8:feed::1234 --> 2001:db8:beef::4321
tun0/alt   static    ok       2001:db8::4728:56bc --> 2001:db8::1428:57ab
```

▼ Cómo configurar un túnel 6to4

En túneles 6to4, un enrutador 6to4 debe actuar como enrutador IPv6 para los nodos de los sitios 6to4 de la red. Por lo tanto, al configurar un enrutador 6to4, ese enrutador también debe estar configurado como enrutador IPv6 en las interfaces físicas. Para obtener más información sobre los enrutadores IPv6, consulte [“Enrutamiento de IPv6” en la página 170](#).

1 Cree un túnel 6to4.

```
# dladm create-iptun -T 6to4 -a local=address tunnel-link
```

Para este comando, están disponibles las opciones o los argumentos siguientes:

- a local=*dirección* Especifica la dirección local del túnel, que ya debe existir en el sistema para ser una dirección válida.
- enlace_túnel Especifica el enlace de túnel IP. Al admitir nombres significativos en una administración de enlace de red, los nombres de los túneles ya no se restringen al tipo de túnel que se está creando. En cambio, se puede asignar a un túnel cualquier nombre elegido administrativamente. Los nombres de túneles está formados por una cadena y el número de PPA, por ejemplo, *mitúnel0*. Para conocer las reglas que rigen la asignación de nombres significativos, consulte [“Reglas para nombres de enlace válidos” de Administración de Oracle Solaris: interfaces y virtualización de redes](#).

2 Cree la interfaz IP del túnel.

```
# ipadm create-ip tunnel-interface
```

Donde *interfaz_túnel* utiliza el mismo nombre que el enlace de túnel.

3 (Opcional) Agregue direcciones IPv6 alternativas para el uso del túnel.**4 Agregue las siguientes dos líneas para editar el archivo `/etc/inet/ndpd.conf` para anunciar el enrutamiento 6to4:**

```
if subnet-interface AdvSendAdvertisements 1
IPv6-address subnet-interface
```

La primera línea especifica la subred que recibe el anuncio. Donde *interfaz_subred* se refiere al enlace al que está conectada la subred. La dirección IPv6 de la segunda línea debe tener el prefijo 6to4 2000 que se utiliza para direcciones IPv6 en túneles 6to4.

Para obtener información detallada sobre el archivo `ndpd.conf`, consulte la página del comando `man ndpd.conf(4)`.

5 Habilite el reenvío de IPv6.

```
# ipadm set-prop -p forwarding=on ipv6
```

6 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.

7 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 89](#).

Ejemplo 6–4 Creación de un túnel 6to4

En este ejemplo, la interfaz de subred es `bge0`, a la que se referirá `/etc/inet/ndpd.conf` en el paso correspondiente.

En este ejemplo, se muestra cómo crear un túnel 6to4. Tenga en cuenta que únicamente las interfaces IPv6 se pueden configurar en túneles 6to4.

```
# dladm create-iptun -T 6to4 -a local=192.168.35.10 tun0
# ipadm create-ip tun0
# ipadm show-addr
```

ADDROBJ	TYPE	STATE	ADDR
lo0/v4	static	ok	127.0.0.1/8
bge0/static	static	ok	192.168.35.10/24

```

lo0/v6          static  ok      ::1/128
tun0/_a         static  ok      2002:c0a8:57bc::1/64

# ipadm create-addr -T static -a 2002:c0a8:230a::2/16 tun0/a2
# ipadm create-addr -T static -a 2002:c0a8:230a::3/16 tun0/a3
# ipadm show-addr tun0/
ADDROBJ        TYPE      STATE    ADDR
lo0/v4         static   ok       127.0.0.1/8
bge0/static    static  ok       192.168.35.10/24
lo0/v6         static  ok       ::1/128
tun0/_a        static  ok       2002:c0a8:57bc::1/64
tun0/a2        static  ok       2002:c0a8:230a::2/16
tun0/a3        static  ok       2002:c0a8:230a::3/16

# vi /etc/inet/ndpd.conf
if bge0 AdvSendAdvertisements 1
2002:c0a8:57bc::1/64 bge0

# ipadm set-prop -p forwarding=on ipv6

```

Tenga en cuenta que para los túneles 6to4, el prefijo para la dirección IPv6 es 2002. Para obtener más explicaciones, consulte [“Prefijos de IPv6” de Guía de administración del sistema: servicios IP](#).

▼ 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 142](#).

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 el sitio, como se explica en [“Cómo crear y configurar un túnel IP” en la página 127](#)
- Revisar los problemas de seguridad relacionados con el establecimiento de un túnel hasta un enrutador de reenvío 6to4

1 Habilite un túnel hasta el enrutador de reenvío 6to4 utilizando uno de los siguientes formatos:

- Activar 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_enrutador_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 pseudointerfaz de túnel 6to4.

2 Elimine el túnel hasta el enrutador de reenvío 6to4 cuando ya no sea necesario:

```
# /usr/sbin/6to4relay -d
```

3 (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 el 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 6–5 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
```

▼ Cómo modificar una configuración de túnel IP

● Cambie la configuración del túnel.

```
# dladm modify-iptun -a [local|remote]=addr,... tunnel-link
```

No puede modificar el tipo de un túnel existente. Por lo tanto, la opción `-T tipo` no se permite para este comando. Únicamente pueden modificarse los parámetros de túnel siguientes:

- `-a [local|remote]=dirección,...` Especifica los nombres de host o las direcciones IP literales que corresponden a la dirección local y a la dirección de túnel remota. Según el tipo de túnel, debe especificar una sola dirección o ambas direcciones (locales y remotas). Si especifica direcciones locales y remotas, debe separarlas con una coma.
- Los túneles IPv4 requieren direcciones IPv4 locales y remotas para funcionar.
 - Los túneles IPv6 requieren direcciones IPv6 locales y remotas para funcionar.
 - Los túneles 6to4 requieren una dirección IPv4 local para funcionar.

Para configuraciones de enlace de datos de túneles IP, si está utilizando nombres de host para las direcciones, estos nombres de host se guardan en el almacenamiento de la configuración. Durante un inicio posterior del sistema, si el nombre remite a direcciones IP distintas de las direcciones IP utilizadas cuando se creó el túnel, el túnel adquiere una nueva configuración.

Si está cambiando las direcciones locales y remotas del túnel, asegúrese de que estas direcciones sean coherentes con el tipo de túnel que está modificando.

Nota – Si desea cambiar el nombre del enlace de túnel, no utilice el subcomando `modify-iptun`. En cambio, utilice `dladm rename-link`.

```
# dladm rename-link old-tunnel-link new-tunnel-link
```

De manera similar, no utilice el comando `modify-iptun` para cambiar las propiedades del túnel, como `hoplimit` o `encaplimit`. En cambio, utilice el comando `dladm set-linkprop` para configurar valores para estas propiedades.

Ejemplo 6-6 Modificación de la dirección y las propiedades de un túnel

Este ejemplo consta de dos procedimientos. En primer lugar, las direcciones locales y remotas del túnel IPv4 `vpn0` se cambian temporalmente. Cuando el sistema se reinicia más adelante, el túnel vuelve a utilizar las direcciones originales. En un segundo procedimiento, el valor de `hoplimit` de `vpn0` se cambia a 60.

```
# dladm modify-iptun -t -a local=10.8.48.149,remote=192.1.2.3 vpn0
# dladm set-linkprop -p hoplimit=60 vpn0
```

▼ **Cómo visualizar una configuración de túnel IP**

● **Visualice la configuración del túnel IP.**

```
# dladm show-iptun [-p] -o fields [tunnel-link]
```

Con el comando, se pueden utilizar las siguientes opciones:

- p Muestra la información en un formato que la máquina puede analizar. Este argumento es opcional.
- o *campos* Muestra campos seleccionados que proporcionan información de un túnel específico.
- enlace_túnel* Especifica el túnel cuya información de configuración desea visualizar. Este argumento es opcional. Si omite el nombre del túnel, el comando muestra la información sobre todos los túneles del sistema.

Ejemplo 6-7 Visualización de información sobre todos los túneles

En este ejemplo, únicamente existe un túnel en el sistema.

```
# dladm show-iptun
LINK   TYPE   FLAGS   LOCAL           REMOTE
tun0   6to4   --      192.168.35.10   --
```



```
vpn0      ipv4      --      10.8.48.149    192.1.2.3
```

Ejemplo 6–8 Visualización de campos seleccionados en un formato que la máquina puede analizar

En este ejemplo, únicamente se muestran campos específicos con información del túnel.

```
# dladm show-iptun -p -o link,type,local
tun0:6to4:192.168.35.10
vpn0:ipv4:10.8.48.149
```

▼ **Cómo visualizar las propiedades de un túnel IP**

- Visualice las propiedades del enlace de túnel.

```
# dladm show-linkprop [-c] [-o fields] [tunnel-link]
```

Con el comando, se pueden utilizar las siguientes opciones:

-c Muestra la información en un formato que la máquina puede analizar. Este argumento es opcional.

-o *campos* Muestra campos seleccionados que proporcionan información sobre las propiedades del enlace.

enlace_túnel Especifica el túnel cuya información de propiedades se desea visualizar. Este argumento es opcional. Si omite el nombre del túnel, el comando muestra la información sobre todos los túneles del sistema.

Ejemplo 6–9 Visualización de las propiedades de un túnel

En este ejemplo, se muestra cómo visualizar todas las propiedades del enlace de un túnel.

```
# dladm show-linkprop tun0
LINK      PROPERTY  PERM   VALUE    DEFAULT  POSSIBLE
tun0      autopush   --     --       --       --
tun0      zone       rw     --       --       --
tun0      state     r-     up        up        up,down
tun0      mtu       r-     65515    --       576-65495
tun0      maxbw     rw     --       --       --
tun0      cpus      rw     --       --       --
tun0      priority  rw     high     high     low,medium,high
tun0      hoplimit  rw     64       64       1-255
```

▼ Cómo suprimir un túnel IP

- 1 Utilice la sintaxis adecuada para desconectar la interfaz IP configurada en el túnel según el tipo de interfaz.

```
# ipadm delete-ip tunnel-link
```

Nota – Para suprimir correctamente un túnel, no puede conectarse en el túnel ninguna interfaz IP existente.

- 2 Suprima el túnel IP.

```
# dladm delete-iptun tunnel-link
```

La única opción para este comando es `-t`, que suprime el túnel temporalmente. Al reiniciar el sistema, se restaura el túnel.

Ejemplo 6–10 Supresión de un túnel IPv6 configurado con una interfaz IPv6

En este ejemplo, se suprime permanentemente un túnel persistente.

```
# ipadm delete-ip ip6.tun0  
# dladm delete-iptun ip6.tun0
```

Resolución de problemas de red

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 139
- “Problemas comunes al utilizar IPv6” en la página 140

Consejos de resolución de problemas de red generales

Uno de los primeros signos de problemas en una red es la pérdida de comunicación en uno o más 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 utilizar el comando `ipadm` para obtener información sobre las 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 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 95](#) y la página del comando `man netstat(1M)`.

2 Compruebe la base de datos `hosts` para asegurarse de que las entradas sean correctas y estén actualizadas.

Para obtener información sobre la base de datos `/etc/inet/hosts`, consulte [“Archivos de configuración de red” en la página 143](#) y la página del comando `man hosts(4)`.

3 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.

4 Intente conectarse al host local con el comando `telnet`.

Si necesita la sintaxis e información sobre `telnet`, consulte la página del comando `man telnet(1)`.

5 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
```

6 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 2, “Consideraciones para el uso de direcciones IPv6”](#).

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 las tareas relativas a la configuración de túneles, consulte [“Configuración y administración de túneles con el comando `dladm`” en la página 126](#).

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

Por lo general, un túnel entre un enrutador de 6to4 y un enrutador de relé de 6to4 es inseguro. 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 *Consideraciones de seguridad para 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 *Consideraciones de seguridad para 6to4*.

Referencia de IPv4

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.

El capítulo contiene la información siguiente:

- “Archivos de configuración de red” en la página 143
- “Daemon de servicios de Internet `inetd`” en la página 145
- “El servicio SMF `name-service/switch`” en la página 145
- “Protocolos de enrutamiento en Oracle Solaris” en la página 147

Archivos de configuración de red

En una red, la información de configuración se almacena en distintos archivos y bases de datos que regulan la forma en que funciona la red. En esta sección, se proporciona una breve descripción de estos archivos. Algunos archivos requieren actualización y mantenimiento a medida que se implementan cambios en la red. Otros archivos requieren muy poca o ninguna administración.

<code>/etc/defaultrouter</code>	Este archivo contiene los nombres de interfaces IP de los enrutadores que están directamente conectados a la red. La existencia de este archivo en el sistema es opcional. Si existe el archivo, el sistema está configurado para admitir el enrutamiento estático.
<code>/etc/inet/hosts</code>	Este archivo contiene las direcciones IPv4 en la red junto con los nombres de las interfaces correspondientes en las que están configuradas las direcciones. Si utiliza el servicio de nombres NIS o DNS, o el servicio de directorios LDAP, la información de host se almacena en una base de datos diferente, como <code>hosts.byname</code> , que existe en los servidores. Para obtener más información, consulte <i>Oracle Solaris Administration: Naming and Directory Services</i> .

<code>/etc/inet/netmasks</code>	Este archivo contiene el número de red, como 192.168.0.0, y la información de máscara de red de ese número de red, como 255.255.255.0. En una red que utiliza NIS o LDAP, esta información se almacena en una base de datos de máscara de red en los servidores. Consulte la página del comando <code>man netmasks(4)</code> para obtener más información.
<code>/etc/bootparams</code>	Este archivo contiene los parámetros que determinan los procesos de inicio para los sistemas que están configurados para iniciarse en modo de cliente de red. Para obtener más información, consulte “Configuración de los modos de configuración del sistema” en la página 51 . El archivo sirve de base para la creación de la base de datos <code>bootparams</code> que el servicio de nombres usa cuando no se está utilizando el modo de archivos locales. Para obtener información específica sobre el contenido y el formato de este archivo, consulte la página del comando <code>man bootparams(4)</code> .
<code>/etc/ethers</code>	El archivo asocia los nombres de host con las direcciones MAC. El archivo sirve de base para la creación de una base de datos <code>ethers</code> que se utiliza en la red donde los sistemas están configurados como clientes de red. Para obtener más información, consulte la página del comando <code>man ethers(4)</code> .
<code>/etc/inet/networks</code>	Este archivo asocia nombres de red con números de red. También se pueden agregar comentarios para ofrecer una aclaración adicional de cada entrada en la base de datos. Este archivo permite que las aplicaciones utilicen y muestren los nombres de red en lugar de los números de red. Por ejemplo, el programa <code>netstat</code> utiliza la información de esta base de datos para producir tablas de estado. Se deben incluir en este archivo todas las subredes que se conectan a la red local mediante enrutadores. Para obtener más información, consulte la página del comando <code>man networks(4)</code> .
<code>/etc/inet/protocols</code>	Este archivo enumera los protocolos TCP/IP instalados en el sistema, además de sus números de protocolo. Este archivo rara vez requiere administración. Para obtener más información, consulte la página del comando <code>man protocols(4)</code> .
<code>/etc/inet/services</code>	Este archivo enumera los nombres de los servicios TCP y UDP, además de sus números de puerto conocidos. Los programas que llaman a los servicios de red utilizan esta lista. Por lo general, este archivo no requiere ninguna administración. Para obtener más información, consulte la página del comando <code>man services(4)</code> .

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 información sobre el uso de los comandos SMF, consulte [“Utilidades administrativas de la línea de comandos de la SMF” de Administración de Oracle Solaris: tareas comunes](#).
- 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 71](#).
- Para obtener información sobre cómo agregar servicios que manejen solicitudes IPv4 e IPv6, consulte [“Daemon de servicios de Internet inetd” en la página 145](#).

El servicio SMF name-service/switch

El servicio SMF `name-service/switch` define el orden de búsqueda de información de configuración en las bases de datos de red. Parte de la información de configuración de red que antes estaba almacenada en los archivos de configuración, como el dominio predeterminado, se convirtió en las propiedades de este servicio SMF. Las propiedades de este servicio SMF determinan la implementación de los servicios de nombres en el sistema. Las propiedades se enumeran de la siguiente manera:

```
% svccfg -s name-service/switch listprop config
config                                application
config/value_authorization           astring          solaris.smf.value.name-service.switch
config/default                       astring          files
config/password                      astring          "files nis"
```

config/group	astring	"files nis"
config/host	astring	"files dns nis"
config/network	astring	"nis [NOTFOUND=return] files"
config/protocol	astring	"nis [NOTFOUND=return] files"
config/rpc	astring	"nis [NOTFOUND=return] files"
config/ether	astring	"nis [NOTFOUND=return] files"
config/netmask	astring	"files nis"
config/bootparam	astring	"nis [NOTFOUND=return] files"
config/publickey	astring	"nis [NOTFOUND=return] files"
config/netgroup	astring	nis
config/automount	astring	"files nis"
config/alias	astring	"files nis"
config/service	astring	"files nis"
config/printer	astring	"user nis"
config/auth_attr	astring	"files nis"
config/prof_attr	astring	"files nis"
config/project	astring	"files nis"

Los valores establecidos para cada una de las propiedades determinan en qué servicio de nombres se debe buscar la información que puede afectar a los usuarios de la red, como contraseñas, alias o máscaras de red. En el ejemplo, las propiedades de montaje automático y de contraseñas están establecidas en `files` y `nis`. De esta manera, la información de montaje automático y de contraseñas se obtiene de los archivos y del servicio NIS.

Si desea cambiar de un servicio de nombres a otro, debe configurar las propiedades pertinentes del servicio SMF `name-service/switch` para habilitar el servicio de nombres seleccionado.

Por ejemplo, suponga que desea utilizar el servicio de nombres LDAP en la red. Se deben configurar las siguientes propiedades del servicio SMF:

- `config/default` se debe configurar para utilizar archivos y LDAP.
- `config/host` se debe configurar para utilizar archivos y DNS.
- `config/netgroup` se debe configurar para utilizar LDAP.
- `config/printer` se debe configurar para utilizar usuarios, archivos y LDAP.

Por lo tanto, debe escribir los comandos siguientes para configurar estas propiedades correctamente.

```
# svccfg -s name-service/switch setprop config/default = astring: "files ldap"
# svccfg -s name-service/switch setprop config/host = astring: "files dns"
# svccfg -s name-service/switch setprop config/netgroup = astring: "ldap"
# svccfg -s name-service/switch setprop config/printer = astring: "user files ldap"
# svccfg -s name-service/switch:default refresh
```

Para obtener detalles completos sobre el cambio de servicios de nombres, consulte [Oracle Solaris Administration: Naming and Directory Services](#).

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.

Las bases de datos de red se utilizan de la siguiente manera:

- Las redes que utilizan archivos locales para el servicio de nombres dependen de los archivos de los directorios `/etc/inet` y `/etc`.
- NIS utiliza bases de datos denominadas mapas NIS.
- DNS utiliza registros con información de host.

Nota – Los archivos de datos e inicio DNS no se corresponden directamente con las bases de datos de red.

Consulte *Oracle Solaris Administration: Naming and Directory Services* para obtener información sobre las correspondencias de bases de datos de red en NIS, DNS y LDAP.

Protocolos de enrutamiento en Oracle Solaris

Esta sección describe dos protocolos de enrutamiento que admite Oracle Solaris: el protocolo de información de enrutamiento (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 en Oracle Solaris, consulte la [Tabla 8–1](#) y la [Tabla 8–2](#).

Protocolo de información de enrutamiento (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)`.

Tablas de protocolos de enrutamiento en Oracle Solaris

En la siguiente tabla, se enumeran todos los protocolos de enrutamiento admitidos en Oracle Solaris.

TABLA 8–1 Protocolos de enrutamiento de Oracle Solaris

Protocolo	Daemon asociado	Descripción	Para obtener instrucciones
Protocolo de información de enrutamiento (RIP)	<code>in.routed</code>	IGP que enruta paquetes IPv4 y mantiene una tabla de enrutamiento	"Configuración de un enrutador IPv4" en la página 57
Descubrimiento de enrutador de protocolo de mensajes de control de Internet (ICMP)	<code>in.routed</code>	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 65 y "Cómo habilitar el enrutamiento dinámico en un sistema de interfaz única" en la página 67
Protocolo de información de enrutamiento, nueva generación (RIPng)	<code>in.ripngd</code>	IGP que enruta paquetes IPv6 y mantiene una tabla de enrutamiento	"Cómo configurar un enrutador habilitado para IPv6" en la página 80

TABLA 8-1 Protocolos de enrutamiento de Oracle Solaris (Continuación)

Protocolo	Daemon asociado	Descripción	Para obtener instrucciones
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 77

En la siguiente tabla, se enumeran los protocolos Quagga admitidos en Oracle Solaris.

TABLA 8-2 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.
Protocolo de portal de límite (BGP)	bgpd	Protocolo EGP para IPv4 y IPv6 para el enrutamiento en dominios administrativos.

Referencia de IPv6

Este capítulo proporciona la siguiente información de referencia relativa a la implementación de IPv6 en Oracle Solaris.

- “Implementación de IPv6 en Oracle Solaris” en la página 151
- “Protocolo ND de IPv6” en la página 163
- “Enrutamiento de IPv6” en la página 170
- “Extensiones de IPv6 para servicios de nombres de Oracle Solaris” en la página 172
- “Admisión de NFS y RPC IPv6” en la página 172
- “Admisión de IPv6 en ATM” en la página 172

Para obtener una descripción general de IPv6, consulte el [Capítulo 3, “Introducción a IPv6 \(descripción general\)”](#) de *Guía de administración del sistema: servicios IP*. Para obtener información sobre tareas relativas a la configuración de redes permitidas para IPv6, consulte el [Capítulo 4, “Habilitación de IPv6 en una red”](#). Para obtener información completa sobre los túneles IP, consulte el [Capítulo 6, “Configuración de túneles IP”](#).

Implementación de IPv6 en Oracle Solaris

Esta sección describe los archivos, comandos y daemons que habilitan IPv6 en Oracle Solaris. Para obtener una descripción general detallada de las direcciones IPv6 y del formato del encabezado IPv6, consulte “[Formatos de direcciones IPv6 que no son los básicos](#)” de *Guía de administración del sistema: servicios IP*.

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 152
- “[Archivo de configuración `/etc/inet/ipaddrsel.conf`](#)” en la página 155

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 9-1 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 9-2 Variables de configuración de interfaz de `/etc/inet/ndpd.conf`

Variable	Predeterminado	Definición
<code>AdvRetransTimer</code>	0	Especifica el valor del campo <code>RetransTimer</code> en los mensajes de anuncio que envía el enrutador.
<code>AdvCurHopLimit</code>	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.
<code>AdvDefaultLifetime</code>	3 + <code>MaxRtrAdvInterval</code>	Especifica la vida útil predeterminada de los anuncios de enrutador.

TABLA 9-2 Variables de configuración de interfaz de /etc/inet/ndpd.conf (Continuación)

Variable	Predeterminado	Definición
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 80 .
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 86 .
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 84 .
TmpMaxDesyncFactor	600 segundos	Especifica un valor aleatorio que se debe sustraer de la variable de vida útil preferente <code>TmpPreferredLifetime</code> al iniciarse <code>in.ndpd</code> . La finalidad de la variable <code>TmpMaxDesyncFactor</code> es impedir que todos los sistemas de la red vuelvan a generar sus direcciones temporales al mismo tiempo. <code>TmpMaxDesyncFactor</code> 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 84 .

TABLA 9-2 Variables de configuración de interfaz de /etc/inet/ndpd.conf (Continuación)

Variable	Predeterminado	Definición
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 84 .
TmpValidLifetime	Falso	Establece la vida útil válida de una dirección temporal. Para obtener más información, consulte “Cómo configurar una dirección temporal” en la página 84 .

En la siguiente tabla se muestran las variables que se utilizan para configurar prefijos IPv6.

TABLA 9-3 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 indicador on-link ("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 9-1 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
#
# Per interface configuration variables
#
#DupAddrDetectTransmits
#AdvSendAdvertisements
#MaxRtrAdvInterval
#MinRtrAdvInterval
#AdvManagedFlag
#AdvOtherConfigFlag
#AdvLinkMTU
#AdvReachableTime
#AdvRetransTimer
```

EJEMPLO 9-1 Archivo `/etc/inet/ndpd.conf` (Continuación)

```
#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 `/etc/inet/ipaddrsel.conf`

El archivo `/etc/inet/ipaddrsel.conf` contiene la tabla de directrices de selección de direcciones predeterminadas de IPv6. Al instalar Oracle Solaris habilitado para IPv6, este archivo incluye el contenido que se muestra en la [Tabla 9-4](#).

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 114](#). Para obtener más información sobre `ipaddrsel.conf`, consulte “[Motivos para modificar la tabla de directrices de selección de direcciones IPv6](#)” en la [página 156](#) y la página del comando `man ipaddrsel.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 ipaddrsel

El comando `ipaddrsel` 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/ipaddrsel.conf` contiene la tabla de políticas.

En la tabla siguiente se enumeran los formatos de direcciones predeterminadas y las correspondientes prioridades en la tabla de directrices. En la página del comando [man inet6\(7P\)](#) hay más información referente a aspectos técnicos sobre la selección de direcciones IPv6.

TABLA 9-4 Tabla de directrices de selección de direcciones IPv6

Prefijo	Prioridad	Definición
::1/128	50	Bucle de retorno
::/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. Luego, puede utilizar el comando `ipadm` para marcar estas direcciones como preferidas. Para obtener más información sobre el comando `ipadm`, consulte la página del comando `man ipadm(1M)`.
- 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 del 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 122. Si decide habilitar la compatibilidad con enrutadores de relé 6to4, consulte “[Cómo crear y configurar un túnel IP](#)” en la página 127 para conocer los procedimientos relacionados.

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 del comando `man 6to4relay(1M)`.

EJEMPLO 9-2 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 9-3 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 9-4 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.

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 del 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 del comando `man netstat(1M)` para

obtener más información. Consulte [“Cómo visualizar el estado de los sockets” en la página 98](#) 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 del comando man [snoop\(1M\)](#) para obtener más información. Consulte [“Cómo supervisar tráfico de redes IPv6” en la página 109](#) 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 del 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 del 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 101](#).

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 del 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 105.

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 9–1](#) 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 de información de enrutamiento de próxima generación (RIPng) 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 utiliza 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 SMF, consulte [“Utilidades administrativas de la línea de comandos de la SMF” de Administración de Oracle Solaris: tareas comunes](#).
- 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 71](#).

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>). Para obtener una descripción general de las funciones principales del descubrimiento de vecinos, consulte “Descripción general del protocolo ND de IPv6” de *Guía de administración del sistema: servicios IP*.

Esta sección trata sobre las características siguientes del protocolo ND:

- “Mensajes de ICMP del protocolo ND” en la página 164
- “Proceso de configuración automática” en la página 164
- “Solicitud e inasequibilidad de vecinos” en la página 166
- “Algoritmo de detección de direcciones duplicadas” en la página 167
- “Comparación del protocolo ND con ARP y protocolos relacionados con IPv4” en la página 168

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 controlar 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 unidad de transmisión máxima (MTU, Maximum Transmission Unit) 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.

Enrutamiento 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.

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 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

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 175
- “Ventajas del uso de DHCP” en la página 176
- “Funcionamiento de DHCP” en la página 177
- “Servidor DHCP de ISC” en la página 180
- “Cliente DHCP” en la página 181

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

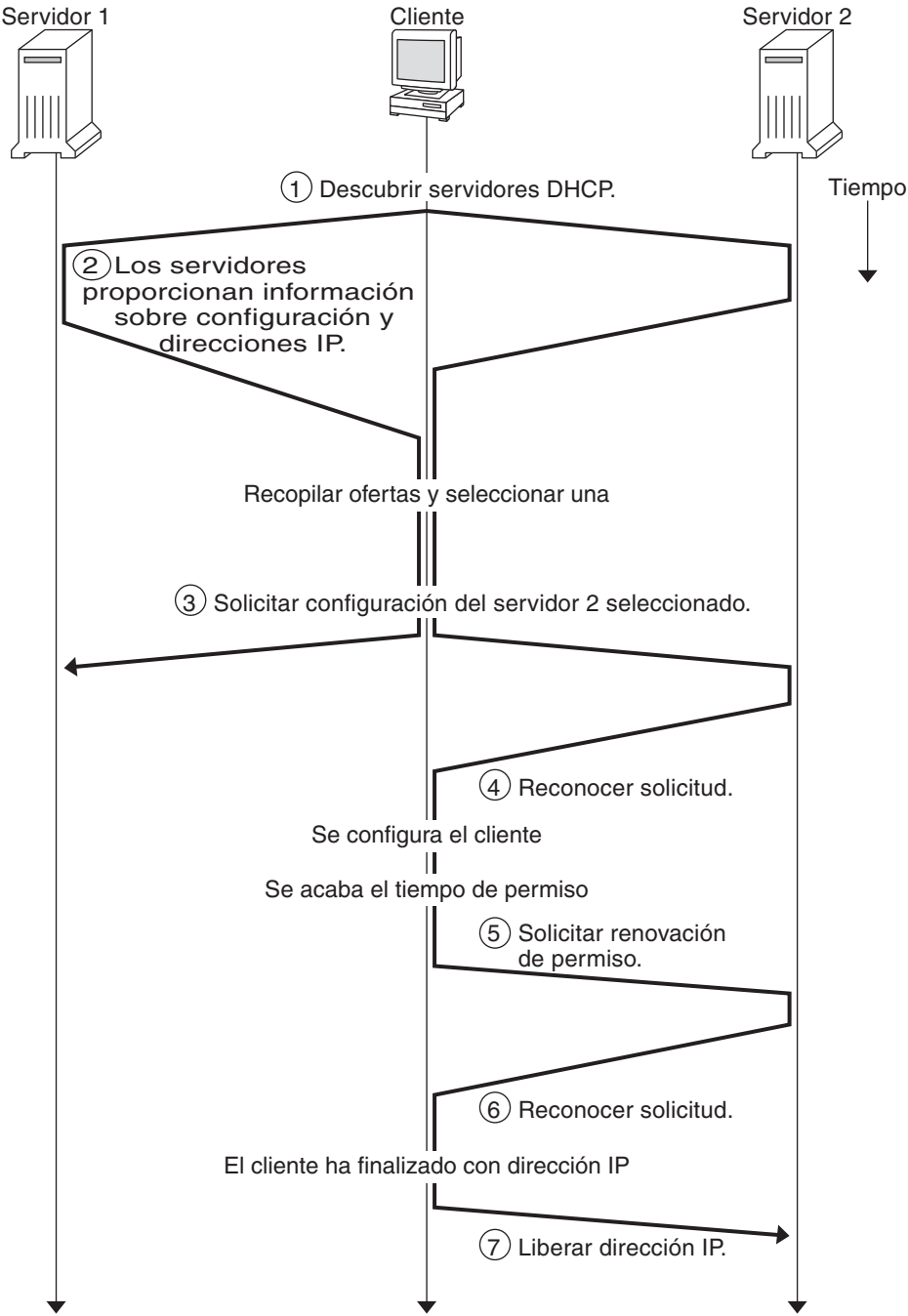
administrar grandes cantidades de datos. El acceso de los almacenes de datos se administra mediante módulos de procesamiento independientes. Este tipo de almacén de datos permite la compatibilidad para cualquier base de datos que se necesite.

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 10-1 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 política 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.

Servidor DHCP de ISC

Una implementación del servidor DHCP de Internet Systems Consortium (ISC) se agregó a Oracle Solaris. Debido a que este software no se instala automáticamente, puede agregar este servidor al sistema escribiendo el siguiente comando:

```
# pkg install pkg:/service/network/dhcp/isc-dhcp
```

El servidor DHCP de ISC, `dhcpcd`, implementa el protocolo de configuración dinámica de host (DHCP) y el protocolo de arranque de Internet (BOOTP). El DHCP permite que los hosts de una red TCP/IP soliciten y sean asignados direcciones IP, y, además, que detecten información sobre la red a la cual están conectados. BOOTP proporciona una funcionalidad similar.

A continuación, se enumeran algunas de las incorporaciones importantes a la versión para DHCP:

- Se agregaron varios servicios para admitir el DHCP de ISC y el servicio DHCP de Sun antiguo. Consulte [“Servicios SMF usados por el servicio DHCP” en la página 208](#) para obtener una lista de todos los servicios utilizados por el DHCP.
- Se agregaron tres comandos: `dhcpcd`, `dhcprelay` y `omshell`. Consulte [“Archivos que utiliza el servicio DHCP” en la página 207](#) para obtener una lista de todos los comandos asociados con el DHCP.
- Para el DHCP de ISC, los archivos de configuración del servidor son `/etc/inet/dhpcpd4.conf` para DHCPv4 y `/etc/inet/dhpcpd6.conf` para DHCPv6.
- Un usuario denominado `dhcpserv` se agregó para el servicio DHCP de ISC.
- Los accesos a los tres comandos nuevos se pueden gestionar mediante las autorizaciones `solaris.smf.manage.dhcp` y `solaris.smf.value.dhcp`.

Para obtener más información sobre el DHCP de ISC, consulte la página web [ISC DHCP Documentation](#).

Servidor DHCP de Sun antiguo

El software del servidor DHCP de Sun antiguo aún viene incluido en la versión Oracle Solaris 11, pero está marcado como obsoleto y se eliminará en versiones futuras. Para obtener más información sobre el servicio DHCP antiguo, consulte el [Chapter 11, Administración del servicio DHCP de ISC](#).

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 (dhcpcagent) que se ejecuta en Oracle Solaris en un sistema configurado para recibir su configuración de red de un servidor DHCP. El cliente DHCP puede interoperar con el servidor DHCP de Sun antiguo y con el servidor DHCP de ISC.

Consulte el [Capítulo 12, “Configuración y administración del cliente DHCP”](#) para obtener información detallada sobre el cliente DHCP.

Administración del servicio DHCP de ISC

En este capítulo, se describen las tareas que le pueden ser de utilidad durante la administración del servicio DHCP de ISC. Contiene los temas siguientes:

- “Configuración del acceso de usuario a los comandos de DHCP” en la página 183
- “Tareas del servidor DHCP” en la página 184

Configuración del acceso de usuario a los comandos de DHCP

De manera predeterminada, sólo el usuario `root` puede ejecutar `svcadm` y otros comandos que son necesarios para configurar el servicio DHCP. 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 inicial de RBAC (mapa de tareas)” de *Administración de Oracle Solaris: 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 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de gestión de DHCP.**

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

- 2 **Agregue un usuario o rol al archivo `/etc/user_attr`.**

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
```

Tareas del servidor DHCP

▼ Cómo configurar un servidor DHCP de ISC

Puede usar estos pasos para configurar inicialmente un servidor DHCP de ISC.

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de gestión de DHCP.**

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

- 2 **Edite el archivo de configuración de DHCP.**

Cree el archivo `/etc/dhcp/dhcpd4.conf` o `/etc/dhcp/dhcpd6.conf`. Para obtener más información, consulte la página del comando `man dhcpd.conf(5)`.

- 3 **Habilite el servicio necesario.**

```
# svcadm enable service
```

El *servicio* puede ser uno de los siguientes valores:

<code>svc:/network/dhcp/server:ipv4</code>	Proporciona solicitudes DHCP y BOOTP de clientes IPv4
--	---

<code>svc:/network/dhcp/server:ipv6</code>	Proporciona solicitudes DHCP y BOOTP de clientes IPv6
<code>svc:/network/dhcp/relay:ipv4</code>	Reenvía solicitudes DHCP y BOOTP de clientes IPv4 a una red con un servidor DHCP
<code>svc:/network/dhcp/relay:ipv6</code>	Reenvía solicitudes DHCP y BOOTP de clientes IPv6 a una red con un servidor DHCP

▼ Cómo modificar la configuración del servicio DHCP

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de gestión de DHCP.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración inicial de RBAC \(mapa de tareas\)](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

- 2 **Edite el archivo de configuración de DHCP.**

Edite el archivo `/etc/dhcp/dhcpd4.conf` o `/etc/dhcp/dhcpd6.conf`. Para obtener más información, consulte la página del comando `man dhcpd.conf(5)`.

- 3 **Refresque los datos SMF.**

```
# svcadm refresh service
```


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 contrapartida sin estado para obtener parámetros de configuración.

Este capítulo contiene la información siguiente:

- “Acerca del cliente DHCP” en la página 187
- “Habilitación y deshabilitación de un cliente DHCP” en la página 195
- “Administración del cliente DHCP” en la página 196
- “Sistemas cliente DHCP con varias interfaces de red” en la página 199
- “Nombres de host de cliente DHCPv4” en la página 199
- “Sistemas cliente DHCP y servicios de nombres” en la página 201
- “Secuencias de eventos de cliente DHCP” en la página 203

Acerca del cliente DHCP

El cliente DHCP es el daemon `dhcpgent`. Si instala Oracle Solaris mediante el instalador de la interfaz gráfica de usuario de LiveCD, los protocolos DHCPv4 y DHCPv6 se habilitan en el sistema instalado. Si instala Oracle Solaris mediante el instalador de texto, se le solicita que seleccione el modo en que la red se debe configurar en el sistema instalado. Si especifica la configuración automática de red, los protocolos DHCPv4 y DHCPv6 se habilitan en el sistema instalado.

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 [“Habilitación y deshabilitación de un cliente DHCP” en la página 195](#) 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.

Diferencias entre DHCPv4 y DHCPv6

Las dos diferencias principales entre DHCPv4 y DHCPv6 son las siguientes:

- **El modelo de administración**
 - DHCPv4: el administrador habilita 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 es proporcionada por los anuncios de enrutador, no por el servidor DHCPv6. No existe la opción de nombre de host DHCPv6.

El modelo administrativo de DHCP

DHCPv4 requiere una configuración de cliente explícita. Debe configurar el sistema DHCPv4 para realizar el direccionamiento cuando lo desee, lo que, por lo general, se realiza durante la instalación inicial del sistema o dinámicamente mediante el uso del comando `ipadm`. Consulte la página del comando `man ipadm(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 se 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 (bge0:1), 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 mediante la función `getaddrinfo(3SOCKET)`) para averiguar la información de nombre correspondiente. Esto implica que si solamente utiliza DHCPv6 y desea que un nodo tenga un nombre específico, debe especificar el nombre del nodo mediante el comando `svccfg`, de la siguiente manera:

```
# svccfg -s svc:/system/identity:node setprop config/nodename = astring: hostname
```

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):

bge0.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 el control de DHCP, de modo que, aunque DHCPv6 se ejecute en esa interfaz (que se denomina también interfaz “física”), sólo 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 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 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:

```
bge0.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:

```
bge0.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.

Sin embargo, para DHCPv4 se debe solicitar el inicio del cliente, si no se hizo durante la instalación de Oracle Solaris. Consulte [“Cómo habilitar un cliente DHCP” en la página 195](#).

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 lo puede detener con el comando `ipadm delete-addr`. 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`.

En el siguiente ejemplo, se muestra cómo cerrar DHCPv6 de inmediato:

```
ex# echo ifdefault StatefulAddrConf false >> /etc/inet/ndpd.conf
ex# pkill -HUP -x in.ndpd
ex# ipadm delete-addr -r dhcp-addrobj
```

En el inicio, si existen configuraciones persistentes de DHCP en el sistema, `dhcpgent` se inicia como parte de los procesos de secuencias de comandos de inicio. `dhcpgent` configura las interfaces de red, como se describe en [“Funcionamiento de DHCP” en la página 177](#).

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 `ipadm`:

```
ipadm delete-addr objeto_dirección_dhcp
```


o

```
ipadm delete-addr -r objeto_dirección_dhcp
```

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 10, “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 `ipadm` 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 `dhcpage` 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, `dhcpage` llama a dicho archivo. Consulte [“Secuencias de eventos de cliente DHCP” en la página 203](#) 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 que asignó las direcciones para indicarle que ya no utilizará una o varias de las direcciones asignadas. Cuando el sistema cliente DHCPv4 se cierra normalmente, `dhcpgent` escribe la información de la configuración actual en un archivo (si el archivo existe). El nombre de archivo para DHCPv4 es `/etc/dhcp/interface.dhc` y `/etc/dhcp/interface.dh6` es para DHCPv6. De manera predeterminada, el permiso se suele guardar en vez de liberar, de modo que el servidor DHCP no puede detectar que la dirección IP no se está usando de forma activa, lo que permite al cliente recuperar fácilmente la dirección en el siguiente inicio. La acción predeterminada es la misma que el comando `ipadm delete-addr dhcp-addrobj`.

Si el permiso en ese archivo aún es válido cuando el sistema se reinicia, `dhcpage` 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, `dhcpage` 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, `dhcpage` inicia la secuencia del protocolo DHCP que se describe en [“Funcionamiento de DHCP” en la página 177](#). El resultado es que el cliente obtiene nueva información de configuración de red.

Habilitación y deshabilitación 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 un cliente DHCP

Este procedimiento sólo debe efectuarse si no se activó DHCPv4 durante la instalación de Oracle Solaris. Nunca es necesario para DHCPv6.

1 Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de gestión 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 183](#).

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

2 Reconfigure el sistema.

Escoja uno de los siguientes métodos de configuración:

- **Reconfigure el sistema de manera interactiva.**

- # `sysconfig configure`

Cuando la herramienta interactiva de configuración del sistema se inicia, seleccione la configuración automática de red en la pantalla Red.

- **Reconfigure el sistema de manera no interactiva.**

`sysconfig configure -c sc_profile`

Consulte la página del comando `man sysconfig(1M)` para obtener más información sobre el uso del archivo de configuración `sc_profile`.

▼ **Cómo deshabilitar un cliente DHCP**

- 1 **Conviértase en superusuario o asuma un rol o nombre de usuario asignado al perfil de gestión 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 183.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “Configuración inicial de RBAC (mapa de tareas)” de *Administración de Oracle Solaris: servicios de seguridad*.

- 2 **Reconfigure el sistema.**

Escoja uno de los siguientes métodos de configuración:

- **Reconfigure el sistema de manera interactiva.**

`sysconfig configure`

Cuando la herramienta interactiva de configuración del sistema se inicia, seleccione Manual o Ninguna como la configuración de red en la pantalla Red.

- **Reconfigure el sistema de manera no interactiva.**

`sysconfig configure -c sc_profile`

Consulte la página del comando `man sysconfig(1M)` para obtener más información sobre el uso del archivo de configuración `sc_profile`.

Administración del cliente DHCP

El software de cliente DHCP no requiere administración si el sistema se utiliza normalmente. El daemon `dhcpgent` 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 `dhcpgent` directamente. En vez de eso, como superusuario del sistema cliente, puede utilizar el comando `ipadm` para modificar la gestión que `dhcpgent` efectúa de la interfaz de red, si es necesario.

Opciones del comando `ipadm` usadas con el cliente DHCP

En esta sección, se resumen las opciones del comando, documentadas en la página del comando `man ipadm(1M)`.

El comando `ipadm` le permite realizar lo siguiente:

- **Crear la interfaz IP.** El comando `ipadm create-ip` crea la interfaz IP, que luego usted configura con direcciones IP. Las direcciones pueden ser estáticas o dinámicas. La creación de la interfaz IP es un requisito para poder asignar las direcciones.
- **Iniciar el cliente DHCP.** El comando `ipadm create-addr -T dhcp dhcp-addrobj` inicia la interacción entre `dhcpgent` 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.
- **Solicitar solamente información de configuración de red.** El comando `ipadm refresh-addr -i dhcp-addrobj` hace que `dhcpgent` 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 extensión de permiso.** El comando `ipadm refresh-addr dhcp-addrobj` hace que `dhcpgent` 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 `ipadm delete-addr -r dhcp-addrobj` hace que `dhcpgent` ceda la dirección IP usada por 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/dhcpgent`.
- **Abandonar la dirección IP.** El comando `ipadm delete-addr dhcp-addrobj` hace que `dhcpgent` cierre la interfaz de red sin informar al servidor DHCP y guarde el permiso en el sistema de archivos. Este comando permite al cliente utilizar la misma dirección IP al reiniciar.

Nota – Actualmente, el comando `ipadm` no tiene una funcionalidad equivalente para el comando `ifconfig [inet6] interface status`.

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)`.

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 199](#).
- 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 la página del comando `man dhcpd(8)` y [“Cómo usar macros DHCP \(mapa de tareas\)” de Guía de administración del sistema: servicios IP](#) 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 199](#).
- 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 201](#) 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.

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 203](#).

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 mediante DHCP, el sistema cliente comprueba

el valor establecido en la propiedad `config/nodename` del servicio `svc:/system/identity:node` de un nombre para usarlo como el nombre de host. Si el archivo está vacío, se asigna el nombre de host `unknown` (desconocido).

Si el servidor DHCP proporciona un nombre en la opción `Hostname` del DHCP, el cliente usa ese nombre de host, incluso si un valor diferente se coloca en el valor establecido en la propiedad `config/nodename` del servicio `svc:/system/identity:node`. 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**

Los pasos que se deben realizar dependen de la existencia de una interfaz IP con una dirección DHCP.

- 1 Si la interfaz IP ya existe con una dirección DHCP, realice lo siguiente:
 - a. Elimine la dirección DHCP existente.

```
# ipadm delete-addr -r dhcp-addrobj
```
 - b. Registre una nueva dirección DHCP con un nombre de host específico que desee usar.

```
# ipadm create-addr -T dhcp -h hostname dhcp-addrobj
```
- 2 Si la interfaz IP aún no existe, realice lo siguiente:
 - a. Cree la interfaz IP.

```
# ipadm create-ip interface
```
 - b. Registre una dirección DHCP con un nombre de host específico que desee usar.

```
# ipadm create-addr -T dhcp -h hostname dhcp-addrobj
```


Sistemas cliente DHCP y servicios de nombres

Los sistemas Oracle Solaris admiten los siguientes servicios de nombres: DNS, NIS y un almacén de archivo local (`/etc/inet/hosts`). Cada servicio de nombres requiere configurar algunos aspectos antes de poder utilizarse. El servicio SMF `name-service/switch` también debe estar configurado de manera adecuada. Consulte la página del comando `man nsswitch.conf(4)` para obtener más información.

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 referencias cruzadas a documentación que puede ayudarlo a configurar clientes para cada servicio de nombres.

TABLA 12-1 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>dhcpinfo</code> en el cliente, de la siguiente forma:</p> <pre># /usr/sbin/dhcpinfo NISdmain # /usr/sbin/dhcpinfo NISservs</pre> <p>Nota – Para DHCPv6, incluya <code>-v6</code> y palabras clave de protocolo distintas en el comando, de la siguiente manera:</p> <pre># /usr/sbin/dhcpinfo -v6 NISDomain # /usr/sbin/dhcpinfo -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 6, “Setting Up and Configuring NIS (Tasks)” de Oracle Solaris Administration: Naming and Directory Services.</p> <p>Consejo – Puede escribir una secuencia de comandos que utilice <code>dhcpinfo</code> e <code>yppinit</code> para automatizar la configuración de clientes NIS en sistemas cliente DHCP.</p>
/etc/inet/hosts	<p>Deberá configurar el archivo <code>/etc/inet/hosts</code> para un sistema cliente DHCP que vaya a utilizar <code>/etc/inet/hosts</code> para su servicio de nombres.</p> <p>El nombre de host del sistema cliente DHCP se agrega a su propio archivo <code>/etc/inet/hosts</code> mediante las herramientas de DHCP. Sin embargo, se debe agregar manualmente el nombre de host al archivo <code>/etc/inet/hosts</code> de otros sistemas de la red. Si el sistema servidor DHCP utiliza <code>/etc/inet/hosts</code> para la resolución de nombres, deberá agregar también manualmente el nombre de host del cliente al sistema.</p>
DNS	<p>Si el sistema cliente DHCP recibe el nombre de dominio DNS a través de DHCP, las propiedades del servicio SMF <code>dns/client</code> también se configuran automáticamente. Para obtener más información acerca de DNS, consulte la Oracle Solaris Administration: Naming and Directory Services.</p>

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.

dhcpcagent 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 que 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, `dhcpage` 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 se configura por primera vez para DHCP, `dhcpage` invoca a la secuencia de comandos de eventos de la siguiente forma:

```
/etc/dhcp/eventhook net0 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 `dhcpage`, 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 `dhcpage` espera la salida de la secuencia de eventos para todos los eventos. Si la secuencia de eventos no sale transcurridos 55 segundos, `dhcpage` 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 dhcpagent(1M)` se muestra un ejemplo de secuencia de eventos.

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 205
- “Archivos que utiliza el servicio DHCP” en la página 207
- “Servicios SMF usados por el servicio DHCP” en la página 208

Comandos DHCP

En la tabla siguiente se enumeran los comandos que se pueden utilizar para gestionar DHCP en la red.

TABLA 13-1 Comandos utilizados en DHCP

Orden	Descripción
<code>/usr/lib/inet/dhcpd</code>	Sólo DHCP de ISC: el daemon del servidor DHCP de ISC. Para obtener más información, consulte la página del comando <code>man dhcpd(8)</code> .
<code>/usr/lib/inet/dhcrelay</code>	Sólo DHCP de ISC: permite un medio para retransmitir solicitudes DHCP y BOOTP de un cliente de una red sin servidores DHCP a servidores de otras redes. Para obtener más información, consulte la página de comando <code>man dhcrelay(8)</code> .
<code>/usr/lib/inet/in.dhcpd</code>	Sólo DHCP de Sun antiguo: el daemon del servidor DHCP de Sun antiguo. El daemon se inicia al iniciarse el sistema. No es conveniente iniciar el daemon del servidor directamente. Utilice DHCP Manager, el comando <code>svcadm o dhcpconfig</code> 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. Para obtener más información, consulte la página del comando <code>man in.dhcpd(1M)</code> .

TABLA 13-1 Comandos utilizados en DHCP (Continuación)

Orden	Descripción
<code>/usr/sadm/admin/bin/dhcppmgr</code>	Sólo DHCP de Sun antiguo: el administrador de DHCP, una herramienta de 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. Para obtener más información, consulte la página del comando man dhcppmgr(1M) .
<code>/usr/sbin/dhcpagent</code>	El daemon del cliente DHCP, que implementa el lado del cliente del protocolo DHCP. Para obtener más información, consulte la página del comando man dhcpagent(1M) .
<code>/usr/sbin/dhcpconfig</code>	Sólo DHCP de Sun antiguo: 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. Para obtener más información, consulte la página del comando man dhcpconfig(1M) .
<code>/usr/sbin/dhcpinfo</code>	Sólo DHCP de Sun antiguo: lo utilizan las secuencias de comando de inicio de los sistemas cliente de Oracle Solaris para obtener información (como el nombre de host) para el daemon del cliente DHCP, <code>dhcpagent</code> . También se puede utilizar <code>dhcpinfo</code> en secuencias de comandos o en la línea de comandos para obtener valores de parámetros específicos. Para obtener más información, consulte la página del comando man dhcpinfo(1) .
<code>/usr/sbin/dhtadm</code>	Sólo DHCP de Sun antiguo: se utiliza para efectuar cambios en las opciones y macros de la tabla <code>dhcptab</code> . Este comando resulta útil en secuencias creadas para automatizar los cambios en la información DHCP. Utilice <code>dhtadm</code> con la opción <code>-P</code> y redirija la salida al comando <code>grep</code> para buscar de forma rápida valores específicos de opciones en la tabla <code>dhcptab</code> . Para obtener más información, consulte la página del comando man dhtadm(1M) .
<code>/usr/sbin/ipadm</code>	Se utiliza en el inicio del sistema para asignar direcciones IP a interfaces de red, configurar parámetros de interfaz de red o ambas funciones. En un cliente DHCP, <code>ipadm</code> inicia DHCP para obtener los parámetros (incluida la dirección IP) necesarios para configurar una interfaz de red. Para obtener más información, consulte la página del comando man ipadm(1M) .
<code>/usr/sbin/omshell</code>	Sólo DHCP de ISC: brinda una manera de consultar y cambiar el estado del servidor DHCP de ISC mediante la API de gestión de objetos (OMAPI). Para obtener más información, consulte la página del comando man omshell(1) .
<code>/usr/sbin/pntadm</code>	Sólo DHCP de Sun antiguo: 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. Para obtener más información, consulte la página del comando man pntadm(1M) .
<code>/usr/sbin/snoop</code>	Se utiliza para capturar y mostrar el contenido de paquetes que circulan por la red. <code>snoop</code> resulta útil para solucionar problemas del servicio DHCP. Para obtener más información, consulte la página del comando man snoop(1M) .

Archivos que utiliza el servicio DHCP

En la siguiente tabla, se enumeran los archivos asociados con DHCP.

TABLA 13-2 Archivos y tablas utilizados por los daemons y comandos DHCP

Nombre de archivo o tabla	Descripción
dhcptab	Sólo DHCP de Sun antiguo: un término genérico para la tabla que contiene la información de configuración de DHCP registrada en forma de opciones con valores asignados y luego agrupadas en forma de macros. El nombre de la tabla dhcptab y su ubicación son determinados por el almacén de datos que se utiliza para la información DHCP. Para obtener más información, consulte la página del comando man dhcptab(4) .
Tabla de red DHCP	Sólo DHCP de Sun antiguo: 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 10.21.32.0. No hay ningún archivo llamado dhcp_network. El nombre y la ubicación de las tablas de red DHCP son determinados por el almacén de datos utilizado para la información DHCP. Para obtener más información, consulte la página del comando man dhcp_network(4) .
/etc/dhcp/eventhook	Sólo DHCP de Sun antiguo: una secuencia de comandos o un archivo ejecutable que el daemon dhcpagent puede ejecutar de manera automática. Para obtener más información, consulte la página del comando man dhcpagent(1M) .
/etc/inet/dhcpd4.conf /etc/inet/dhcpd6.conf	Sólo DHCP de ISC: Contiene información de configuración para el servidor DHCP de ISC, dhcpd. Para obtener más información, consulte la página de comando man dhcpd.conf(5) .
/etc/inet/dhcpsvc.conf	Sólo DHCP de Sun antiguo: almacena opciones de inicio para el daemon DHCP e información de almacenamiento de datos. Este archivo no debe editarse de forma manual. Utilice el comando dhcpconfig para modificar las opciones de inicio. Para obtener más información, consulte la página del comando man dhcpsvc.conf(4) .
/etc/dhcp/interfaz.dhc /etc/dhcp/interface.dh6	Contiene los parámetros de configuración obtenidos de DHCP para la interfaz de red especificada. Para DHCPv4, el nombre de archivo termina con dhc. Para DHCPv6, el nombre de archivo termina con dh6. El cliente guarda la información de configuración actual en /etc/dhcp/interface.dhc cuando se termina el permiso de la dirección IP actual. Por ejemplo, si se usa DHCP en la interfaz qe0, dhcpagent guarda la información de configuración en /etc/dhcp/qe0.dhc. 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.
/etc/default/dhcpagent	Establece valores de parámetros para el daemon de cliente dhcpagent. Consulte el archivo /etc/default/dhcpagent o la página del comando man dhcpagent(1M) para obtener información sobre los parámetros.

TABLA 13-2 Archivos y tablas utilizados por los daemons y comandos DHCP (Continuación)

Nombre de archivo o tabla	Descripción
/etc/dhcp/inittab /etc/dhcp/inittab6	<p>Sólo DHCP de Sun antiguo: define diversos aspectos de códigos de opciones DHCP, como el tipo de datos, y asigna etiquetas mnemónicas. Consulte la página del comando <code>man dhcp_inittab(4)</code> para más información acerca de la sintaxis del archivo. El archivo <code>/etc/dhcp/inittab6</code> es utilizado por clientes DHCPv6.</p> <p>En el cliente, la información del archivo <code>/etc/dhcp/inittab</code> es utilizada por el comando <code>dhcpinfo</code> para proporcionar información más significativa a los lectores 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.</p>
/var/db/isc-dhcp/dhcp4.leases /var/db/isc-dhcp/dhcp4.leases- /var/db/isc-dhcp/dhcp6.leases /var/db/isc-dhcp/dhcp6.leases-	<p>Sólo DHCP de ISC: enumera permisos para servidores DHCPv4 y DHCPv6. Archivos con “-” al final del nombre de archivo son copias anteriores.</p>

Servicios SMF usados por el servicio DHCP

En la siguiente tabla, se enumeran los servicios SMF asociados con DHCP.

TABLA 13-3 Servicios SMF usados por comandos y daemons DHCP

Nombre de servicio SMF	Descripción
svc:/network/dhcp-server:default	Contiene información para el servicio DHCP de Sun antiguo.
svc:/network/dhcp/server:ipv4 svc:/network/dhcp/server:ipv6	Contiene información para el servicio DHCP de ISC.
svc:/network/dhcp/relay:ipv4 svc:/network/dhcp/relay:ipv6	Contiene información para el servicio que puede retransmitir solicitudes DHCP o BOOTP a un servidor DHCP de ISC remoto.
svc:/network/dns/client	Contiene información usada para resolver consultas DNS. Durante la configuración del servidor DHCP, este servicio SMF se consulta para obtener información acerca del dominio DNS y del servidor DNS.
svc:/system/name-service/switch	Especifica la ubicación de las bases de datos de servicios de nombres y el orden en que se debe buscar en los servicios de nombres diversos tipos de información. Este servicio brinda información de configuración precisa al configurar un servicio DHCP.

P A R T E I I I

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. La función de filtro IP de Oracle Solaris 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:

- “Introducción a IPsec” en la página 211
- “Flujo de paquetes IPsec” en la página 214
- “Asociaciones de seguridad IPsec” en la página 217
- “Mecanismos de protección de IPsec” en la página 218
- “Políticas de protección IPsec” en la página 221
- “Modos de transporte y túnel en IPsec” en la página 221
- “Redes privadas virtuales e IPsec” en la página 224
- “Paso a través de IPsec y NAT” en la página 224
- “IPsec y SCTP” en la página 225
- “IPsec y zonas de Oracle Solaris” en la página 226
- “IPsec y dominios lógicos” en la página 226
- “Archivos y utilidades IPsec” en la página 226

Para implementar IPsec en la red, consulte el [Capítulo 15, “Configuración de IPsec \(tareas\)”](#).

Para obtener información de referencia, consulte el [Capítulo 16, “Arquitectura de seguridad IP \(referencia\)”](#).

Introducción a IPsec

IPsec protege los paquetes IP autenticándolos, cifrándolos o llevando a cabo ambas acciones. IPsec se realiza dentro del módulo IP. Por tanto, una aplicación de Internet puede aprovechar IPsec aunque no esté configurada para el uso de IPsec. Cuando se utiliza correctamente, la política IPsec es una herramienta eficaz para proteger el tráfico de la red.

La protección IPsec incluye los siguientes componentes principales:

- **Protocolos de seguridad:** mecanismo de protección de datagramas IP. El [encabezado de autenticación](#) (AH) incluye un hash del paquete 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 [carga de seguridad encapsuladora](#) (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.
- **Asociaciones de seguridad (SA):** los parámetros criptográficos y el protocolo de seguridad IP, aplicados a un flujo de tráfico de red específico. Cada SA tiene una referencia exclusiva denominada índice de parámetros de seguridad (SPI).
- **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.
- **Gestión 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 políticas 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.

Si el socket de un puerto está conectado y, posteriormente, se aplica la política 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 política 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” (Documentos de seguridad IP), noviembre de 1998
- RFC 2401, “Security Architecture for the Internet Protocol” (Arquitectura de seguridad para el protocolo de Internet), noviembre de 1998
- RFC 2402, “IP Authentication Header” (Encabezado de autenticación IP), noviembre de 1998
- RFC 2406, “IP Encapsulating Security Payload (ESP)” (Carga de seguridad encapsuladora de IP [ESP]), noviembre de 1998
- RFC 2408, “Internet Security Association and Key Management Protocol (ISAKMP)” (protocolo de gestión de claves y asociaciones de seguridad de Internet [ISAKMP]), noviembre de 1998
- RFC 2407, “The Internet IP Security Domain of Interpretation for ISAKMP” (El dominio de interpretación de seguridad de IP de Internet para ISAKMP), noviembre de 1998
- RFC 2409, “The Internet Key Exchange (IKE)” (Intercambio de claves de Internet [KIE]), noviembre de 1998
- RFC 3554, “On the Use of Stream Control Transmission Protocol (SCTP) with IPsec” (Sobre el uso del protocolo de transmisión para el control de flujo con IPsec), julio de 2003

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 17-1](#).

TABLA 14-1 Términos, acrónimos y usos de IPsec

Término de IPsec	Acrónimo	Definición
Asociación de seguridad	SA	Los parámetros criptográficos y el protocolo de seguridad IP que se aplican a un flujo de tráfico de red específico. La SA se define mediante tres elementos: un protocolo de seguridad, un índice de parámetros de seguridad (SPI) exclusivo y un destino IP.

TABLA 14-1 Términos, acrónimos y usos de IPsec (Continuación)

Término de IPsec	Acrónimo	Definición
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 políticas 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 mediante algoritmos criptográficos asimétricos. Los dos métodos principales son RSA y Diffie-Hellman.
Diffie-Hellman	DH	Un algoritmo de intercambio de claves que permite la generación y la autenticación de claves. A menudo se denomina <i>intercambio de claves autenticadas</i> .
RSA	RSA	Un algoritmo de intercambio de claves que permite la generación y la distribución de claves. El protocolo recibe el nombre de sus tres creadores, Rivest, Shamir y Adleman.
Protocolo de gestión 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 gestionar un intercambio IKE.

Flujo de paquetes IPsec

En la [Figura 14-1](#), se 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 14-2](#) muestra el proceso entrante de IPsec.

FIGURA 14-1 IPsec aplicado al proceso de paquetes salientes

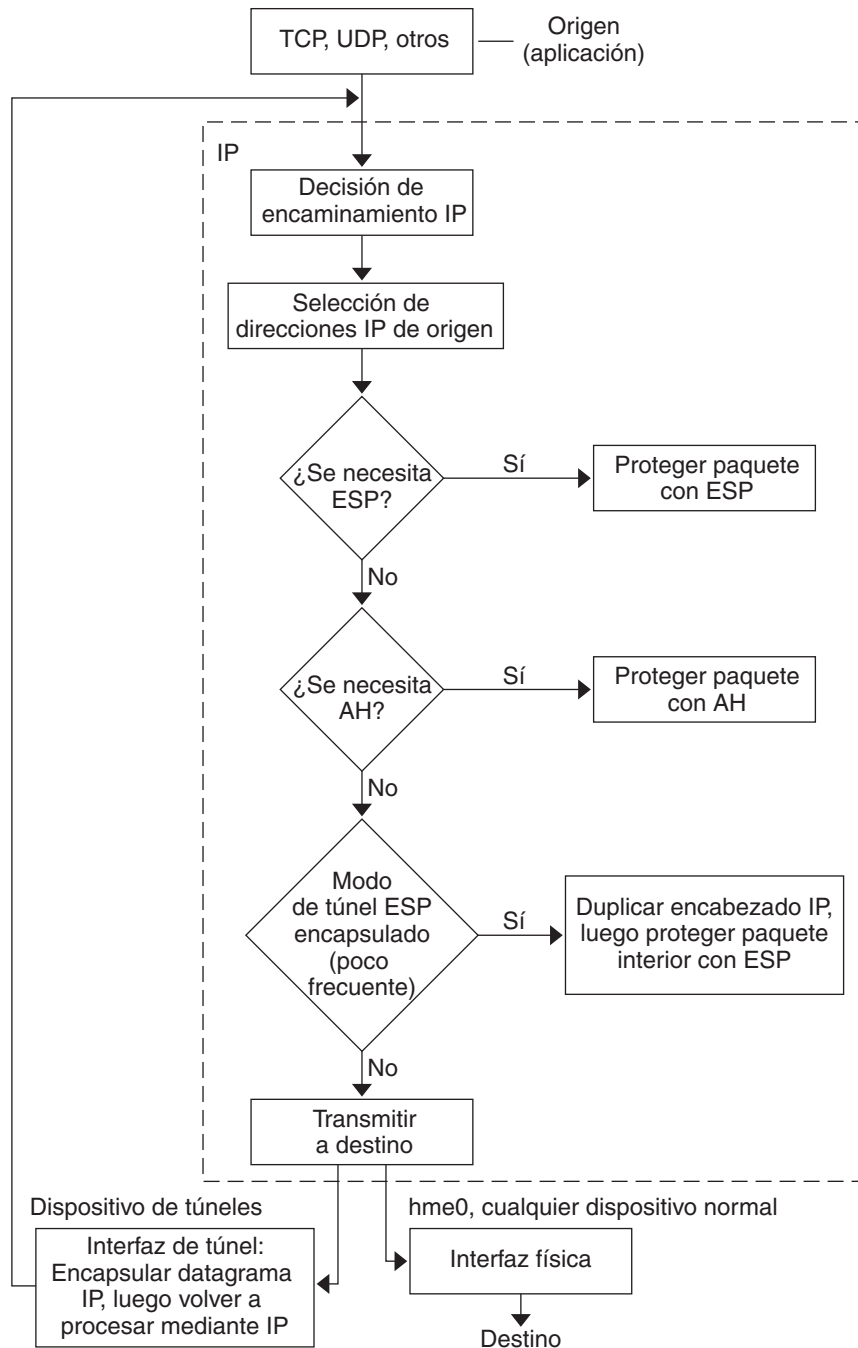
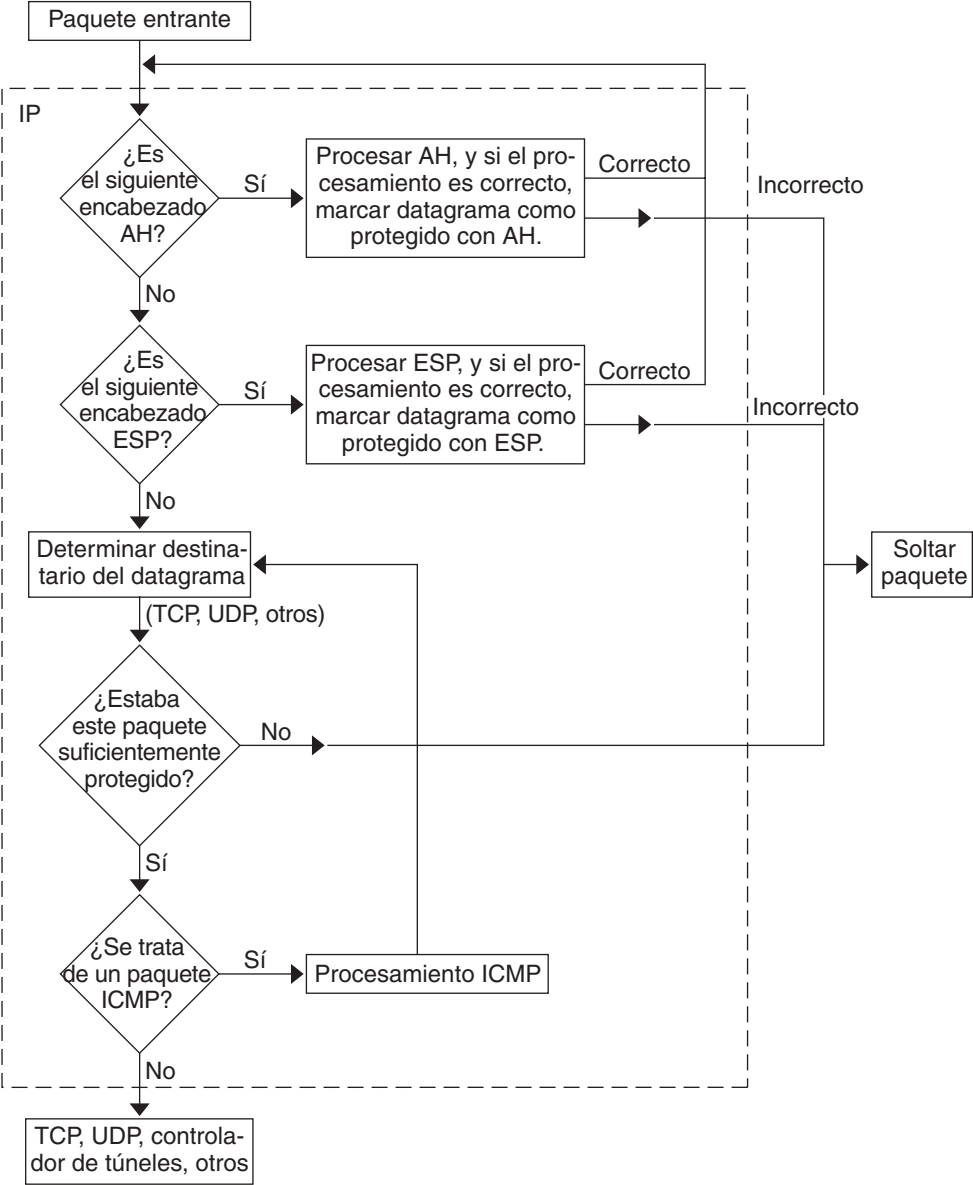


FIGURA 14-2 IPsec aplicado al proceso de paquetes entrantes



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). PF_KEY, una interfaz administrativa basada en sockets, permite que las aplicaciones privilegiadas gestionen 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 255](#).
- Para obtener más información sobre cómo administrar SADB, consulte la [página del comando man pf_key](#) (7P).

Gestión de claves en IPsec

Las asociaciones de seguridad (SA) requieren materiales para la autenticación y para el cifrado. La gestión de este material de claves se denomina *gestión de claves*. El protocolo de intercambio de claves de Internet (IKE) gestiona automáticamente la gestión 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 gestión manual de claves, se prefiere IKE.

La utilidad de gestión de servicios (SMF) de Oracle Solaris proporciona los siguientes servicios de gestión de claves para IPsec:

- Servicio `svc:/network/ipsec/ike:default`: es el servicio SMF para la gestión 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 17, “Intercambio de claves de Internet \(descripción general\)”](#). Para obtener más información sobre el daemon `in.iked`, consulte la página del comando `man in.iked(1M)`. Para obtener información sobre el servicio `ike`, consulte [“Servicio IKE” en la página 301](#).
- Servicio `svc:/network/ipsec/manual-key:default`: es el servicio SMF para la gestión manual de claves. El servicio `manual-key` ejecuta el comando `ipseckey` con varias opciones para administrar claves manualmente. Para obtener una descripción del comando `ipseckey`, consulte [“Utilidades para la generación de SA en IPsec” en la página 255](#). Para obtener más información sobre las opciones del comando `ipseckey`, consulte la página del 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. ESP puede utilizarse, y debería utilizarse, con un mecanismo de autenticación. Si no está atravesando una NAT, puede combinar ESP con AH. De lo contrario, puede utilizar un algoritmo de autenticación y un mecanismo de cifrado con ESP. Un algoritmo de modo combinado, como AES-GCM, proporciona cifrado y autenticación dentro de un único algoritmo.

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 [carga de seguridad encapsuladora \(ESP\)](#) 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.



☐ 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 política 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 221](#).

Consideraciones de seguridad para el uso de AH y ESP

La tabla siguiente compara las protecciones que proporcionan AH y ESP.

TABLA 14–2 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 la carga útil IP. Garantiza la confidencialidad.	Intercepción de comunicaciones
		Con la opción de autenticación, proporciona la misma protección de carga útil que AH.	Repetición, cortar y pegar
		Con ambas opciones, proporciona integridad sólida, autenticación de datos y confidencialidad.	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 utiliza la estructura criptográfica de Oracle Solaris para acceder a los algoritmos. La estructura criptográfica 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.

Para obtener más información, consulte las siguientes direcciones:

- Capítulo 11, “Estructura criptográfica (descripción general)” de *Administración de Oracle Solaris: servicios de seguridad*
- Capítulo 8, “Introduction to the Oracle Solaris Cryptographic Framework” de *Developer’s Guide to Oracle Solaris 11 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*.

Políticas de protección IPsec

Las políticas de protección IPsec pueden utilizar cualquiera de los mecanismos de seguridad. Las políticas IPsec se pueden aplicar en los niveles siguientes:

- En el sistema
- Por socket

IPsec aplica la política 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 política indica que el tráfico debe omitir las demás políticas.

La política que normalmente protege un datagrama se puede omitir. Puede especificar una excepción en la política del sistema, o solicitar una omisión en la política por socket. Para el tráfico de un sistema, se aplican las políticas, pero no se aplican los mecanismos de seguridad reales. En lugar de ello, la política 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 políticas 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 política 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 política IPsec que protege el paquete IP interior.
- En modo túnel, el paquete IP interior determina la política 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 política IPsec. En efecto, IPsec puede aplicar diferentes políticas 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 política 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 política 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 política IPsec se aplica en el contenido del datagrama IP interior. Se pueden aplicar diferentes políticas 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 política. A diferencia del modo transporte, en el modo túnel el encabezado IP exterior no dicta la política de su datagrama IP interior.

Por tanto, en modo túnel, la política IPsec se puede especificar para las subredes de una LAN detrás de un enrutador y para puertos de dichas subredes. La política 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 política 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 política 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 236](#).

En Oracle Solaris, el modo de túnel únicamente se puede aplicar en una interfaz de red de túneles IP. Para obtener información sobre las interfaces de túneles, consulte [Capítulo 6, “Configuración 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 14-3 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 14-4 Paquete IP protegido con información TCP



☐ Cifrado

En modo transporte, AH protege los datos como se muestra en la figura siguiente.

FIGURA 14-5 Paquete protegido por encabezado de autenticación



La protección de AH, incluso en el modo de transporte, abarca la mayor parte del encabezado IP.

En modo túnel, todo el datagrama está *dentro* de la protección de un encabezado IPsec. El datagrama de la [Figura 14-3](#) está protegido en modo túnel por otro encabezado IPsec exterior, en este caso ESP, tal como se muestra en la figura siguiente.

FIGURA 14-6 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 política por socket, consulte la página del comando `man ipsec(7P)`.
- Si desea ver un ejemplo de la política por socket, consulte “[Cómo utilizar IPsec para proteger un servidor web del tráfico que no procede de Internet](#)” en la página 233.
- 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 IPsec en modo de túnel](#)” en la página 239.

Redes privadas virtuales e IPsec

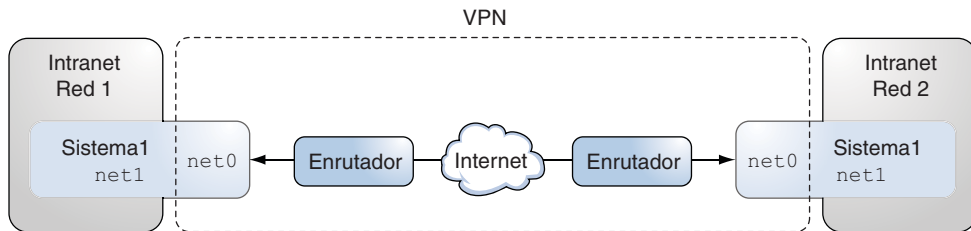
Un túnel configurado es una interfaz de punto a punto. El túnel permite la encapsulación de un paquete IP dentro de otro paquete IP. Un túnel configurado correctamente requiere tanto un origen como un destino. Para obtener más información, consulte [“Cómo crear y configurar un túnel IP” en la página 127](#).

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 agregar protecciones IPsec a una VPN. IPsec protege la conexión. Por ejemplo, una organización que utiliza tecnología VPN para conectar oficinas con redes separadas puede agregar IPsec para proteger el tráfico entre las dos oficinas.

En la figura siguiente, se ilustra cómo dos oficinas forman una VPN con IPsec implementado en sus sistemas de red.

FIGURA 14-7 Red privada virtual



Para ver un ejemplo detallado del procedimiento de configuración, consulte [“Cómo proteger una VPN con IPsec en modo de túnel” en la página 239](#).

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 317](#).

La posibilidad de utilizar IKE cuando hay un cuadro NAT entre los sistemas que se comunican se denomina NAT transversal o NAT-T. NAT-T tiene las siguientes limitaciones:

- El protocolo AH depende de un encabezado IP sin cambios, por lo que AH no puede funcionar 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.

Las siguientes RFC describen la funcionalidad de NAT y los límites de NAT-T. Las copias de RFC se pueden obtener en <http://www.rfc-editor.org>.

- RFC 3022, “Traditional IP Network Address Translator (Traditional NAT)” (Traductor tradicional de direcciones de red IP [NAT tradicional]), enero de 2001
- RFC 3715, “IPsec-Network Address Translation (NAT) Compatibility Requirements” (Requisitos de compatibilidad entre IPsec y la traducción de direcciones de red [NAT]), marzo de 2004
- RFC 3947, “Negotiation of NAT-Traversal in the IKE” (Negociación de NAT transversal en IKE), enero de 2005
- RFC 3948, “UDP Encapsulation of IPsec Packets” (Encapsulación UDP de paquetes IPsec), enero de 2005

Para utilizar IPsec en una NAT, consulte “[Configuración de IKE para sistemas portátiles \(mapa de tareas\)](#)” en la [página 290](#).

IPsec y SCTP

Oracle Solaris admite el protocolo de control de transmisión de flujo (SCTP). Se admite el uso del protocolo SCTP y el número de puerto SCTP para especificar la política 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 política IPsec para SCTP.

SCTP puede utilizar varias direcciones de origen y destino en el contexto de una sola asociación SCTP. Cuando la política 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 política IPsec sólo reconoce la dirección original. Para obtener información sobre SCTP, consulte las RFC y “[Protocolo SCTP](#)” de *Guía de administración del sistema: servicios IP*.

IPsec y zonas de Oracle Solaris

IPsec se configura desde la zona global para las zonas IP compartidas. El archivo de configuración de la política 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 por zona no global.

Para obtener información sobre cómo utilizar IPsec con zonas, consulte [“Protección del tráfico con IPsec” en la página 229](#). Para obtener información sobre las zonas, consulte el [Capítulo 15, “Introducción a Zonas de Oracle Solaris” de Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#).

IPsec y dominios lógicos

IPsec funciona con dominios lógicos. El dominio lógico debe ejecutar una versión de Oracle Solaris que incluya IPsec, como la versión Oracle 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 [Guía de administración del servidor Oracle VM para SPARC 2.1](#) o la [Guía de administración de Oracle VM Server para SPARC 2.0](#).

Archivos y utilidades IPsec

La [Tabla 14–3](#) 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 gestión de claves.

Para obtener más información sobre identificadores de servicio, consulte el [Capítulo 6, “Gestión de servicios \(descripción general\)” de Administración de Oracle Solaris: tareas comunes](#).

- Para obtener instrucciones sobre cómo implementar IPsec en la red, consulte [“Protección del tráfico con IPsec” en la página 229](#).
- Para mas información sobre los archivos y las utilidades IPsec, consulte el [Capítulo 16, “Arquitectura de seguridad IP \(referencia\)”](#).

TABLA 14–3 Lista de archivos y utilidades IPsec seleccionados

Utilidad IPsec, archivo o servicio	Descripción	Página del comando man
<code>svc:/network/ipsec/ipsecalg</code>	El servicio SMF que gestiona los algoritmos IPsec.	ipsecalgs(1M)

TABLA 14-3 Lista de archivos y utilidades IPsec seleccionados (Continuación)

Utilidad IPsec, archivo o servicio	Descripción	Página del comando man
<code>svc:/network/ipsec/manual-key</code>	El servicio SMF que gestiona las SA de IPsec con claves manuales.	ipseckey(1M)
<code>svc:/network/ipsec/policy</code>	El servicio SMF que gestiona la política IPsec.	smf(5) , ipseconf(1M)
<code>svc:/network/ipsec/ike</code>	El servicio SMF para la gestión automática de SA de IPsec mediante IKE.	smf(5) , in.iked(1M)
Archivo <code>/etc/inet/ipsecinit.conf</code>	Archivo de política IPsec. El servicio SMF <code>policy</code> utiliza este archivo para configurar la política IPsec durante el inicio del sistema.	ipseconf(1M)
Comando <code>ipseconf</code>	Comando de política IPsec. Es útil para visualizar y modificar la política IPsec actual, así como para realizar pruebas. El servicio SMF <code>policy</code> lo utiliza para configurar la política IPsec durante el inicio del sistema.	ipseconf(1M)
Interfaz de socket <code>PF_KEY</code>	Interfaz para la base de datos de asociaciones de seguridad (SADB). Controla la gestión de claves manual y automática.	pf_key(7P)
Comando <code>ipseckey</code>	Comando de material de claves de asociaciones de seguridad (SA) de IPsec. <code>ipseckey</code> es un componente frontal de línea de comandos para la interfaz <code>PF_KEY</code> . <code>ipseckey</code> puede crear, destruir o modificar SA.	ipseckey(1M)
Archivo <code>/etc/inet/secret/ipseckey</code>	Contiene SA con claves manuales. El servicio SMF <code>manual-key</code> lo utiliza para configurar SA manualmente durante el inicio del sistema.	
Comando <code>ipsecalgs</code>	Comando de algoritmos IPsec. Es útil para visualizar y modificar la lista de algoritmos IPsec y sus propiedades. El servicio SMF <code>ipsecalgs</code> lo utiliza para sincronizar algoritmos IPsec conocidos con el núcleo durante el inicio del sistema.	ipsecalgs(1M)
Archivo <code>/etc/inet/ipsecalgs</code>	Contiene los protocolos IPsec configurados y las definiciones de algoritmos. Este archivo lo administra el comando <code>ipsecalgs</code> y nunca se debe editar manualmente.	
Archivo <code>/etc/inet/ike/config</code>	Archivo de configuración y política de IKE. De manera predeterminada, este archivo no existe. La administración se basa en reglas y parámetros globales del archivo <code>/etc/inet/ike/config</code> . Consulte “Archivos y utilidades IKE” en la página 263. Si este archivo existe, el servicio <code>svc:/network/ipsec/ike</code> inicia el daemon IKE, <code>in.iked</code> , para proporcionar la gestión automática de claves.	ike.config(4)

Configuración de IPsec (tareas)

Este capítulo incluye los procedimientos para implementar IPsec en la red. Los procedimientos se describen en las secciones siguientes:

- “Protección del tráfico con IPsec” en la página 229
- “Protección de una VPN con IPsec” en la página 236
- “Gestión de IPsec e IKE” en la página 243

Para obtener información general sobre IPsec, consulte el [Capítulo 14, “Arquitectura de seguridad IP \(descripción general\)”](#). Para obtener información de referencia sobre IPsec, consulte el [Capítulo 16, “Arquitectura de seguridad IP \(referencia\)”](#).

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” en la página 236](#). Para conocer los procedimientos adicionales para gestionar IPsec y utilizar comandos SMF con IPsec e IKE, consulte [“Gestión de IPsec e IKE” en la página 243](#).

La información siguiente se aplica a todas las tareas de configuración de IPsec:

- **IPsec y zonas:** para administrar la política IPsec y las claves para una zona no global IP compartida, cree el archivo de política 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. Para una zona de IP exclusiva, configure la política IPsec en la zona no global.
- **IPsec y RBAC:** para utilizar roles para administrar IPsec, consulte [Capítulo 9, “Uso del control de acceso basado en roles \(tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#). Si desea ver un ejemplo, consulte [“Cómo configurar una función para la seguridad de la red” en la página 245](#).

- **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 225](#).
- **IPsec y etiquetas Trusted Extensions:** en sistemas configurados con la función Trusted Extensions de Oracle Solaris, se pueden agregar etiquetas a los paquetes IPsec. Para obtener más información, consulte [“Administración de IPsec con etiquetas” de Configuración y administración de Trusted Extensions](#).
- **Direcciones IPv4 e IPv6:** en el ejemplo de IPsec de esta guía, se utilizan direcciones IPv4. Oracle Solaris también admite direcciones IPv6. Para configurar IPsec para una red IPv6, sustituya las direcciones IPv6 en los ejemplos. Al proteger túneles con IPsec, puede combinar direcciones IPv4 e IPv6 para las direcciones internas y externas. Esta configuración permite establecer un túnel para IPv6 en una red IPv4, por ejemplo.

El siguiente mapa de tareas hace referencia a los procedimientos que configuran IPsec entre uno o más sistemas. En las secciones de ejemplo correspondientes de las páginas del comando `man ipsecconf(1M)`, `ipseckey(1M)` y `ipadm(1M)`, también se describen procedimientos útiles.

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 230
Proteger un servidor web con la política 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 233
Visualizar las políticas IPsec.	Muestra las políticas IPsec que se están aplicando, según el orden de aplicación.	“Cómo visualizar las políticas de IPsec” en la página 235
Utilizar IKE para crear automáticamente material de claves para las SA de IPsec.	Proporciona los datos no procesados para las asociaciones de seguridad.	“Configuración de IKE (mapa de tareas)” en la página 267
Configurar una red privada virtual protegida (VPN).	Configura IPsec entre dos sistemas de Internet.	“Protección de una VPN con IPsec” en la página 236

▼ 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 una dirección IP. Ésta puede ser una dirección IPv4, una dirección IPv6 o ambas.

- Cada sistema requiere cifrado ESP con el algoritmo AES, el cual requiere una clave de 128 bits, y autenticación ESP con un resumen de mensajes SHA-2, el cual requiere una clave de 512 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.

Nota – Para utilizar IPsec con etiquetas en un sistema Trusted Extensions, consulte la extensión de este procedimiento en [“Cómo aplicar las protecciones IPsec en una red de Trusted Extensions de varios niveles” de Configuración y administración de Trusted Extensions](#).

Antes de empezar

La política IPsec se puede configurar en la zona global o en una zona de pila IP exclusiva. La política para una zona de pila IP compartida se debe configurar en la zona global. Para una zona de IP exclusiva, configure la política IPsec en la zona no global.

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#). Si inicia sesión de manera remota, utilice el comando `ssh` para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15-1](#).

2 En cada sistema, agregue entradas de host al archivo `/etc/inet/hosts`.

Este paso permite que la utilidad de gestión de servicios (SMF) utilice los nombres del sistema sin depender de servicios de nombres no existentes. Para obtener más información, consulte la página del comando `man smf(5)`.

a. En un sistema denominado `partym`, escriba lo siguiente en el archivo `hosts`:

```
# Secure communication with enigma
192.168.116.16 enigma
```

b. En un sistema denominado `enigma`, escriba lo siguiente en el archivo `hosts`:

```
# Secure communication with partym
192.168.13.213 partym
```

3 En cada sistema, cree el archivo de política 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 política IPsec al archivo `ipsecinit.conf`.

a. En el sistema `enigma`, agregue la política siguiente:

```
{laddr enigma raddr partym} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

b. En el sistema partym, agregue una política idéntica:

```
{laddr partym raddr enigma} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

Para ver la sintaxis de las entradas de la política IPsec, consulte la página del comando `man ipsecconf(1M)`.

5 En cada sistema, configure IKE para agregar un par de asociaciones de seguridad de IPsec entre los dos sistemas.

Configure IKE siguiendo uno de los métodos de configuración de “[Configuración de IKE \(mapa de tareas\)](#)” en la [página 267](#). Para ver la sintaxis del archivo de configuración de IKE, consulte la página del comando `man ike.config(4)`.

Nota – Si debe generar y mantener las claves de forma manual, consulte “[Cómo crear manualmente claves IPsec](#)” en la [página 243](#).”

6 Compruebe la sintaxis del archivo de política IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

Subsane los posibles errores, compruebe la sintaxis del archivo y continúe.

7 Refresque la política IPsec.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

La política IPsec está habilitada de forma predeterminada, por lo que *puede actualizarla*. Si ha inhabilitado la política IPsec, habilítela.

```
# svcadm enable svc:/network/ipsec/policy:default
```

8 Active las claves para IPsec.**■ 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 configuró manualmente las claves en el [Paso 5](#), complete “[Cómo crear manualmente claves IPsec](#)” en la [página 243](#) para activar las claves.

9 Compruebe que los paquetes se estén protegiendo.

Para ver el procedimiento, consulte “[Cómo verificar que los paquetes estén protegidos con IPsec](#)” en la [página 248](#).

Ejemplo 15-1 Adición de políticas IPsec al utilizar una conexión ssh

En este ejemplo, el administrador con el rol root configura las claves y la política IPsec en dos sistemas con el comando ssh para llegar al segundo sistema. Para obtener más información, consulte la página del comando man `ssh(1)`.

- En primer lugar, el administrador realiza del [Paso 2](#) al [Paso 6](#) 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 política IPsec y las claves del segundo sistema; para ello, realiza del [Paso 2](#) al [Paso 8](#).
- A continuación, el administrador termina la sesión ssh.

```
other-system # exit
local-system #
```

- Por último, el administrador completa el [Paso 7](#) y el [Paso 8](#) para habilitar la política IPsec en el primer sistema.

La próxima ocasión que los dos sistemas se comunican, incluida la conexión ssh, la comunicación queda protegida por IPsec.

▼ 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-2.

Antes de empezar

Debe encontrarse en la zona global para poder configurar la política IPsec. Para una zona de IP exclusiva, configure la política IPsec en la zona no global. Ha completado “[Cómo proteger el tráfico entre dos sistemas con IPsec](#)” en la [página 230](#) 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 mediante IKE.
- Que haya comprobado que los paquetes se estén protegiendo.

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#). Si inicia sesión de manera remota, utilice el comando `ssh` para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15-1](#).

2 Determine qué servicios deben omitir las comprobaciones de política 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 Agregue la política de servidor web al archivo de política 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-2.
# Use a unique SA for outbound traffic from the port
{} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

Esta configuración sólo permite que el tráfico seguro acceda al sistema, con las excepciones de omisión que se describen en el [Paso 2](#).

4 Compruebe la sintaxis del archivo de política IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

5 Actualice la política IPsec.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

6 Actualice las claves para IPsec.

Reinicie el servicio `ike`.

```
# svcadm restart svc:/network/ipsec/ike
```

Si debe generar y mantener las claves de forma manual, siga las instrucciones de [“Cómo crear manualmente claves IPsec” en la página 243](#).

La configuración se ha completado. Si lo desea, puede llevar a cabo el [Paso 7](#).

7 (Opcional) Habilite un sistema remoto para comunicarse con el servidor web para tráfico que no sea de red.

Agregue las siguientes líneas al archivo `/etc/inet/ipsecinit.conf` de un sistema remoto:

```
# Communicate with web server about nonweb stuff
#
```

```
{laddr webserver} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

Verifique la sintaxis y, luego, refresque la política IPsec para activarla.

```
remote-system # ipseconf -c -f /etc/inet/ipsecinit.conf
remote-system # svcadm refresh svc:/network/ipsec/policy:default
```

Un sistema remoto puede comunicarse de forma segura con el servidor web para tráfico que no sea de web sólo cuando las políticas IPsec del sistema coinciden.

▼ Cómo visualizar las políticas de IPsec

Puede ver las políticas 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 gestión IPsec de red.

Para crear un rol discreto de seguridad de red y asignar ese rol a un usuario, consulte [“Cómo configurar una función para la seguridad de la red” en la página 245](#).

2 Visualice las políticas IPsec.

- Visualice las entradas de la política IPsec global en el orden en que se agregaron las entradas.

```
$ ipseconf
```

El comando muestra cada entrada con un *índice*, seguida de un número.

- Visualice las entradas de la política IPsec en el orden en que se produzca una coincidencia.

```
$ ipseconf -l -n
```

- Visualice las entradas de la política IPsec, incluidas las entradas por túnel, en el orden en que se produzca una coincidencia.

```
$ ipseconf -L -n
```

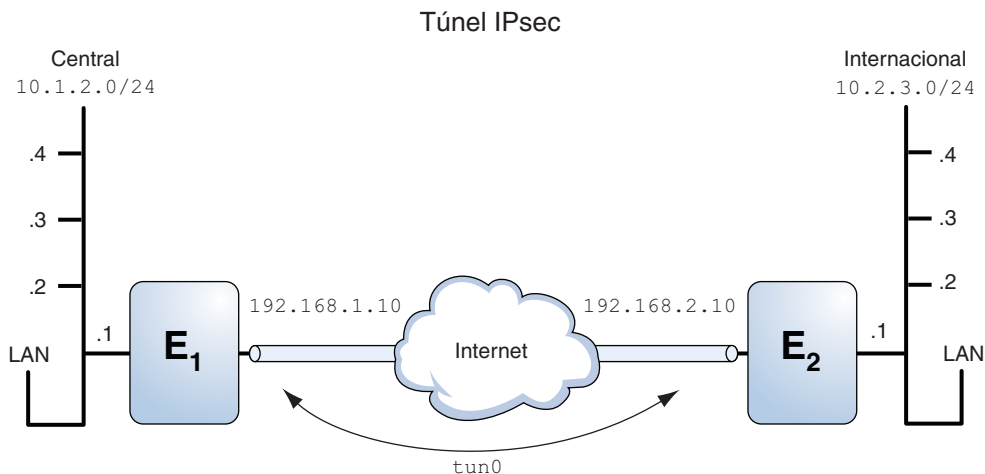
Protección de una VPN con IPsec

Oracle Solaris puede configurar una VPN que esté protegida por IPsec. Los túneles pueden crearse en *modo de túnel* o en *modo de transporte*. Para ver una explicación, consulte [“Modos de transporte y túnel en IPsec” en la página 221](#). En los ejemplos y procedimientos de esta sección, se utilizan direcciones IPv4, pero los ejemplos y procedimientos también se aplican a VPN IPv6. Para ver una breve explicación, consulte [“Protección del tráfico con IPsec” en la página 229](#).

Para ver ejemplos de políticas IPsec para túneles en modo de túnel, consulte [“Ejemplos de protección de una VPN con IPsec mediante el uso del modo de túnel” en la página 236](#).

Ejemplos de protección de una VPN con IPsec mediante el uso del modo de túnel

FIGURA 15-1 Túnel protegido por IPsec



Los ejemplos siguientes presuponen que el túnel se ha configurado para todas las subredes de la LAN:

```
## Tunnel configuration ##
# Tunnel name is 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
```

```
# Tunnel name address object is tun0/to-central
# Tunnel name address object is tun0/to-overseas
```

EJEMPLO 15-2 Creación de un túnel que puedan utilizar todas las subredes

En este ejemplo, se puede crear un túnel de todo el tráfico de las LAN locales de la LAN central de la [Figura 15-1](#) a través del enrutador 1 al enrutador 2 y, luego, transferirlo a todas las LAN locales de la LAN internacional. El tráfico se cifra con AES.

```
## IPsec policy ##
{tunnel tun0 negotiate tunnel}
ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

EJEMPLO 15-3 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 políticas IPsec para Central, si la LAN central intenta enrutar el tráfico para otras LAN por este túnel, el tráfico se transferirá al enrutador 1.

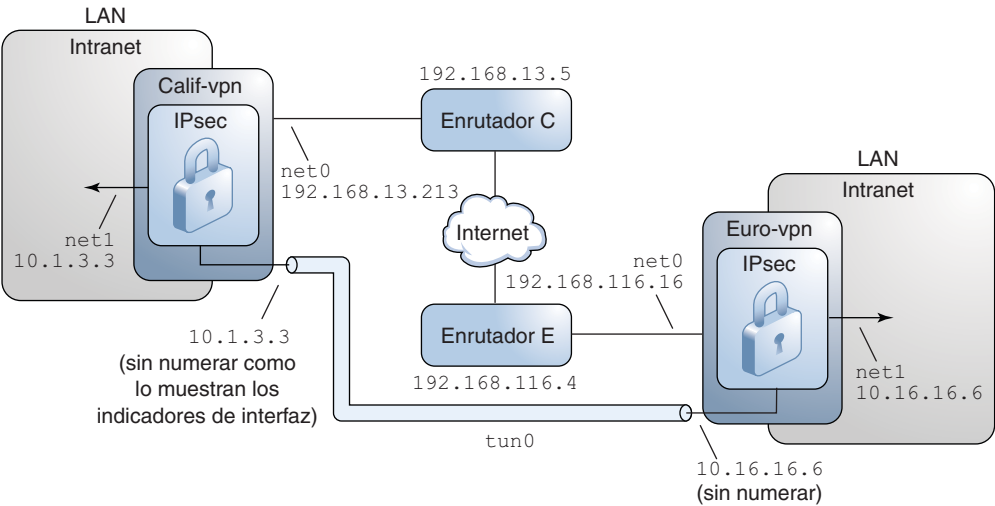
```
## IPsec policy ##
{tunnel tun0 negotiate tunnel laddr 10.1.2.0/24 raddr 10.2.3.0/24}
ipsec {encr_algs aes encr_auth_algs sha512 shared}
```

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 15-2](#).

- Cada sistema utiliza un espacio de dirección IPv4.
- Cada sistema cuenta con dos interfaces. La interfaz net0 se conecta a Internet. En este ejemplo, las direcciones IP de Internet empiezan por 192.168. La interfaz net1 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-2. En este ejemplo, el algoritmo SHA-2 requiere una clave de 512 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 15-2 VPN de ejemplo entre oficinas conectadas a través de Internet



Como se muestra en la ilustración anterior, los procedimientos utilizan los siguientes parámetros de configuración.

Parámetro	Europa	California
Nombre del sistema	euro-vpn	calif-vpn
Interfaz de la intranet del sistema	net1	net1
La dirección de intranet del sistema, también la dirección <i>-punto</i> en el Paso 7	10.16.16.6	10.1.3.3
Objeto de dirección de intranet del sistema	net1/inside	net1/inside
Interfaz de Internet del sistema	net0	net0
Dirección de Internet del sistema, también 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	tun0	tun0
Objeto de dirección de nombre de túnel	tun0/v4tunaddr	tun0/v4tunaddr

Para obtener información sobre los nombres de túnel, consulte [“Configuración y administración de túneles con el comando dladm”](#) en la página 126. Para obtener información sobre los objetos de dirección, consulte [“Cómo configurar una interfaz IP”](#) en la página 47 y la página del comando `man ipadm(1M)`.

▼ Cómo proteger una VPN con IPsec en modo de túnel

En modo túnel, el paquete IP interior determina la política IPsec que protege su contenido.

Este procedimiento amplía el procedimiento de [“Cómo proteger el tráfico entre dos sistemas con IPsec”](#) en la página 230. 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 237.

Para ver una descripción completa de los motivos para ejecutar comandos determinados, consulte los pasos correspondientes en [“Cómo proteger el tráfico entre dos sistemas con IPsec”](#) en la página 230.

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.

Nota – Para utilizar IPsec en modo de túnel con etiquetas en un sistema Trusted Extensions, consulte la extensión de este procedimiento en [“Cómo configurar un túnel en una red que no es de confianza”](#) de *Configuración y administración de Trusted Extensions*.

Antes de empezar

Debe estar en la zona global para configurar la política IPsec para el sistema o para una zona de IP compartida. Para una zona de IP exclusiva, configure la política IPsec en la zona no global.

1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos”](#) de *Administración de Oracle Solaris: servicios de seguridad*. Si inicia sesión de manera remota, utilice el comando `ssh` para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15-1](#).

2 Controle el flujo de paquetes antes de configurar IPsec.

a. Deshabilite el reenvío de IP y el enrutamiento dinámico de IP.

```
# routeadm -d ipv4-routing
# ipadm set-prop -p forwarding=off ipv4
# routeadm -u
```

La desactivación del reenvío de IP impide que los paquetes se reenvíen 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 la función estricta de hosts múltiples de IP.

```
# ipadm set-prop -p hostmodel=strong ipv4
```

La activación de la función estricta de hosts múltiples de IP requiere que los paquetes de una de las direcciones de destino del sistema lleguen a la dirección de destino correcta.

Cuando el parámetro `hostmodel` está configurado en `strong`, los paquetes que llegan a una interfaz determinada deben dirigirse a una de las direcciones IP locales de esa interfaz. Todos los demás paquetes, incluidos los que se dirigen a otras direcciones locales del sistema, se eliminan.

c. Compruebe que la mayoría de los servicios de red estén inhabilitados.

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 la política IPsec.

Edita el archivo `/etc/inet/ipsecinit.conf` para agregar la política IPsec para la VPN. Para ver ejemplos adicionales, consulte “Ejemplos de protección de una VPN con IPsec mediante el uso del modo de túnel” en la página 236.

En esta política, 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 `euro-vpn`, 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-2.
{tunnel tun0 negotiate tunnel}
ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

b. En el sistema `calif-vpn`, 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-2.
{tunnel tun0 negotiate tunnel}
ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```


- 4 En cada sistema, configure IKE para agregar un par de asociaciones de seguridad IPsec entre los dos sistemas.**

Configure IKE siguiendo uno de los métodos de configuración de “[Configuración de IKE \(mapa de tareas\)](#)” en la página 267. Para ver la sintaxis del archivo de configuración de IKE, consulte la página del comando `man ike.config(4)`.

Nota – Si debe generar y mantener las claves de forma manual, consulte “[Cómo crear manualmente claves IPsec](#)” en la página 243.

- 5 Verifique la sintaxis del archivo de política IPsec.**

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

Subsane los posibles errores, compruebe la sintaxis del archivo y continúe.

- 6 Actualice la política IPsec.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

La política IPsec está habilitada de forma predeterminada, por lo que *puede actualizarla*. Si ha inhabilitado la política IPsec, habilítela.

```
# svcadm enable svc:/network/ipsec/policy:default
```

- 7 Cree y configure el túnel, *nombre_túnel*.**

Los comandos siguientes configuran las interfaces internas y externas, crean el túnel `tun0` y asignan direcciones IP al túnel.

- a. En el sistema *calif-vpn*, cree el túnel y configúrelo.**

Si la interfaz `net1` no existe, el primer comando la crea.

```
# ipadm create-addr -T static -a local=10.1.3.3 net1/inside
# dladm create-iptun -T ipv4 -a local=10.1.3.3,remote=10.16.16.6 tun0
# ipadm create-addr -T static \
-a local=192.168.13.213,remote=192.168.116.16 tun0/v4tunaddr
```

- b. En el sistema *euro-vpn*, cree el túnel y configúrelo.**

```
# ipadm create-addr -T static -a local=10.16.16.6 net1/inside
# dladm create-iptun -T ipv4 -a local=10.16.16.6,remote=10.1.3.3 tun0
# ipadm create-addr -T static \
-a local=192.168.116.16,remote=192.168.13.213 tun0/v4tunaddr
```

Nota – La opción `-T` del comando `ipadm` permite especificar el tipo de dirección que se creará. La opción `-T` del comando `dladm` permite especificar el túnel.

Para obtener información sobre estos comandos, consulte las páginas del comando `man dladm(1M)` y `ipadm(1M)`, y “[Cómo configurar una interfaz IP](#)” en la página 47. Para obtener información sobre los nombres personalizados, consulte “[Dispositivos de red y nombres de enlaces de datos](#)” de *Administración de Oracle Solaris: interfaces y virtualización de redes*.

8 En cada sistema, configure el reenvío.

```
# ipadm set-ifprop -m ipv4 -p forwarding=on net1
# ipadm set-ifprop -m ipv4 -p forwarding=off net0
```

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 `net1` está *dentro* de la intranet, el reenvío de IP debe estar activo para `net1`. Dado que `tun0` conecta los dos sistemas a través de Internet, el reenvío de IP debe permanecer activado para `tun0`. La interfaz `net0` 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.

9 En cada sistema, impida el anuncio de la interfaz privada.

```
# ipadm set-addrprop -p private=on net0
```

Aunque `net0` 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 `net0` 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.

10 Reinicie los servicios de red.

```
# svcadm restart svc:/network/initial:default
```

11 Agregue manualmente una ruta predeterminada a través de la interfaz `net0`.

La ruta predeterminada debe ser un enrutador con acceso directo a Internet.

a. En el sistema `calif-vpn`, agregue la ruta siguiente:

```
# route -p add net default 192.168.13.5
```

b. En el sistema `euro-vpn`, agregue la ruta siguiente:

```
# route -p add net default 192.168.116.4
```

Aunque la interfaz `net0` no forme parte de la intranet, `net0` necesita alcanzar su sistema equivalente a través de Internet. Para encontrar su equivalente, `net0` 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)`.

Gestión de IPsec e IKE

El mapa de tareas siguiente hace referencia a las tareas que se pueden utilizar al gestionar IPsec.

Tarea	Descripción	Para obtener instrucciones
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 El security parameter index (SPI) Direcciones IP de origen y de destino, y otros parámetros 	“Cómo crear manualmente claves IPsec” en la página 243
Crear un rol de seguridad de red.	Crea un rol que puede configurar una red segura, pero que puede desempeñar menos funciones que el rol root.	“Cómo configurar una función para la seguridad de la red” en la página 245
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 gestionar servicios IPsec e IKE” en la página 247
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 248

▼ Cómo crear manualmente claves IPsec

El procedimiento siguiente proporciona los materiales de claves para el [Paso 5 de “Cómo proteger el tráfico entre dos sistemas con IPsec” en la página 230](#). Está generando claves para dos sistemas, partym y enigma. Se generan las claves en un sistema, y después se utilizan las teclas del primer sistema en ambos sistemas.

Antes de empezar Debe estar en la zona global para gestionar manualmente el material de claves para una zona no global.

1 Genere el material de claves para la SA.

a. Determine las claves que necesita.

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-2 para AH. Cada número debe tener 512 caracteres de longitud. Un número es para dst enigma. Un número es para dst partym.
- Dos números aleatorios hexadecimales para el algoritmo 3DES para ESP. Cada número debe tener 168 caracteres de longitud. Un número es para dst enigma. Un número es para dst partym.

b. Genere las claves necesarias.

- Si dispone de un generador de números aleatorios en su sitio, utilícelo.
- Utilice el comando `pktool`, como se muestra en [“Cómo generar una clave simétrica con el comando pktool” de Administración de Oracle Solaris: servicios de seguridad](#) y en el ejemplo de IPsec en esa sección.

2 En el rol root de cada sistema, agregue las claves a los archivos de claves manuales para IPsec.

a. Edite el archivo `/etc/inet/secret/ipseckeys` en el sistema enigma para que tenga 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.
#
# Backslashes indicate command continuation.
#
# for outbound packets on enigma
add esp spi 0x8bcd1407 \
  src 192.168.116.16 dst 192.168.13.213 \
  encr_alg 3des \
  auth_alg sha512 \
  encrkey d41fb74470271826a8e7a80d343cc5aa... \
  authkey e896f8df7f78d6cab36c94ccf293f031...
#
# for inbound packets
add esp spi 0x122a43e4 \
  src 192.168.13.213 dst 192.168.116.16 \
  encr_alg 3des \
  auth_alg sha512 \
  encrkey dd325c5c137fb4739a55c9b3a1747baa... \
  authkey ad9ced7ad5f255c9a8605fba5eb4d2fd...
```

b. Proteja el archivo con permisos de sólo lectura.

```
# chmod 400 /etc/inet/secret/ipseckeys
```

c. Verifique la sintaxis del archivo.

```
# ipseckey -c -f /etc/inet/secret/ipseckeys
```

Nota – El material de claves de los dos sistemas *debe* ser idéntico.

3 Active las claves para IPsec.

- 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 ipsec/manual-key
```

Pasos siguientes Si no terminó de establecer la política IPsec, regrese al procedimiento IPsec para habilitar o refrescar la política IPsec.

▼ Cómo configurar una función para la seguridad de la red

Si está utilizando la función de acceso basado en roles (RBAC) de Oracle Solaris para administrar los sistemas, siga este procedimiento para proporcionar un rol de gestión de red o de seguridad de red.

1 Enumere los perfiles de derechos relacionados con la red disponibles.

```
% getent prof_attr | grep Network | more
```

```
Console User:RO::Manage System as the Console User...
Network Management:RO::Manage the host and network configuration...
Network Autoconf Admin:RO::Manage Network Auto-Magic configuration via nwamd...
Network Autoconf User:RO::Network Auto-Magic User...
Network ILB:RO::Manage ILB configuration via ilbadm...
Network LLDP:RO::Manage LLDP agents via lldpadm...
Network VRRP:RO::Manage VRRP instances...
Network Observability:RO::Allow access to observability devices...
Network Security:RO::Manage network and host security...:profiles=Network Wifi
Security,Network Link Security,Network IPsec Management...
Network Wifi Management:RO::Manage wifi network configuration...
Network Wifi Security:RO::Manage wifi network security...
Network Link Security:RO::Manage network link security...
Network IPsec Management:RO::Manage IPsec and IKE...
System Administrator:RO::Can perform most non-security administrative tasks:profiles=...Network Management...
Information Security:RO::Maintains MAC and DAC security policies:profiles=...Network Security...
```

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 Enumere los comandos en el perfil de derechos de gestión de red.

```
% getent exec_attr | grep "Network Management"
...
Network Management:solaris:cmd::/sbin/dlstat:euid=dladm;egid=sys
...
Network Management:solaris:cmd::/usr/sbin/snoop:privs=net_observability
Network Management:solaris:cmd::/usr/sbin/spray:euid=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.
- Para crear un rol que gestione sólo IPsec e IKE, utilice el perfil de derechos de gestión de IPsec de red.

4 Cree un rol de seguridad de red que incluya el perfil de derechos de gestión de la red.

Un rol con el perfil derechos de seguridad de la red o el perfil de derechos de gestión de IPsec de red, además del perfil de gestión de red, puede ejecutar los comandos `ipadm`, `ipseckey` y `snoop`, entre otros, con privilegios adecuados.

Para crear el rol, asignarlo a un usuario y registrar los cambios con el servicio de nombres, consulte “[Configuración inicial de RBAC \(mapa de tareas\)](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

Ejemplo 15–4 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 gestionar servicios IPsec e IKE

Los siguientes pasos ofrecen los usos más probables de los servicios SMF para IPsec, IKE y la gestión manual de claves. De manera predeterminada, los servicios `policy` e `ipsecalgs` están habilitados. También por defecto, los servicios `ike` y `manual-key` están inhabilitados.

1 Para administrar la política IPsec, lleve a cabo una de las siguientes acciones:

- Después de agregar nuevas políticas al archivo `ipseccinit.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
# svccfg -s policy listprop config/config_file
config/config_file astring /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`, reinicie el servicio `ike`.

```
# svcadm restart svc:/network/ipsec/ike:default
```
- Tras cambiar el valor de una propiedad de servicio, consulte el valor de la propiedad; a continuación, actualice y reinicie el servicio.

```
# svccfg -s ike setprop config/admin_privilege = astring: "modkeys"
# svccfg -s ike listprop config/admin_privilege
config/admin_privilege astring modkeys
# svcadm refresh svc:/network/ipsec/ike
# svcadm restart svc:/network/ipsec/ike
```
- Para detener el servicio `ike`, inhabílitelo.

```
# 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`s, habilite el servicio `manual-key`.

```
# svcadm enable svc:/network/ipsec/manual-key:default
```

- 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; a continuación, actualice y reinicie el servicio.


```
# svccfg -s manual-key setprop config/config_file=/etc/inet/secret/MyIpseckeyfile
# svccfg -s manual-key listprop config/config_file
config/config_file astring /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, inhabilite 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`.

## ▼ 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 tener el rol `root` para crear el comando `snoop`. Para poder probar la conexión, es preciso tener acceso a ambos sistemas.

- 1 En un sistema, como `partym`, asuma el rol `root`.

```
% 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 -d net0 -v enigma
Using device /dev/bge (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, asuma el rol *root* 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 -----
...
```



## Arquitectura de seguridad IP (referencia)

---

Este capítulo contiene la siguiente información de referencia:

- “Servicios IPsec” en la página 251
- “Comando `ipseconf`” en la página 252
- “Archivo `ipsecinit.conf`” en la página 252
- “Comando `ipsecalgs`” en la página 254
- “Base de datos de asociaciones de seguridad para IPsec” en la página 255
- “Utilidades para la generación de SA en IPsec” en la página 255
- “Comando `snoop` e IPsec” en la página 257

Para obtener instrucciones sobre cómo implementar IPsec en la red, consulte el [Capítulo 15](#), “Configuración de IPsec (tareas)”. Para ver una descripción general de IPsec, consulte el [Capítulo 14](#), “Arquitectura de seguridad IP (descripción general)”.

## Servicios IPsec

La utilidad de gestión de servicios (SMF) proporciona los siguientes servicios para IPsec:

- Servicio `svc:/network/ipsec/policy`: administra la política IPsec. De manera predeterminada, 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`.
- Servicio `svc:/network/ipsec/ipsecalgs`: gestiona los algoritmos que están disponibles para IPsec. De manera predeterminada, este servicio está habilitado.
- Servicio `svc:/network/ipsec/manual-key`: activa la gestión manual de claves. De manera predeterminada, este servicio está inhabilitado. El valor de la propiedad `config_file` determina la ubicación del archivo de configuración `ipseckey`. El valor inicial es `/etc/inet/secret/ipseckey`.

- Servicio `svc:/network/ipsec/ike`: gestiona IKE. De manera predeterminada, este servicio está inhabilitado. Para conocer las propiedades configurables, consulte [“Servicio IKE” en la página 301](#).

Para obtener información sobre SMF, consulte el [Capítulo 6, “Gestión de servicios \(descripción general\)” de Administración de Oracle Solaris: tareas comunes](#). Consulte también las páginas de comando `man smf(5)`, `svcadm(1M)` y `svccfg(1M)`.

## Comando ipsecconf

El comando `ipsecconf` permite configurar la política IPsec para un host. Al ejecutar el comando para configurar la política, el sistema crea las entradas de la política IPsec en el núcleo. El sistema utiliza estas entradas para comprobar la política en todos los datagramas IP entrantes y salientes. Los datagramas reenviados no están sujetos a las comprobaciones de políticas que se agregan utilizando este comando. El comando `ipsecconf` también configura la base de datos de políticas de seguridad (SPD). Para conocer las opciones de política IPsec, consulte la página del comando `man ipsecconf(1M)`.

Debe tener el rol `root` 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 política con un formato de dirección local y dirección remota pueden proteger el tráfico en ambas direcciones con una sola entrada de política. 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 política para cada host.

Las entradas de políticas agregadas por el comando `ipsecconf` no persisten tras un reinicio del sistema. Para garantizar que la política IPsec esté activa cuando se inicia el sistema, agregue las entradas de la política al archivo `/etc/inet/ipsecinit.conf` y, luego, refresque o habilite el servicio `policy`. Para ver ejemplos, consulte [“Protección del tráfico con IPsec” en la página 229](#).

## Archivo ipsecinit.conf

Para habilitar la política de seguridad IPsec al iniciar Oracle Solaris, debe crear un archivo de configuración para inicializar IPsec con las entradas de política IPsec específicas. El nombre predeterminado para este archivo es `/etc/inet/ipsecinit.conf`. Consulte la página del comando `man ipsecconf(1M)` para obtener más información acerca de las entradas de política y su formato. Después de configurar la política, puede refrescar la política con el comando `svcadm refresh ipsec/policy`.

## Archivo ipsecinit.conf de ejemplo

El software Oracle Solaris incluye un archivo de política 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:

```
...
In the following simple example, outbound network traffic between the local
host and a remote host will be encrypted. Inbound network traffic between
these addresses is required to be encrypted as well.
#
This example assumes that 10.0.0.1 is the IPv4 address of this host (laddr)
and 10.0.0.2 is the IPv4 address of the remote host (raddr).
#

{laddr 10.0.0.1 raddr 10.0.0.2} ipsec
 {encr_algs aes encr_auth_algs sha256 sa shared}

The policy syntax supports IPv4 and IPv6 addresses as well as symbolic names.
Refer to the ipseconf(1M) man page for warnings on using symbolic names and
many more examples, configuration options and supported algorithms.
#
This example assumes that 10.0.0.1 is the IPv4 address of this host (laddr)
and 10.0.0.2 is the IPv4 address of the remote host (raddr).
#
The remote host will also need an IPsec (and IKE) configuration that mirrors
this one.
#
The following line will allow ssh(1) traffic to pass without IPsec protection:

{lport 22 dir both} bypass {}

#
{laddr 10.0.0.1 dir in} drop {}
#
Uncommenting the above line will drop all network traffic to this host unless
it matches the rules above. Leaving this rule commented out will allow
network packets that does not match the above rules to pass up the IP
network stack. , , ,
```

## Consideraciones de seguridad para ipsecinit.conf e ipseconf

La política IPsec no se puede cambiar para las conexiones establecidas. Un socket cuya política no se puede modificar se denomina *socket bloqueado*. Las nuevas entradas de política no protegen los sockets que ya están bloqueados. Para más información, consulte las páginas del comando `man connect(3SOCKET)` y `accept(3SOCKET)`. Si no está seguro, reinicie la conexión.

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 `ipseconf` con precaución. Utilice `ssh`, una consola u otro TTY conectado físicamente para lograr el funcionamiento más seguro.

## Comando ipsecalg

La función de estructura criptográfica de Oracle Solaris proporciona a IPsec algoritmos de cifrado y autenticación. El comando `ipsealg` puede enumerar los algoritmos que cada protocolo de IPsec admite. La configuración `ipsealg` se almacena en el archivo `/etc/inet/ipsealg`. Normalmente, este archivo no necesita modificarse. Sin embargo, si el archivo debe modificarse, utilice el comando `ipsealg`. El archivo nunca debe editarse directamente. Los algoritmos admitidos se sincronizan con el núcleo en el inicio del sistema mediante en servicio `svc:/network/ipsec/ipsealg:default`.

El [dominio de interpretación](#) ISAKMP, 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.

Específicamente, ISAKMP DOI 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/ipsealg`. Los números de protocolo y algoritmos los define la Autoridad de números asignados de Internet (IANA). El comando `ipsealg` permite ampliar la lista de algoritmos para IPsec.

Para obtener más información acerca de los algoritmos, consulte la página del comando [man ipsecalg\(1M\)](#). Para obtener más información sobre la estructura criptográfica, consulte el [Capítulo 11, “Estructura criptográfica \(descripción general\)” de Administración de Oracle Solaris: 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)`. Únicamente el rol `root` puede 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 SA en IPsec

El protocolo IKE permite administrar automáticamente las claves para las direcciones IPv4 e IPv6. Consulte el [Capítulo 18, “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` se puede utilizar para ver todas las SA conocidas por el sistema, independientemente de si las claves se agregaron manualmente o mediante IKE. Con la opción `-c`, el comando `ipseckey` comprueba la sintaxis del archivo de claves que se proporciona como argumento.

Las IPsec SA que añade el comando `ipseckey` no persisten tras el reinicio del sistema. Para habilitar las SA agregadas manualmente en el inicio del sistema, agregue entradas al archivo `/etc/inet/secret/ipseckey` y, luego, habilite el servicio `svc:/network/ipsec/manual-key:default`. Para conocer el procedimiento, consulte [“Cómo crear manualmente claves IPsec” en la página 243](#).

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 que un rol con el perfil derechos de seguridad de la red o el perfil de derechos de gestión de IPsec de red especifique información criptográfica confidencial de claves. Si un adversario obtiene acceso a esta información, puede poner en peligro la seguridad del tráfico IPsec.

---

**Nota** – Si es posible, utilice IKE y no las claves manuales con `ipseckey`.

---

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 `ssh`, una consola u otro TTY conectado físicamente para lograr el funcionamiento más seguro.



## 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 248.

También hay disponibles analizadores de red de terceros, como el software de código abierto gratuito [Wireshark](http://www.wireshark.org/about.html) (<http://www.wireshark.org/about.html>), que se integra en esta versión.



## Intercambio de claves de Internet (descripción general)

---

El intercambio de claves de Internet (IKE) automatiza la gestión de claves de IPsec. Oracle Solaris implementa IKEv1. Este capítulo contiene la información siguiente sobre IKE:

- “Gestión de claves con IKE” en la página 259
- “Negociación de claves IKE” en la página 260
- “Opciones de configuración de IKE” en la página 261
- “Archivos y utilidades IKE” en la página 263

Para obtener instrucciones sobre cómo implementar IKE, consulte el [Capítulo 18](#), “Configuración de IKE (tareas)”. Para obtener información de referencia, consulte el [Capítulo 19](#), “Intercambio de claves de Internet (referencia)”. Para obtener información sobre IPsec, consulte el [Capítulo 14](#), “Arquitectura de seguridad IP (descripción general)”.

## Gestión de claves con IKE

La administración del material de claves de las asociaciones de seguridad de IPsec se denomina *gestión de claves*. La gestión de claves automática requiere un canal de comunicación seguro para la creación, la autenticación y el intercambio de claves. Oracle Solaris usa el intercambio de claves de Internet (IKE), versión 1, para automatizar la gestión 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.

IKE puede aprovechar el almacenamiento de hardware y la aceleración de hardware que hay disponible. Los aceleradores de hardware permiten que las operaciones intensivas de claves se gestionen fuera del sistema. El almacenamiento de claves en hardware 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 IPsec en forma segura. El daemon utiliza valores de inicialización aleatorios para claves de funciones internas proporcionadas por el sistema operativo. 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)`.

## 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 17-1 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 Diffie-Hellman.                                                                                                                                                             |
| Algoritmo Diffie-Hellman          | DH       | Un algoritmo de intercambio de claves que permite la generación y la autenticación de claves. A menudo se denomina <i>intercambio de claves autenticadas</i> .                                                                                                                                                      |
| Algoritmo RSA                     | RSA      | Un algoritmo de intercambio de claves que permite 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. 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. |
| Grupo Oakley                      |          | Método para establecer claves para la fase 2 de un modo seguro. 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 gestión 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).

## 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 política IPsec, `ipsecinit.conf`.

## Opciones de configuración de IKE

El archivo de configuración `/etc/inet/ike/config` contiene entradas de política 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 autenticación de claves previamente compartidas

Las claves previamente compartidas se utilizan para autenticar dos sistemas equivalentes. La clave previamente compartida es un número hexadecimal o una cadena ASCII creada por un administrador en un sistema. La clave se comparte con administradores del sistema equivalente de manera segura. Si la clave previamente compartida es interceptada por un adversario, es posible que dicho adversario pueda suplantar uno de los sistemas equivalentes.

La clave previamente compartida en los sistemas equivalentes que usan este método de autenticación debe ser idéntica. Las claves están vinculadas a una dirección IP específica o a un rango de direcciones. Las claves se colocan en el archivo `/etc/inet/secret/ike.preshared` de cada sistema. 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 [algoritmo 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 cert db` 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.

## Archivos y utilidades IKE

La siguiente tabla resume los archivos de configuración para la política IKE, las ubicaciones de almacenamiento para las claves IKE y los distintos comandos y servicios que implementan IKE. Para obtener información sobre servicios, consulte el [Capítulo 6, “Gestión de servicios \(descripción general\)”](#) de *Administración de Oracle Solaris: tareas comunes*.

TABLA 17-2 Archivos de configuración de IKE, ubicaciones de almacenamiento de claves, comandos y servicios

| Archivo, ubicación, comando o servicio | Descripción                                                                                                                                                                                                                                                                                                                                                 | Página del comando man           |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| svc: /network/ipsec/ike                | El servicio SMF que gestiona IKE.                                                                                                                                                                                                                                                                                                                           | <a href="#">smf(5)</a>           |
| /usr/lib/inet/in.iked                  | Daemon de intercambio de claves de Internet (IKE). Activa la gestión de claves automatizada cuando el servicio ike está habilitado.                                                                                                                                                                                                                         | <a href="#">in.iked(1M)</a>      |
| /usr/sbin/ikeadm                       | Comando de administración de IKE para ver y modificar temporalmente la política IKE. Permite ver objetos administrativos de IKE, como los algoritmos de fase 1 y los grupos Diffie-Hellman disponibles.                                                                                                                                                     | <a href="#">ikeadm(1M)</a>       |
| /usr/sbin/ikecert                      | Comando de administración de bases de datos de certificados para administrar bases de datos locales que contienen certificados de claves públicas. Las bases de datos también se pueden almacenar en hardware conectado.                                                                                                                                    | <a href="#">ikecert(1M)</a>      |
| /etc/inet/ike/config                   | Archivo de configuración predeterminado para la política IKE. Contiene las reglas del sitio para hacer coincidir las solicitudes IKE entrantes y preparar las solicitudes IKE salientes.<br><br>Si este archivo existe, el daemon in.iked se inicia cuando el servicio ike está habilitado. El comando svccfg puede modificar la ubicación de este archivo. | <a href="#">ike.config(4)</a>    |
| ike.preshared                          | Archivo de claves previamente compartidas del directorio /etc/inet/secret. Contiene material de claves secretas para autenticación en el intercambio de fase 1. Se utiliza al configurar IKE con claves previamente compartidas.                                                                                                                            | <a href="#">ike.preshared(4)</a> |

TABLA 17-2 Archivos de configuración de IKE, ubicaciones de almacenamiento de claves, comandos y servicios  
(Continuación)

| Archivo, ubicación, comando o servicio | Descripción                                                                                                                                                                                                                                                                                                | Página del comando man      |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| ike.privatekeys                        | Directorio de claves privadas del directorio /etc/inet/secret. Contiene las claves privadas que forman parte de un par de claves pública-privada.                                                                                                                                                          | <a href="#">ikecert(1M)</a> |
| Directorio publickeys                  | Directorio del directorio /etc/inet/ike que contiene archivos de certificados y claves públicas. Contiene la parte de clave pública de un par de claves pública-privada.                                                                                                                                   | <a href="#">ikecert(1M)</a> |
| Directorio crls                        | Directorio del directorio /etc/inet/ike que incluye listas de revocación para archivos de certificados y claves públicas.                                                                                                                                                                                  | <a href="#">ikecert(1M)</a> |
| Sun Crypto Accelerator 6000 board      | 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. La placa Sun Crypto Accelerator 6000 es un dispositivo certificado por FIPS 140-2 en el nivel 3. | <a href="#">ikecert(1M)</a> |



## 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:

- “Visualización de información IKE” en la página 265
- “Configuración de IKE (mapa de tareas)” en la página 267
- “Configuración de IKE con claves previamente compartidas (mapa de tareas)” en la página 268
- “Configuración de IKE con certificados de clave pública (mapa de tareas)” en la página 273
- “Configuración de IKE para sistemas portátiles (mapa de tareas)” en la página 290
- “Configuración de IKE para buscar el hardware conectado” en la página 298

Para obtener una descripción general sobre IKE, consulte el [Capítulo 17, “Intercambio de claves de Internet \(descripción general\)”](#). Para obtener información de referencia sobre IKE, consulte el [Capítulo 19, “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)`.

## Visualización de información IKE

Puede visualizar los algoritmos y los grupos que se pueden usar en las negociaciones IKE de fase 1.

### ▼ Cómo visualizar grupos y algoritmos disponibles para intercambios IKE de fase 1

En este procedimiento, puede determinar qué grupos Diffie-Hellman están disponibles para utilizarse en intercambios IKE de fase 1. También puede visualizar los algoritmos de cifrado y

autenticación que están disponibles para los intercambios IKE de fase 1. Los valores numéricos coinciden con los valores especificados para estos algoritmos por la Autoridad de números asignados de Internet ([IANA](#)).

### 1 Visualice la lista de grupos Diffie-Hellman que IKE puede utilizar en la fase 1.

Los grupos Diffie-Hellman configuran SA de IKE.

```
ikeadm dump groups
Value Strength Description
1 66 ietf-ike-grp-modp-768
2 77 ietf-ike-grp-modp-1024
5 91 ietf-ike-grp-modp-1536
14 110 ietf-ike-grp-modp-2048
15 130 ietf-ike-grp-modp-3072
16 150 ietf-ike-grp-modp-4096
17 170 ietf-ike-grp-modp-6144
18 190 ietf-ike-grp-modp-8192
```

Completed dump of groups

Debe utilizar uno de estos valores como argumento del parámetro `oakley_group` en una transformación IKE de fase 1, como en el ejemplo siguiente:

```
p1_xform
{ auth_method preshared oakley_group 15 auth_alg sha encr_alg aes }
```

### 2 Visualice la lista de algoritmos de autenticación que IKE puede utilizar en la fase 1.

```
ikeadm dump authalgs
Value Name
1 md5
2 sha1
4 sha256
5 sha384
6 sha512
```

Completed dump of authalgs

Debe utilizar uno de estos nombres como argumento del parámetro `auth_alg` en una transformación IKE de fase 1, como en el ejemplo siguiente:

```
p1_xform
{ auth_method preshared oakley_group 15 auth_alg sha256 encr_alg 3des }
```

### 3 Visualice la lista de algoritmos de cifrado que IKE puede utilizar en la fase 1.

```
ikeadm dump encralgs
Value Name
3 blowfish-cbc
5 3des-cbc
1 des-cbc
7 aes-cbc
```

Completed dump of encralgs

Debe utilizar uno de estos nombres como argumento del parámetro `encr_alg` en una transformación IKE de fase 1, como en el ejemplo siguiente:

```
pl_xform
{ auth_method preshared oakley_group 15 auth_alg sha256 encr_alg aes }
```

**Véase también** Para conocer las tareas para configurar las reglas IKE que requieren estos valores, consulte [“Configuración de IKE \(mapa de tareas\)” en la página 267](#).

## 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 que IKE utilice 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.                                                 | <a href="#">“Configuración de IKE con claves previamente compartidas (mapa de tareas)” en la página 268</a> |
| 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. | <a href="#">“Configuración de IKE con certificados de clave pública (mapa de tareas)” en la página 273</a>  |
| Cruzar un límite NAT.                                                                  | Configura IPsec e IKE para comunicarse con un sistema portátil.                                                                                   | <a href="#">“Configuración de IKE para sistemas portátiles (mapa de tareas)” en la página 290</a>           |
| Configurar IKE para utilizar un almacén de claves para generar un par de certificados. | Permite que una placa Sun Crypto Accelerator 6000 acelere las operaciones IKE y almacene certificados de clave pública.                           | <a href="#">“Configuración de IKE para buscar el hardware conectado” en la página 298</a>                   |

# 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 configuración IKE y una clave para compartir.                                                      | <a href="#">“Cómo configurar IKE con claves previamente compartidas” en la página 268</a> |
| Agregar claves previamente compartidas a un sistema IKE en ejecución. | Agrega una nueva entrada de política IKE y nuevo material de claves en un sistema que está aplicando la política IKE. | <a href="#">“Cómo actualizar IKE para un sistema equivalente nuevo” en la página 271</a>  |

## Configuración de IKE con claves previamente compartidas

Las claves previamente compartidas constituyen el método de autenticación más sencillo para IKE. Si está configurando un sistema equivalente para que utilice IKE, y usted es el administrador de estos sistemas, el uso de claves previamente configuradas es una buena opción. Sin embargo, a diferencia de los certificados de clave pública, las claves previamente compartidas están vinculadas a direcciones IP. Puede asociar claves previamente compartidas con direcciones IP específicas o rangos de direcciones IP. Las claves previamente compartidas no se pueden utilizar con sistemas portátiles o sistemas que pueden reenumerarse, a menos que la reenumeración esté dentro del rango especificado de direcciones IP.

### ▼ 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.

En este procedimiento, se generan claves en formato ASCII.

Estos procedimientos utilizan los nombres de sistema `enigma` y `partym`. Sustituya los nombres de los sistemas con los nombres `enigma` y `partym`.

---

**Nota** – Para utilizar IPsec con etiquetas en un sistema Trusted Extensions, consulte la extensión de este procedimiento en [“Cómo aplicar las protecciones IPsec en una red de Trusted Extensions de varios niveles” de Configuración y administración de Trusted Extensions](#).

---

### 1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#). Si inicia sesión de manera remota, utilice el comando `ssh` para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15-1](#).

### 2 En cada sistema, cree un archivo `/etc/inet/ike/config`.

Puede usar `/etc/inet/ike/config.sample` como plantilla.

### 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 política IPsec en el archivo `ipsecinit.conf` del sistema. Los siguientes ejemplos de configuración IKE funcionan con los ejemplos `ipsecinit.conf` de [“Cómo proteger el tráfico entre dos sistemas con IPsec” en la página 230](#).

#### a. Por ejemplo, modifique el archivo `/etc/inet/ike/config` del sistema `enigma`:

```
ike/config file on enigma, 192.168.116.16

Global parameters
#
Defaults that individual rules can override.
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
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 sha256 encr_alg aes }
 p2_pfs 5
}
```

#### b. Modifique el archivo `/etc/inet/ike/config` del sistema `partym`:

```
ike/config file on partym, 192.168.13.213
Global Parameters
#
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
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 sha256 encr_alg aes }
 p2_pfs 5
}
```

**4 En cada sistema, verifique la sintaxis del archivo.**

```
/usr/lib/inet/in.iked -c -f /etc/inet/ike/config
```

**5 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
 # The preshared key can also be represented in hex
 # as in 0xf47cb0f432e14480951095f82b
 # key "This is an ASCII Cqret phrAz, use str0ng p@ssword tekniques"
}
```

**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
 # The preshared key can also be represented in hex
 # as in 0xf47cb0f432e14480951095f82b
 key "This is an ASCII Cqret phrAz, use str0ng p@ssword tekniques"
}
```

**6 Habilite el servicio IKE.**

```
svcadm enable ipsec/ike
```

## **Ejemplo 18–1 Refrescamiento de una clave IKE previamente compartida**

Cuando los administradores de IKE desean refrescar la clave previamente compartida, editan los archivos en los sistemas equivalentes y reinician el daemon `in.iked`.

En primer lugar, el administrador agrega una entrada de clave previamente compartida, válida para cualquier host en la subred `192.168.13.0/24`.

```
#...
{ localidtype IP
 localid 192.168.116.0/24
 remoteidtype IP
 remoteid 192.168.13.0/24
 # enigma and partym's shared passphrase for keying material
 key "LOooong key Th@t m^st Be Ch*angEd \"reguLarLy)"
}
```

Luego, el administrador reinicia el servicio IKE en cada sistema.

```
svcadm enable ipsec/ike
```

**Pasos siguientes** Si no terminó de establecer la política IPsec, regrese al procedimiento IPsec para habilitar o refrescar la política IPsec.

## ▼ Cómo actualizar IKE para un sistema equivalente nuevo

Si agrega entradas de política IPsec a una configuración operativa entre los mismos sistemas equivalentes, debe refrescar el servicio de política IPsec. No necesita privilegios para reconfigurar o reiniciar IKE.

Si agrega un sistema equivalente nuevo a la política IPsec, además de los cambios IPsec, debe modificar la configuración IKE.

**Antes de empezar** Actualizó el archivo `ipsecinit.conf` y refrescó la política IPsec para los sistemas equivalentes.

### 1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#). Si inicia sesión de manera remota, utilice el comando `ssh` para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15-1](#).

### 2 Cree una regla para que IKE gestione las claves para el nuevo sistema que utiliza IPsec.

#### a. Por ejemplo, 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 sha256 encr_alg aes}
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
 pl_xform
 {auth_method preshared oakley_group 5 auth_alg sha256 encr_alg aes}
 p2_pfs 5
}
```

**3 Cree una clave IKE previamente compartida para los sistemas equivalentes.**

**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
 key "Twas brillig and the slivey toves did *s0mEtHiNg* be CareFULL hEEEr"
}
```

**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
 key "Twas brillig and the slivey toves did *s0mEtHiNg* be CareFULL hEEEr"
}
```

**4 En cada sistema, actualice el servicio ike.**

```
svcadm refresh ike
```

**Pasos siguientes** Si no terminó de establecer la política IPsec, regrese al procedimiento IPsec para habilitar o refrescar la política IPsec.



## 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.

Un certificado público debe ser exclusivo, de modo que el creador de un certificado de clave pública genera un nombre exclusivo y arbitrario para el certificado. Por lo general, se utiliza un nombre X.509 distintivo. También se puede utilizar un nombre alternativo para la identificación. El formato de estos nombres es *etiqueta=valor*. Los valores son arbitrarios, aunque el formato del valor debe corresponder al tipo de etiqueta. Por ejemplo, el formato de la etiqueta email es *nombre@ dominio.sufijo*.

| 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"> <li>■ Un certificado autofirmado</li> <li>■ El certificado de clave pública del sistema equivalente</li> </ul>                                                                                                                                                                                      | <a href="#">“Cómo configurar IKE con certificados de clave pública autofirmados” en la página 274</a>               |
| 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"> <li>■ El certificado que crea la autoridad de certificación a partir de su solicitud</li> <li>■ El certificado de clave pública de la autoridad de certificación</li> <li>■ La lista CRL de la autoridad de certificación</li> </ul>                                  | <a href="#">“Cómo configurar IKE con certificados firmados por una autoridad de certificación” en la página 279</a> |
| Configurar certificados de clave pública en el hardware local.     | Implica una de estas acciones: <ul style="list-style-type: none"> <li>■ Generar un certificado autofirmado en el hardware local y, luego, agregar la clave pública de un sistema remoto al hardware.</li> <li>■ Generar una solicitud de certificado en el hardware local y, luego, agregar los certificados de clave pública de la autoridad de certificación al hardware.</li> </ul> | <a href="#">“Cómo generar y almacenar certificados de clave pública en el hardware” en la página 284</a>            |
| Actualizar la lista de revocación de certificados (CRL) desde PKI. | Accede a la CRL desde un punto de distribución central.                                                                                                                                                                                                                                                                                                                                | <a href="#">“Cómo administrar una lista de revocación de certificados” en la página 288</a>                         |

---

**Nota** – Para etiquetar paquetes y negociaciones IKE en un sistema Trusted Extensions, siga los procedimientos de [“Configuración de IPsec con etiquetas \(mapa de tareas\)”](#) de *Configuración y administración de Trusted Extensions*.

Los certificados de clave pública se gestionan en la zona global en sistemas Trusted Extensions. Trusted Extensions no cambia la forma en que se gestionan y se almacenan los certificados.

---

## 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 se pueden generar y almacenar en el hardware conectado. Para conocer el procedimiento, consulte [“Configuración de IKE para buscar el hardware conectado”](#) en la página 298.

### ▼ Cómo configurar IKE con certificados de clave pública autofirmados

En este procedimiento, se crea un par de certificados. La clave privada se almacena en un disco en la base de datos local de certificados y puede consultarse con el subcomando `cert local`. La parte pública del certificado se almacena en la base de datos pública de certificados. Puede consultarse con el subcomando `cert db`. Con un sistema equivalente, puede intercambiarse la parte pública. La combinación de dos certificados se utiliza para autenticar las transmisiones IKE.

Los certificados autofirmados requieren menos carga que los certificados públicos de una autoridad de certificación, pero no se escalan fácilmente. A diferencia de los certificados emitidos por una autoridad de certificación, los certificados autofirmados deben verificarse fuera de la banda.

#### 1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos”](#) de *Administración de Oracle Solaris: servicios de seguridad*. Si inicia sesión de manera remota, utilice el comando `ssh` para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15–1](#).

## 2 Cree un certificado autofirmado en la base de datos `ike.privatekeys`.

```
ikecert certlocal -ks -m keysize -t keytype \
-D dname -A altname \
[-S validity-start-time] [-F validity-end-time] [-T token-ID]
```

|                                       |                                                                                                                                                                                                                                      |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-ks</code>                      | Crea un certificado autofirmado.                                                                                                                                                                                                     |
| <code>-m tamaño_clave</code>          | Es el tamaño de la clave. <i>Tamaño_clave</i> puede ser 512, 1024, 2048, 3072 o 4096.                                                                                                                                                |
| <code>-t tipo_clave</code>            | 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> .                                                                                 |
| <code>-D nombre_d</code>              | Es el nombre X.509 distinguido para el tema del certificado. Por lo general, <i>nombre_d</i> tiene la forma: <code>C=país, O=organización, OU=unidad organizativa, CN=nombre común</code> . Las etiquetas válidas son C, O, OU y CN. |
| <code>-A nombre_alt</code>            | Nombre alternativo del certificado; <i>nombre_alt</i> tiene el formato <code>tag=value</code> . Las etiquetas válidas son IP, DNS, email y DN.                                                                                       |
| <code>-S tiempo_inicio_validez</code> | Proporciona un tiempo de inicio de validez absoluto o relativo para el certificado.                                                                                                                                                  |
| <code>-F tiempo_fin_validez</code>    | Proporciona un tiempo de fin de validez absoluto o relativo para el certificado.                                                                                                                                                     |
| <code>-T ID_token</code>              | 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 2048 -t rsa-sha1 \
-D "O=exampleco, OU=IT, C=US, CN=partym" \
-A IP=192.168.13.213
Creating private key.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEfdZgKjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
a...+
zBGi4QkNdI3f
-----END X509 CERTIFICATE-----
```

---

**Nota** – Los valores de las opciones de `-D` y `-A` son arbitrarios. Los valores se utilizan para identificar el certificado únicamente. No se utilizan para identificar un sistema, como 192.168.13.213. De hecho, dado que estos valores son idiosincrásicos, debe verificar fuera de banda que el certificado correcto esté instalado en los sistemas equivalentes.

---

### b. El comando del sistema `enigma` sería como el siguiente:

```
ikecert certlocal -ks -m 2048 -t rsa-sha1 \
-D "O=exampleco, OU=IT, C=US, CN=enigma" \
```

```
-A IP=192.168.116.16
Creating private key.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEB15JnjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
...
y85m6LHJYtC6
-----END X509 CERTIFICATE-----
```

### 3 Guarde el certificado y envíelo al sistema remoto.

La salida es una versión codificada de la parte pública del certificado. Puede pegar de manera segura este certificado en un correo electrónico. La parte receptora debe verificar fuera de banda que se haya instalado el certificado correcto, como se muestra en el [Paso b](#).

#### a. Por ejemplo, debe enviar la parte pública del certificado `partym` al administrador de `enigma`.

```
To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEfdZgKjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
a...+
zBGi4QkNdI3f
-----END X509 CERTIFICATE-----
```

#### b. El administrador de `enigma` debe enviarle la parte pública del certificado `enigma`.

```
To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEB15JnjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
...
y85m6LHJYtC6
-----END X509 CERTIFICATE-----
```

### 4 En cada sistema, agregue el certificado que recibió a la base de datos de clave pública.

#### a. Guarde el correo electrónico del administrador en un archivo legible por `root`.

#### b. Redirija el archivo al comando `ikecert`.

```
ikercert certdb -a < /tmp/certificate.eml
```

El comando importa el texto entre las etiquetas `BEGIN` y `END`.

## 5 Verifique con el otro administrador que el certificado proceda de dicho administrador.

Por ejemplo, puede llamar por teléfono al otro administrador para verificar que el hash del certificado público que usted tiene coincida con el hash del certificado privado que únicamente el administrador tiene.

### a. Enumere el certificado almacenado en `partym`.

En el ejemplo siguiente, Note 1 (Nota 1) indica el nombre distintivo (DN) del certificado en la ranura 0. El certificado privado en la ranura 0 tiene el mismo hash, de modo que estos certificados son el mismo par de certificados. Para que los certificados públicos funcionen, debe haber una pareja coincidente. El subcomando `certdb` enumera la parte pública, mientras que el subcomando `certlocal` enumera la parte privada.

```
partym # ikecert certdb -l
```

```
Certificate Slot Name: 0 Key Type: rsa
 (Private key in certlocal slot 0)
 Subject Name: <O=exampleco, OU=IT, C=US, CN=partym> Note 1
 Key Size: 2048
 Public key hash: 80829EC52FC5BA910F4764076C20FDCF
```

```
Certificate Slot Name: 1 Key Type: rsa
 (Private key in certlocal slot 1)
 Subject Name: <O=exampleco, OU=IT, C=US, CN=Ada>
 Key Size: 2048
 Public key hash: FEA65C5387BBF3B2C8F16C019FEB388
```

```
partym # ikecert certlocal -l
```

```
Local ID Slot Name: 0 Key Type: rsa
 Key Size: 2048
 Public key hash: 80829EC52FC5BA910F4764076C20FDCF Note 3
```

```
Local ID Slot Name: 1 Key Type: rsa-sha1
 Key Size: 2048
 Public key hash: FEA65C5387BBF3B2C8F16C019FEB388
```

```
Local ID Slot Name: 2 Key Type: rsa
 Key Size: 2048
 Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

Esta comprobación verificó que el sistema `partym` tenga un par de certificados válido.

### b. Verifique que el sistema `enigma` tenga el certificado público de `partym`.

El hash de clave pública se puede comunicar por teléfono.

Compare los hashes de Note 3 (Nota 3) en `partym`, en el paso anterior, con Note 4 (Nota 4) en `enigma`.

```
enigma # ikecert certdb -l
```

```
Certificate Slot Name: 0 Key Type: rsa
```

```
(Private key in certlocal slot 0)
Subject Name: <O=exampleco, OU=IT, C=US, CN=Ada>
Key Size: 2048
Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

```
Certificate Slot Name: 1 Key Type: rsa
(Private key in certlocal slot 1)
Subject Name: <O=exampleco, OU=IT, C=US, CN=enigma>
Key Size: 2048
Public key hash: FEA65C5387BBF3B2C8F16C019FEB388
```

```
Certificate Slot Name: 2 Key Type: rsa
(Private key in certlocal slot 2)
Subject Name: <O=exampleco, OU=IT, C=US, CN=partym>
Key Size: 2048
Public key hash: 80829EC52FC5BA910F4764076C20FDCF Note 4
```

El hash de clave pública y el nombre del asunto del último certificado almacenado en la base de datos de certificados de enigma coincide con el hash del certificado privado para partym en el paso anterior.

## 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 self-signed certs
that we verified out of band. The local certificate
is implicitly trusted because we have access to the private key.

cert_trust "O=exampleco, OU=IT, C=US, CN=enigma"

We could also use the Alternate name of the certificate,
if it was created with one. In this example, the Alternate Name
is in the format of an IP address:
cert_trust "192.168.116.16"

Parameters that may also show up in rules.

p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha256 encr_alg 3des }
p2_pfs 5

{
 label "US-partym to JA-enigma"
 local_id type dn
 local_id "O=exampleco, OU=IT, C=US, CN=partym"
 remote_id "O=exampleco, OU=IT, C=US, CN=enigma"

 local_addr 192.168.13.213
 # We could explicitly enter the peer's IP address here, but we don't need
 # to do this with certificates, so use a wildcard address. The wildcard
```

```
allows the remote device to be mobile or behind a NAT box
remote_addr 0.0.0.0/0

pl_xform
{auth_method rsa_sig oakley_group 2 auth_alg sha256 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 exclusivo en el sistema local.

```
...
{
 label "JA-enigmax to US-partym"
 local_id_type dn
 local_id "O=exampleco, OU=IT, C=US, CN=enigma"
 remote_id "O=exampleco, OU=IT, C=US, CN=partym"

 local_addr 192.168.116.16
 remote_addr 0.0.0.0/0
 ...
}
```

**7 En los sistemas equivalentes, habilite IKE.**

```
partym # svcadm enable ipsec/ike
```

```
enigma # svcadm enable ipsec/ike
```

**Pasos siguientes** Si no terminó de establecer la política IPsec, regrese al procedimiento IPsec para habilitar o refrescar la política IPsec.

## ▼ 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 Conviértase en administrador.**

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#). Si inicia sesión de manera remota, utilice el comando ssh para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15-1](#).

## 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 b](#) in “Cómo configurar IKE con certificados de clave pública autofirmados” en la página 274.

```
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 2048 -t rsa-sha1 \
> -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 2048 -t rsa-sha1 \
> -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
...
8qlqdjaStLGfhd00
-----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 usted 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 288](#) 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 262](#).

##### a. Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*. Si inicia sesión de manera remota, utilice el comando `ssh` para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15-1](#).

##### b. Agregue el certificado de clave pública que ha recibido de la organización de PKI.

```
ikecert certdb -a < /tmp/PKIcert.eml
```

##### c. Agregue la autoridad de certificación de la organización de PKI.

```
ikecert certdb -a < /tmp/PKIca.eml
```

##### d. Si la organización de PKI ha enviado una lista de certificados revocados, agregue la CRL a la base de datos `certrl`:

```
ikecert certrl -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 sha384 encr_alg aes}
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 sha256 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-enigmax to US-partym - 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
...
```

## 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 288](#) para ver algunos ejemplos.

## Ejemplo 18–2 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.

```
ikecert certdb -a < /tmp/saved.cert.eml
```

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`.

**Pasos siguientes** Si no terminó de establecer la política IPsec, regrese al procedimiento IPsec para habilitar o refrescar la política IPsec.

## ▼ 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 Sun Crypto Accelerator 6000” en la página 298 para obtener instrucciones sobre la instalación.

### 1 Conviértase en administrador.

Para obtener más información, consulte “Cómo obtener derechos administrativos” de *Administración de Oracle Solaris: servicios de seguridad*. Si inicia sesión de manera remota, utilice el comando `ssh` para un inicio de sesión remoto seguro. Esto se ilustra en el Ejemplo 15-1.

### 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 6000 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 2048 -t rsa-sha1 \
> -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 token de la placa Sun Crypto Accelerator 6000 conectada.

#### ■ Para obtener una solicitud de certificado, utilice esta sintaxis.

```
ikecert certlocal -kc -m 2048 -t rsa-sha1 \
> -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 6000, dos puntos y la contraseña del usuario.

Si la placa Sun Crypto Accelerator 6000 tiene un usuario `ikemgr` cuya contraseña es `rgm4tigt`, debe escribir lo siguiente:

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 279](#).

#### 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

...
{
 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 sha256 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"

...
{
 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 sha256 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 288](#).

**Pasos siguientes** Si no terminó de establecer la política IPsec, regrese al procedimiento IPsec para habilitar o refrescar la política IPsec.

## ▼ **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](#) in [“Cómo configurar IKE con certificados firmados por una autoridad de certificación” en la página 279](#).
- 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 certrlb`. Esto se ilustra en el [Ejemplo 18-3](#).

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.



*esp\_cert* Es un patrón que coincide con un certificado de la base de datos de certificados IKE.

Por ejemplo, Oracle emitió el certificado siguiente. Los detalles se han modificado.

```
ikecert certdb -lv example-protect.oracle.com
Certificate Slot Name: 0 Type: dsa-sha1
 (Private key in certlocal slot 0)
Subject Name: <O=Oracle, CN=example-protect.oracle.com>
Issuer Name: <CN=Oracle CA (Cl B), O=Oracle>
SerialNumber: 14000D93
Validity:
 Not Valid Before: 2011 Sep 19th, 21:11:11 GMT
 Not Valid After: 2015 Sep 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.oracle.com
 Key Usage: DigitalSignature KeyEncipherment
 [CRITICAL]
CRL Distribution Points:
 Full Name:
 URI = #Ihttp://www.oracle.com/pki/pkismica.crl#i
 DN = <CN=Oracle CA (Cl B), O=Oracle>
 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.oracle.com:389,ldap2.oracle.com"
...
```

IKE recupera la CRL y almacena en caché la CRL hasta que caduque el certificado.

**Ejemplo 18–3**    Cómo pegar una CRL en la base de datos certltdb 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 certltdb 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 certltdb -a`.

```
ikercert certltdb -a < Oracle.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                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Comunicarse remotamente con un sitio central.                                                                                            | Permite a los sistemas remotos comunicarse con un sitio central. Los sistemas remotos pueden ser portátiles.         | <a href="#">“Cómo configurar IKE para sistemas remotos” en la página 291</a> |
| Utilizar un certificado público de una autoridad de certificación 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. | <a href="#">Ejemplo 18–4</a>                                                 |

| Tarea                                                                                                                     | Descripción                                                                                                           | Para obtener instrucciones   |
|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------|
| Utilizar un certificado público de una autoridad de certificación 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.  | <a href="#">Ejemplo 18-5</a> |
| 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. | <a href="#">Ejemplo 18-6</a> |
| 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.             | <a href="#">Ejemplo 18-7</a> |

## 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 política 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 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*. Si inicia sesión de manera remota, utilice el comando ssh para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15-1](#).

## 2 Configure el sistema central para que reconozca los sistemas portátiles.

### a. Configure el archivo `ipsecinit.conf`.

El sistema central necesita una política que permite una amplia gama de direcciones IP. Los certificados de la política 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 sha256 sa shared}
```

### b. Configure el archivo de configuración IKE.

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
 # CA's public 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 aes auth_alg sha256 }
}
```

### 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
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 política IPsec.

```
/etc/inet/ipsecinit.conf on mobile
Find central
{raddr 192.xxx.xxx.x} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}
```

#### c. Configure el archivo de configuración IKE.

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 aes auth_alg sha256 }
}
```

#### 4 Habilite el servicio ike.

```
svcadm enable svc:/network/ipsec/ike
```

### Ejemplo 18-4 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, el certificado público de una autoridad de certificación se colocó en el sistema portátil y en 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 18-5](#).

```
/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 sha256 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

CA's public 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 aes auth_alg sha256}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
}

```

### Ejemplo 18-5 Configuración de un sistema con una NAT con IPsec

En el ejemplo siguiente, el certificado público de una autoridad de certificación se coloca en el sistema portátil y en el sistema central. `mobile1` se conecta a la oficina central de la compañía desde su 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 en las oficinas de la compañía, consulte el [Ejemplo 18-4](#).

```

/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 sha256 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 aes auth_alg sha256 }
}
```

### **Ejemplo 18–6** 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 18–7](#).

```
/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 sha256 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 aes auth_alg sha256 }
}
```

### Ejemplo 18-7 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 18-6](#).

```
/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 sha256 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 aes auth_alg sha256 }
}
```

**Pasos siguientes** Si no terminó de establecer la política IPsec, regrese al procedimiento IPsec para habilitar o refrescar la política IPsec.

## Configuración de IKE para buscar el hardware conectado

Los certificados de clave pública también se almacenan en el hardware conectado. La placa Sun Crypto Accelerator 6000 proporciona almacenamiento y permite que las operaciones de clave pública se descarguen del sistema a la placa.

### ▼ Cómo configurar IKE para buscar la placa Sun Crypto Accelerator 6000

#### Antes de empezar

En el procedimiento siguiente, se presupone que hay una placa Sun Crypto Accelerator 6000 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 6000 Board Version 1.1 User's Guide*.

#### 1 Conviértase en administrador.

Para obtener más información, consulte [“Cómo obtener derechos administrativos” de Administración de Oracle Solaris: servicios de seguridad](#). Si inicia sesión de manera remota, utilice el comando `ssh` para un inicio de sesión remoto seguro. Esto se ilustra en el [Ejemplo 15-1](#).

#### 2 Compruebe que esté vinculada la biblioteca de PKCS #11.

IKE utiliza las rutinas de la biblioteca para gestionar la generación de claves y el almacenamiento de claves en la placa Sun Crypto Accelerator 6000. 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
$
```

#### 3 Encuentre el ID de token para la placa Sun Crypto Accelerator 6000 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 token, consulte [“Cómo generar y almacenar certificados de clave pública en el hardware” en la página 284](#).

Los espacios finales se rellenan automáticamente con el comando `ikecert`.

**Ejemplo 18-8** Búsqueda y uso de símbolos de metarranura

Los tokens se pueden almacenar en el disco, en una placa conectada o en el almacén de claves de token de software proporcionado por la estructura criptográfica. 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
```

**Pasos siguientes** Si no terminó de establecer la política IPsec, regrese al procedimiento IPsec para habilitar o refrescar la política IPsec.



## Intercambio de claves de Internet (referencia)

---

Este capítulo contiene la siguiente información de referencia sobre IKE:

- “Servicio IKE” en la página 301
- “Daemon IKE” en la página 302
- “Archivo de configuración IKE” en la página 303
- “Comando `ikeadm`” en la página 303
- “Archivos de claves IKE previamente compartidas” en la página 304
- “Comandos y bases de datos de claves públicas IKE” en la página 304

Para obtener instrucciones sobre la implementación de IKE, consulte el [Capítulo 18](#), “Configuración de IKE (tareas)”. Para obtener una descripción general, consulte el [Capítulo 17](#), “Intercambio de claves de Internet (descripción general)”.

### Servicio IKE

**Servicio** `svc:/network/ipsec/ike:default`: la utilidad de gestión de servicios (SMF) proporciona el servicio `ike` para gestionar IKE. De manera predeterminada, 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 del comando `man ikeadm(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 detalles, consulte “Comando `ikeadm`” en la página 303.

Para obtener información sobre SMF, consulte el [Capítulo 6, “Gestión de servicios \(descripción general\)” de Administración de Oracle Solaris: tareas comunes](#). Consulte también las páginas de comando `man smf(5)`, `svcadm(1M)` y `svccfg(1M)`.

## Daemon IKE

El daemon `in.iiked` automatiza la gestión de claves criptográficas para IPsec en un sistema Oracle 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.

De manera predeterminada, el servicio `svc:/network/ipsec/ike:default` 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.iiked` 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 política 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 política. El daemon `in.iiked` 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 política IKE. Para modificar permanentemente la política IKE, puede modificar las propiedades del servicio `ike`. Para modificar las propiedades del servicio IKE, consulte [“Cómo gestionar servicios IPsec e IKE” en la página 247](#). El comando `ikeadm` también se puede utilizar para ver SA de fase 1, reglas de política, claves previamente compartidas, grupos Diffie-Hellman disponibles, algoritmos de autenticación y cifrado de fase 1, y antememoria del certificado.

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 configuración IKE

El archivo de configuración IKE, `/etc/inet/ike/config`, gestiona las claves para las interfaces protegidas en el archivo de política IPsec, `/etc/inet/ipsecinit.conf`.

La gestión 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 política IKE, consulte [“Configuración de IKE con claves previamente compartidas \(mapa de tareas\)” en la página 268](#). Para ver ejemplos y descripciones de las entradas de política IKE, consulte la página del comando `man ike.config(4)`.

Las SA de IPsec admitidas por IKE protegen los datagramas IP de acuerdo con las políticas del archivo de configuración IPsec, `/etc/inet/ipsecinit.conf`. El archivo de política IKE determina si se utiliza la seguridad directa perfecta (PFS) al crear las asociaciones de seguridad de IPsec.

El archivo `/etc/inet/ike/config` puede incluir la ruta a una biblioteca que se implementa según el estándar siguiente: RSA Security Inc. PKCS #11 Cryptographic Token Interface (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 `ipseconf`” en la página 253](#).

## Comando `ikeadm`

Puede utilizar el comando `ikeadm` para:

- 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.
- Visualizar objetos del daemon IKE, como todas las SA de fase 1, reglas de política, claves previamente compartidas, grupos Diffie-Hellman disponibles, algoritmos de autenticación y cifrado de fase 1, y antememoria del certificado.

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 <code>ikeadm</code> .                                |

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`. Para conocer el procedimiento, consulte [“Cómo gestionar servicios IPsec e IKE” en la página 247](#).

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 256](#).

## 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 gestión 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 gestión manual del archivo, consulte [“Cómo crear manualmente claves IPsec” en la página 243](#). 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.

## 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 `certrlb`.



El comando `ikecert` también administra el almacenamiento de claves. Las claves se pueden almacenar en disco, en una placa Sun Crypto Accelerator 6000 conectada o en un almacén de claves de token de software. El almacén de claves de token de software está disponible cuando la metarranura de la estructura criptográfica se utiliza para comunicarse con el dispositivo de hardware. El comando `ikecert` utiliza la biblioteca PKCS #11 para localizar el almacenamiento de claves.

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. Las certificados y las solicitudes de certificados también se pueden almacenar mediante la estructura criptográfica del almacén de claves de token de software, o bien en una placa Sun Crypto Accelerator 6000 conectada. 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 19-1 Correspondencias entre las opciones `ikecert` y las entradas `ike/config`

| Opción <code>ikecert</code>             | Entrada <code>ike/config</code>                                 | Descripción                                                                                                                                                   |
|-----------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-A nombre_alternativo_tema</code> | <code>cert_trust</code><br><code>nombre_alternativo_tema</code> | 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. |

TABLA 19-1 Correspondencias entre las opciones `ikecert` y las entradas `ike/config` (Continuación)

| Opción <code>ikecert</code>                           | Entrada <code>ike/config</code>       | Descripción                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-D nombre_distinguido_X.509</code>              | <code>nombre_distinguido_X.509</code> | 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).                                                                                                                                   |
| <code>-t dsa-sha1</code>                              | <code>auth_method dsa_sig</code>      | Método de autenticación que es ligeramente más lento que <a href="#">RSA</a> .                                                                                                                                                                                                                     |
| <code>-t rsa-md5 y</code><br><code>-t rsa-sha1</code> | <code>auth_method rsa_sig</code>      | Método de autenticación que es ligeramente más lento que <a href="#">DSA</a> .<br><br>La clave pública RSA debe ser lo suficientemente grande para cifrar la <a href="#">carga útil</a> mayor. Normalmente, una carga útil de identidad, como el nombre distinguido X.509, es la mayor carga útil. |
| <code>-t rsa-md5 y</code><br><code>-t rsa-sha1</code> | <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.                                                                                                                                              |

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 `certrldb`.

## 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 274](#). 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 279](#).

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 288](#).

## 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 6000 en lugar de en el 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`

En el directorio `/etc/inet/secret/ike.privatekeys`, se almacenan archivos de clave privada que forman parte del par de claves pública-privada. 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 clave pública se almacenan en el directorio `/etc/inet/ike/publickeys` o en hardware admitido.

## 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 certrladb` 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 21, “Filtro IP \(tareas\)”](#).

Este capítulo contiene la información siguiente:

- “Introducción al filtro IP” en la página 309
- “Procesamiento de paquetes del filtro IP” en la página 310
- “Directrices para utilizar el filtro IP” en la página 313
- “Uso de archivos de configuración del filtro IP” en la página 314
- “Uso de conjuntos de reglas de filtro IP” en la página 314
- “Enlaces de filtros de paquetes” en la página 320
- “IPv6 para filtro IP” en la página 320
- “Páginas del comando `man` del filtro IP” en la página 321

### Introducción al filtro IP

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 del software de filtro IP de código abierto. Para consultar los términos de la licencia y declaraciones de copyright del 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.

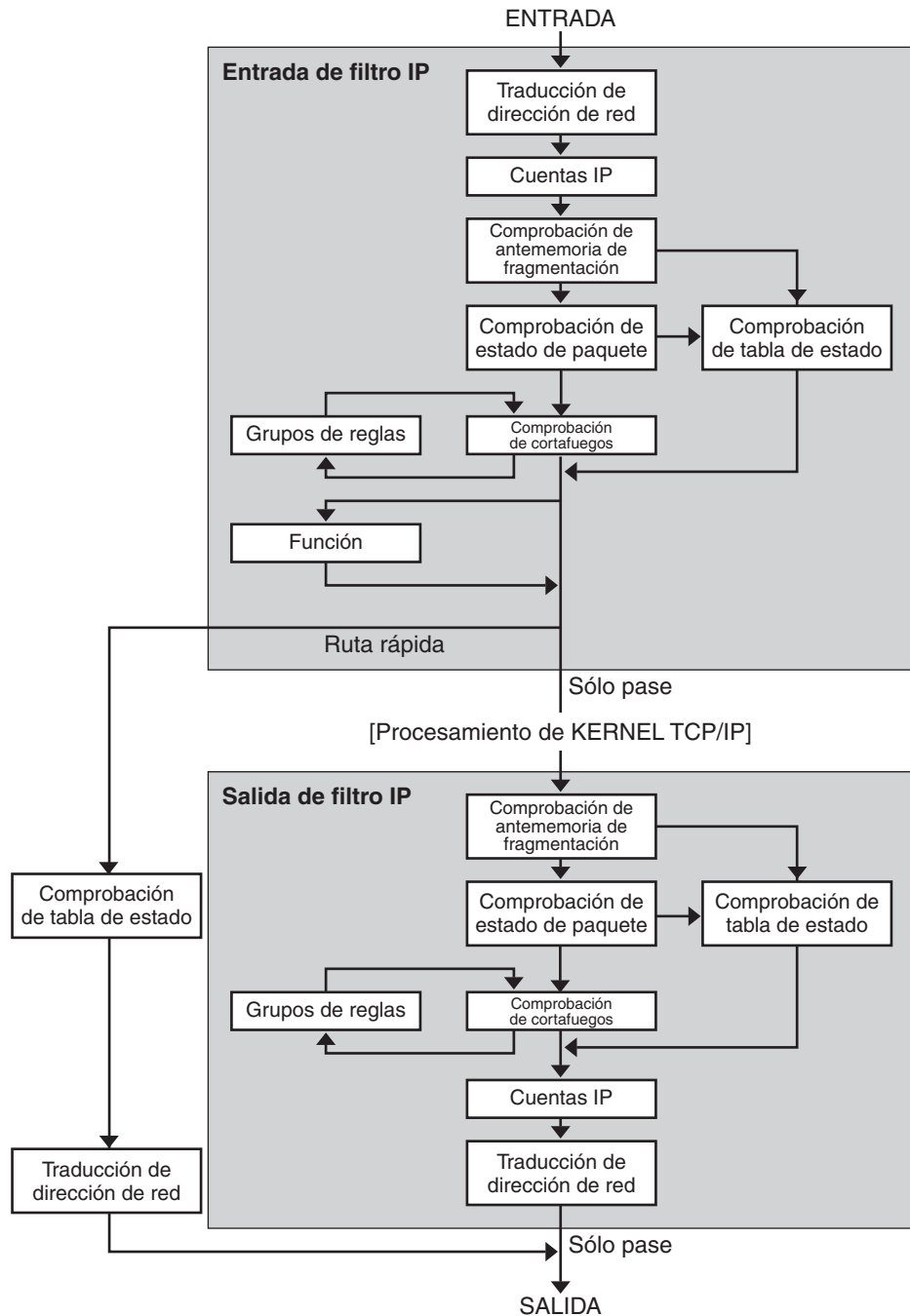
## Fuentes de información para el filtro IP de código abierto

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 enlace 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 del filtro IP.

## 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 20-1 Secuencia de procesamiento de paquetes



La secuencia de procesamiento de paquetes incluye:

- **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 6, “Gestión de servicios \(descripción general\)”](#) de *Administración de Oracle Solaris: tareas comunes*. Si desea información detallada sobre los procedimientos asociados con SMF, consulte el [Capítulo 7, “Gestión de servicios \(tareas\)”](#) de *Administración de Oracle Solaris: tareas comunes*.
- 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 el filtrado reiniciando el sistema o conectando las interfaces con el comando `ipadm`. Para obtener más información, consulte la página del comando `man ipadm(1M)`. Para conocer las tareas asociadas con la activación del filtro IP, consulte [“Configuración de filtro IP”](#) en la [página 323](#).
- 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 inicial de RBAC \(mapa de tareas\)”](#) de *Administración de Oracle Solaris: servicios de seguridad*.
- Las rutas múltiples de redes IP (IPMP) sólo admiten filtros sin estado.  
 Para que el filtro IP realice un filtrado sin estado en tráfico hacia un grupo IPMP y desde un grupo IPMP, debe especificar el parámetro `ipmp_hook_emulation`. De manera predeterminada, el parámetro está establecido en cero (0), lo que significa que el filtro IP no puede realizar una inspección de paquetes con estado del tráfico en interfaces físicas que pertenecen a un grupo IPMP. Para activar los filtros de paquetes IPMP, ejecute el siguiente comando:  

```
ndd -set /dev/ip ipmp_hook_emulation 1
```
- El software Oracle Solaris Cluster no admite el filtrado con filtro IP para servicios escalables, pero admite el filtro IP para servicios de conmutación por error. Para conocer las directrices y restricciones al configurar el filtro IP en un clúster, consulte [“Restricciones de las funciones del sistema operativo Oracle Solaris”](#) de *Guía de instalación del software de Oracle Solaris Cluster*.
- Se admite el filtrado entre zonas siempre que las reglas de filtro IP se implementen en una zona que funciona como enrutador virtual para las otras zonas del sistema.

## 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 348](#).

## Uso de conjuntos de reglas de 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.

|                          |                                                                                                                                                                                     |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>block</code>       | Impide que el paquete se transfiera a través del filtro.                                                                                                                            |
| <code>pass</code>        | Permite que el paquete se transfiera a través del filtro.                                                                                                                           |
| <code>log</code>         | Registra el paquete pero no determina si se bloquea o se transfiere. Utilice el comando <code>ipmon</code> para ver el registro.                                                    |
| <code>count</code>       | Incluye el paquete en las estadísticas de filtro. Utilice el comando <code>ipfstat</code> para ver las estadísticas.                                                                |
| <code>skip número</code> | Hace que el filtro omita <i>número</i> reglas de filtros.                                                                                                                           |
| <code>auth</code>        | 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.

|                    |                                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>log</code>   | Registra el paquete si la regla es la última regla coincidente. Utilice el comando <code>ipmon</code> para ver el registro.                        |
| <code>quick</code> | Ejecuta la regla que contiene la opción <code>quick</code> si hay coincidencia de paquetes. Se detiene cualquier comprobación de reglas adicional. |

- |                                       |                                                                                                                |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <code>on nombre_interfaz</code>       | Aplica la regla sólo si el paquete se transfiere a la interfaz especificada o desde ella.                      |
| <code>dup - to nombre_interfaz</code> | Copia el paquete y envía el duplicado de <i>nombre_interfaz</i> a una dirección IP especificada opcionalmente. |
| <code>to nombre_interfaz</code>       | 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> .                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <code>group <i>número</i></code>           | Agrega la regla al número de grupo <i>número</i> 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 330](#). Para ver una explicación del esquema de direcciones IP (192.168.0.0/16) que se muestra en el ejemplo, consulte el [Capítulo 1, “Planificación de la implementación de red”](#).

## 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`.

## 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:

|           |                                                                                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| map       | Asigna una red o dirección IP a otra red o dirección IP en un proceso por turnos.                                                                                          |
| rdr       | Redirige los paquetes de una dirección IP y un par de puertos a otra dirección IP y otro par de puertos.                                                                   |
| bimap     | Establece una NAT bidireccional entre una dirección IP externa y una dirección IP interna.                                                                                 |
| map-block | 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 bge0.

3. A continuación, puede elegir entre una serie de parámetros, que determinan la configuración de NAT. Algunos de los parámetros son:

|           |                                                                                      |
|-----------|--------------------------------------------------------------------------------------|
| ipmask    | Designa la máscara de red.                                                           |
| dstipmask | Designa la dirección a la que se traduce ipmask.                                     |
| mapport   | Designa los protocolos tcp, udp o tcp/udp, 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
```

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 `192.168.1.0` 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

En la versión actual, los enlaces de filtro 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, consulte el [Capítulo 21, “Filtro IP \(tareas\)”](#).

## 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 características de IPv6, consulte [“Características principales de IPv6” de Guía de administración del sistema: servicios IP](#).



**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 que se hayan configurado las reglas de filtrado de paquetes para IPv6, active las funciones de filtrado de paquetes IPv6 mediante la creación de la interfaz.

Para obtener más información sobre IPv6, consulte el [Capítulo 3, “Introducción a IPv6 \(descripción general\)”](#) de *Guía de administración del sistema: servicios IP*. Para conocer las tareas asociadas con el filtro IP, consulte el [Capítulo 21, “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 del comando man  | Descripción                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">ipf(1M)</a> | Utilice el comando <code>ipf</code> para: <ul style="list-style-type: none"><li>■ Trabajar con conjuntos de reglas de filtros de paquetes.</li><li>■ Desactivar y activar los filtros.</li><li>■ Restablecer las estadísticas y volver a sincronizar la lista de interfaces del núcleo con la lista de estado de la interfaz actual.</li></ul> |

| Página del comando man      | Descripción                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">ipf(4)</a>      | Contiene la gramática y la sintaxis para crear reglas de filtros de paquetes del filtro IP.                                                                                  |
| <a href="#">ipfilter(5)</a> | Proporciona información de licencia del filtro IP de código abierto.                                                                                                         |
| <a href="#">ipfs(1M)</a>    | Utilice el comando <code>ipfs</code> para guardar y restablecer la información NAT y la de la tabla de estado tras los reinicios.                                            |
| <a href="#">ipfstat(1M)</a> | Utilice el comando <code>ipfstat</code> para recuperar y mostrar las estadísticas de procesamiento de paquetes.                                                              |
| <a href="#">ipmon(1M)</a>   | Utilice el comando <code>ipmon</code> para abrir el dispositivo de registro y ver los paquetes registrados para NAT y los filtros de paquetes.                               |
| <a href="#">ipnat(1M)</a>   | Utilice el comando <code>ipnat</code> para: <ul style="list-style-type: none"> <li>■ Trabajar con reglas NAT.</li> <li>■ Recuperar y ver las estadísticas de NAT.</li> </ul> |
| <a href="#">ipnat(4)</a>    | Contiene la gramática y sintaxis para crear reglas NAT.                                                                                                                      |
| <a href="#">ippool(1M)</a>  | Utilice el comando <code>ippool</code> para crear y administrar agrupaciones de direcciones.                                                                                 |
| <a href="#">ippool(4)</a>   | Contiene la gramática y la sintaxis para crear agrupaciones de direcciones del filtro IP.                                                                                    |
| <a href="#">nnd(1M)</a>     | Muestra los parámetros de filtros actuales del módulo <code>pfil</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 20, “Filtro IP en Oracle Solaris \(descripción general\)”](#).

Este capítulo contiene la información siguiente:

- “Configuración de filtro IP” en la página 323
- “Desactivación y deshabilitación de filtro IP” en la página 327
- “Cómo trabajar con conjuntos de reglas del filtro IP” en la página 329
- “Cómo visualizar las estadísticas e información sobre el filtro IP” en la página 341
- “Cómo trabajar con archivos de registro para el filtro IP” en la página 344
- “Creación y edición de archivos de configuración del filtro IP” en la página 348

## Configuración de filtro IP

El siguiente mapa de tareas identifica los procedimientos asociados con la configuración del filtro IP.

**TABLA 21–1** 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. Los enlaces de filtro de paquetes reemplazan el módulo <code>pfil</code> para habilitar el filtro IP. | <a href="#">“Cómo habilitar el filtro IP” en la página 324</a> |

TABLA 21-1 Configuración del filtro IP (mapa de tareas) (Continuación)

| 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> . | <a href="#">“Cómo rehabilitar el filtro IP” en la página 325</a>     |
| Activar filtrado en bucle       | De modo opcional, puede activar el filtrado en bucle, por ejemplo, para filtrar el tráfico entre zonas.                                      | <a href="#">“Cómo activar los filtros en bucle” en la página 326</a> |

## ▼ Cómo habilitar 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 314](#). 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 348](#).

### 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 317](#).

#### 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 318](#).

#### 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 activar los filtros en bucle” en la página 326](#). 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 activar los filtros de paquetes que estén desactivados 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 activar los filtros 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

- 2 **Detenga el filtro IP si se está ejecutando.**

```
svcadm disable network/ipfilter
```

- 3 **Edita 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 filtro 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, utilice el comando siguiente:

```
ipf -T ipf_loopback
ipf_loopback min 0 max 0x1 current 1
#
```

Si el filtro en bucle está desactivado, el comando producirá el resultado siguiente:

```
ipf_loopback min 0 max 0x1 current 0
```

## Desactivación y deshabilitación de filtro IP

La desactivación 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 21-2 Desactivación del filtro IP (mapa de tareas)

| Tarea                                     | Descripción                                                        | Para obtener instrucciones                                                 |
|-------------------------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------|
| Desactivar los filtros de paquetes.       | Desactive los filtros de paquetes utilizando el comando ipf.       | <a href="#">“Cómo desactivar los filtros de paquetes” en la página 327</a> |
| Desactivar NAT.                           | Desactive NAT utilizando el comando ipnat.                         | <a href="#">“Cómo desactivar NAT” en la página 328</a>                     |
| Desactivar los filtros de paquetes y NAT. | Desactive los filtros de paquetes y NAT utilizando el comando ipf. | <a href="#">“Cómo desactivar los filtros de paquetes” en la página 328</a> |

### ▼ 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 desactivar 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 325](#).

- 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 conjuntos de reglas del filtro IP

El siguiente mapa de tareas identifica los procedimientos asociados con los conjuntos de reglas del filtro IP.

TABLA 21–3    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 330                   |
|                                                                                           | Visualiza un conjunto de reglas de filtros de paquetes activo.       | “Cómo visualizar el conjunto de reglas de filtros de paquetes activo” en la página 331                  |
|                                                                                           | Visualiza un conjunto de reglas de filtros de paquetes inactivo.     | “Cómo visualizar el conjunto de reglas de filtros de paquetes inactivo” en la página 331                |
|                                                                                           | Activa un conjunto de reglas activo distinto.                        | “Cómo activar un conjunto de reglas de filtros de paquetes diferente o actualizado” en la página 332    |
|                                                                                           | Elimina un conjunto de reglas.                                       | “Cómo eliminar un conjunto de reglas de filtros de paquetes” en la página 333                           |
|                                                                                           | Agrega reglas a los conjuntos de reglas.                             | “Cómo anexas reglas al conjunto de reglas de filtros de paquetes activo” en la página 334               |
|                                                                                           |                                                                      | “Cómo anexas reglas al conjunto de reglas de filtros de paquetes inactivo” en la página 335             |
|                                                                                           | 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 335 |

TABLA 21-3    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 336 |
|                                                                            | Visualiza las reglas NAT activas.                          | “Gestión de reglas NAT para filtro IP” en la página 337                                           |
|                                                                            | Elimina las reglas NAT.                                    | “Cómo eliminar reglas NAT” en la página 338                                                       |
| Administre, vea y modifique las agrupaciones de direcciones del filtro IP. | Agrega las reglas adicionales a las reglas NAT.            | “Como anexar reglas a las reglas NAT” en la página 338                                            |
|                                                                            | Visualiza las agrupaciones de direcciones activas.         | “Gestión de agrupaciones de direcciones para el filtro IP” en la página 339                       |
|                                                                            | Elimina una agrupación de direcciones.                     | “Cómo eliminar una agrupación de direcciones” en la página 340                                    |
|                                                                            | Agrega reglas adicionales a una agrupación de direcciones. | “Cómo anexar reglas a una agrupación de direcciones” en la página 340                             |

## 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 inicial de RBAC \(mapa de tareas\)](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

- 2 **Visualice el conjunto de reglas de filtros de paquetes activo que se ha cargado en el núcleo.**

```
ipfstat -io
```

### Ejemplo 21–1 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 inicial de RBAC \(mapa de tareas\)](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

- 2 **Visualice el conjunto de reglas de filtros de paquetes inactivo.**

```
ipfstat -I -io
```

### Ejemplo 21–2 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 21–3 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 21–4 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 21–5 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 dmf0 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

- 2 **Utilice uno de os 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\_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 21-6 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 21–7 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 21–8 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 21–9 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

- 2 **Visualice las reglas NAT activas.**

```
ipnat -l
```

### Ejemplo 21–10 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 inicial de RBAC \(mapa de tareas\)](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

- 2 **Elimine las reglas NAT actuales.**

```
ipnat -C
```

### Ejemplo 21–11 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 inicial de RBAC \(mapa de tareas\)](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

- 2 **Utilice uno de os 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 21–12 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 administrar, 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

- 2 **Visualice la agrupación de direcciones activa.**

```
ippool -l
```

### Ejemplo 21–13 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

- 2 **Elimine las entradas de la agrupación de direcciones actual.**

```
ippool -F
```

### Ejemplo 21-14 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

- 2 **Utilice uno de os 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 21–15**    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 21–4    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. | <a href="#">“Cómo ver las tablas de estado para el filtro IP” en la página 342</a>                                    |
| Ver las estadísticas de estado.                       | Visualiza las estadísticas sobre el estado de los paquetes utilizando el comando ipfstat -s.                  | <a href="#">“Cómo ver las tablas de estado para el filtro IP” en la página 342</a>                                    |
| Ver las estadísticas de NAT.                          | Visualiza las estadísticas de NAT utilizando el comando ipnat -s.                                             | <a href="#">“Cómo visualizar las estadísticas de NAT para el filtro IP” en la página 343</a>                          |
| Ver las estadísticas de la agrupación de direcciones. | Visualiza las estadísticas de la agrupación de direcciones utilizando el comando ippool -s.                   | <a href="#">“Cómo visualizar las estadísticas de la agrupación de direcciones para el filtro IP” en la página 344</a> |

## ▼ 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 21-16 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

## 2 Visualice las estadísticas de estado.

```
ipfstat -s
```

### Ejemplo 21-17 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

### 2 Ver las estadísticas de NAT.

```
ipnat -s
```

### Ejemplo 21-18 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).
- 2 **Ver las estadísticas de la agrupación de direcciones.**

```
ippool -s
```

**Ejemplo 21–19** 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 21–5    Cómo trabajar con archivos de registro para el filtro IP (mapa de tareas)

| Tarea                                    | Descripción                                                                                                | Para obtener instrucciones                                                                  |
|------------------------------------------|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Crear un archivo de registro.            | Cree un archivo de registro de filtro IP independiente.                                                    | <a href="#">“Cómo configurar un archivo de registro para el filtro IP” en la página 345</a> |
| Visualizar archivos de registro.         | Visualice el estado, la NAT y los archivos de registro normales utilizando el comando <code>ipmon</code> . | <a href="#">“Cómo visualizar los archivos de registro del filtro IP” en la página 346</a>   |
| Vaciar el búfer de registro de paquetes. | Elimine el contenido del búfer de registro de paquetes utilizando el comando <code>ipmon - F</code> .      | <a href="#">“Cómo vaciar el archivo de registro de paquetes” en la página 347</a>           |



| TABLA 21-5   Cómo trabajar con archivos de registro para el filtro IP (mapa de tareas)    (Continuación) |                                                                                       |                                                                                    |
|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Tarea                                                                                                    | Descripción                                                                           | Para obtener instrucciones                                                         |
| Guardar los paquetes registrados en un archivo.                                                          | Guarde los paquetes registrados en un archivo para poder consultarlos posteriormente. | <a href="#">“Cómo guardar paquetes registrados en un archivo” en la página 347</a> |

## ▼ 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

**2   Edite el archivo `/etc/syslog.conf` agregando las dos líneas siguientes:**

```
Save IP Filter 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 21-20   Creación de un registro del filtro IP**

En el ejemplo siguiente, se muestra cómo crear `ipmon.log` para archivar información de filtro IP.

En `/etc/syslog.conf`:

```
Save IP Filter 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 345](#).

- 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 inicial de RBAC \(mapa de tareas\)](#)” de *Administración de Oracle Solaris: 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 21–21 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 bge0 @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 bge0 @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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

- 2 **Vaciar el búfer de registro de paquetes.**

```
ipmon -F
```

### Ejemplo 21–22 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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 `Control-C` para que vuelva a aparecer la línea de comandos.

**Ejemplo 21–23 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 bge0 @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 bge0 @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 bge0 @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 bge0 @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 bge0 @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 bge0 @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 bge0 @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 bge0 @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 inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: 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 332](#).

Consulte [“Uso de la función de filtros de paquetes del filtro IP” en la página 314](#) 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 317](#) 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 318](#) 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 21–24 Configuración de host del filtro IP

En este ejemplo, se muestra una configuración en un equipo host con una interfaz de red `bge`.

```
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 que todos los datos entren y salgan de la interfaz `bge`. 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 21-25** Configuración del servidor del filtro IP

Este ejemplo muestra una configuración para un equipo host que actúa como servidor web. Esta máquina cuenta con una interfaz de red e1000g.

```
web server with an e1000g 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 e1000g0 from any to any head 100
block out log on e1000g0 from any to any head 200

web rules that get hit most often
pass in quick on e1000g0 proto tcp from any \
to e1000g0/32 port = http flags S keep state group 100
pass in quick on e1000g0 proto tcp from any \
to e1000g0/32 port = https flags S keep state group 100

inbound traffic - ssh, auth
pass in quick on e1000g0 proto tcp from any \
to e1000g0/32 port = 22 flags S keep state group 100
pass in log quick on e1000g0 proto tcp from any \
to e1000g0/32 port = 113 flags S keep state group 100
pass in log quick on e1000g0 proto tcp from any port = 113 \
to e1000g0/32 flags S keep state group 100

outbound traffic - DNS, auth, NTP, ssh, www, smtp
pass out quick on e1000g0 proto tcp/udp from e1000g0/32 \
to any port = domain flags S keep state group 200
pass in quick on e1000g0 proto udp from any \
port = domain to e1000g0/32 group 100

pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = 113 flags S keep state group 200
pass out quick on e1000g0 proto tcp from e1000g0/32 port = 113 \
to any flags S keep state group 200

pass out quick on e1000g0 proto udp from e1000g0/32 to any \
port = ntp group 200
pass in quick on e1000g0 proto udp from any \
port = ntp to e1000g0/32 port = ntp group 100
```

**EJEMPLO 21-25** Configuración del servidor del filtro IP (Continuación)

```
pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = ssh flags S keep state group 200

pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = http flags S keep state group 200
pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = https flags S keep state group 200

pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = smtp flags S keep state group 200

pass icmp packets in and out
pass in quick on e1000g0 proto icmp from any to e1000g0/32 keep state group 100
pass out quick on e1000g0 proto icmp from e1000g0/32 to any keep state group 200

block and ignore NETBIOS packets
block in quick on e1000g0 proto tcp from any \
to any port = 135 flags S keep state group 100

block in quick on e1000g0 proto tcp from any port = 137 \
to any flags S keep state group 100
block in quick on e1000g0 proto udp from any to any port = 137 group 100
block in quick on e1000g0 proto udp from any port = 137 to any group 100

block in quick on e1000g0 proto tcp from any port = 138 \
to any flags S keep state group 100
block in quick on e1000g0 proto udp from any port = 138 to any group 100

block in quick on e1000g0 proto tcp from any port = 139 to any flags S keep state
group 100
block in quick on e1000g0 proto udp from any port = 139 to any group 100
```

**EJEMPLO 21-26** Configuración del enrutador del filtro IP

En este ejemplo, se muestra una configuración para un enrutador que tiene una interfaz interna (nge) y una interfaz externa (ce1).

```
internal interface is nge0 at 192.168.1.1
external interface is nge1 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 nge0 all
block in log on nge1 all
block out log on nge0 all
```



**EJEMPLO 21-26** Configuración del enrutador del filtro IP *(Continuación)*

```

block out log on nge1 all

Packets going in/out of network interfaces that aren't on the loopback
interface should not exist.
block in log quick on nge0 from 127.0.0.0/8 to any
block in log quick on nge0 from any to 127.0.0.0/8
block in log quick on nge1 from 127.0.0.0/8 to any
block in log quick on nge1 from any to 127.0.0.0/8

Deny reserved addresses.
block in quick on nge1 from 10.0.0.0/8 to any
block in quick on nge1 from 172.16.0.0/12 to any
block in log quick on nge1 from 192.168.1.0/24 to any
block in quick on nge1 from 192.168.0.0/16 to any

Allow internal traffic
pass in quick on nge0 from 192.168.1.0/24 to 192.168.1.0/24
pass out quick on nge0 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 nge1 proto tcp/udp from nge1/32 to any port = domain keep state
pass in quick on nge0 proto tcp/udp from 192.168.1.2 to any port = domain keep state
pass in quick on nge0 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 nge0 proto udp from 192.168.1.0/24 to any port = 123 keep state
pass out quick on nge1 proto udp from any to any port = 123 keep state

Allow incoming mail
pass in quick on nge1 proto tcp from any to nge1/32 port = smtp keep state
pass in quick on nge1 proto tcp from any to nge1/32 port = smtp keep state
pass out quick on nge1 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 nge0 proto tcp from 192.168.1.0/24 to any port = 22 keep state
pass out quick on nge1 proto tcp from 192.168.1.0/24 to any port = 22 keep state

pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass out quick on nge1 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = 443 keep state
pass out quick on nge1 proto tcp from 192.168.1.0/24 to any port = 443 keep state

pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = nntp keep state
block in quick on nge1 proto tcp from any to any port = nntp keep state
pass out quick on nge1 proto tcp from 192.168.1.0/24 to any port = nntp keep state

pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = smtp keep state

```

**EJEMPLO 21-26** Configuración del enrutador del filtro IP (Continuación)

```
pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = whois keep state
pass out quick on nge1 proto tcp from any to any port = whois keep state
```

```
Allow ssh from offsite
pass in quick on nge1 proto tcp from any to nge1/32 port = 22 keep state
```

```
Allow ping out
pass in quick on nge0 proto icmp all keep state
pass out quick on nge1 proto icmp all keep state
```

```
allow auth out
pass out quick on nge1 proto tcp from nge1/32 to any port = 113 keep state
pass out quick on nge1 proto tcp from nge1/32 port = 113 to any keep state
```

```
return rst for incoming auth
block return-rst in quick on nge1 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 nge1 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 I V

# Rendimiento de redes

En esta parte, se tratan las funciones de rendimiento de redes, como el equilibrio de carga integrado y el protocolo de redundancia de enrutador virtual.



## Descripción general del equilibrador de carga integrado

---

El equilibrador de carga integrado (ILB), una función de Oracle Solaris, proporciona capacidades de equilibrio de carga de capa 3 y capa 4 para Oracle Solaris instalado en sistemas SPARC y basados en x86. El ILB intercepta las solicitudes entrantes de clientes, decide qué servidor back-end debe gestionar la solicitud sobre la base de reglas de equilibrio de carga y, luego, reenvía la solicitud al servidor seleccionado. El ILB realiza comprobaciones de estado opcionales y proporciona datos para los algoritmos de equilibrio de carga a fin de verificar si el servidor seleccionado puede gestionar la solicitud entrante.

En este capítulo, se tratan las secciones siguientes:

- “Terminología del ILB” en la página 358
- “Funciones del ILB” en la página 360
- “Procesos del ILB” en la página 365
- “Directrices para utilizar el ILB” en la página 366
- “ILB y la utilidad de gestión de servicios” en la página 366
- “Comandos y subcomandos del ILB” en la página 366

Entre las funciones clave del ILB se incluyen las siguientes:

- Admite los modos de funcionamiento Retorno de servidor directo (DSR) y Traducción de direcciones de red (NAT) sin estado para IPv4 e IPv6
- Permite la administración del ILB mediante una interfaz de línea de comandos (CLI)
- Proporciona capacidades de supervisión del servidor mediante comprobaciones de estado

El ILB tiene tres componentes principales:

- CLI `ilbadm`. Esta interfaz se puede utilizar para configurar las reglas de equilibrio de carga, realizar comprobaciones de estado opcionales y ver estadísticas.
- Biblioteca de configuración `libilb`. `ilbadm` y otras aplicaciones de terceros pueden utilizar la funcionalidad implementada en `libilb` para la administración del ILB.
- Daemon `ilbd`. Este daemon realiza las siguientes tareas:
  - Gestiona la configuración persistente

- Proporciona acceso en serie al módulo de núcleo del ILB; para ello, procesa la información de configuración y la envía al módulo de núcleo del ILB para su ejecución
- Realiza comprobaciones de estado e informa los resultados al módulo de núcleo del ILB de modo que la distribución de la carga se ajuste correctamente

## Terminología del ILB

En esta sección, se describen algunos términos que son útiles al implementar el ILB en los sistemas.

- purga de conexión** Un mecanismo que permite impedir que se realicen conexiones nuevas a un servidor que está deshabilitado administrativamente. Esta función es útil para cerrar los servidores sin interrumpir las conexiones o sesiones activas. Las conexiones existentes al servidor funcionarán normalmente. Una vez que el servidor está listo para gestionar las solicitudes, puede volver a habilitarse administrativamente, y el equilibrador de carga le reenviará las conexiones nuevas. El ILB proporciona esta capacidad únicamente a los servidores con servicios virtuales basados en NAT.
- modo Retorno de servidor directo (DSR)** Se refiere a las solicitudes entrantes de equilibrio de carga que se envían a los servidores back-end y permite que el tráfico que regresa de los servidores eluda el equilibrador de carga y se envíe directamente al cliente. La implementación actual de DSR del ILB no permite realizar un seguimiento de las conexiones TCP (es decir, no tiene un estado).
- Ventajas:
- Mejor rendimiento que NAT porque únicamente se cambia la dirección MAC de destino de los paquetes y los servidores responden directamente a los clientes.
  - Transparencia total: los servidores ven una conexión directamente desde la dirección IP del cliente y responden al cliente mediante la puerta de enlace predeterminada.
- Desventajas:
- El servidor back-end debe responder tanto a la dirección IP propia (para comprobaciones de estado) como a la dirección IP virtual (para tráfico con equilibrio de carga).
  - Dado que el equilibrador de carga no mantiene ningún estado de conexión (es decir, no tiene un estado), si se agregan o se eliminan servidores, se interrumpirá la conexión.
- algoritmo de equilibrio de carga** El algoritmo que el ILB utiliza para seleccionar un servidor back-end de un grupo de servidores para una solicitud entrante.

|                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>regla de equilibrio de carga</b>                                                                                                                                                          | <p>En un ILB, un servicio virtual está representado por una regla de equilibrio de carga y está definido por los parámetros siguientes:</p> <ul style="list-style-type: none"> <li>■ Dirección IP virtual</li> <li>■ Protocolo de transporte: TCP o UDP</li> <li>■ Número de puerto (o rango de puertos)</li> <li>■ Algoritmo de equilibrio de carga</li> <li>■ Tipo de modo de equilibrio de carga (DSR, NAT completa o NAT parcial)</li> <li>■ Grupos de servidores compuestos por un conjunto de servidores back-end</li> <li>■ Comprobaciones opcionales de estado de servidor que se pueden ejecutar para cada servidor en el grupo de servidores</li> <li>■ Puerto opcional para usar en comprobaciones de estado</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p><b>Nota</b> – Puede especificar comprobaciones de estado en un puerto determinado o en cualquier puerto daemon i lbd seleccione aleatoriamente del rango de puertos para el servidor.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>equilibrio de carga basado en NAT</b>                                                                                                                                                     | <ul style="list-style-type: none"> <li>■ Nombre de regla para representar un servicio virtual</li> </ul> <p>Implica volver a escribir la información del encabezado IP y gestiona el tráfico de solicitud y el tráfico de respuesta. Hay dos tipos de NAT: NAT parcial y NAT completa. Ambos tipos vuelven a escribir la dirección IP de destino. Sin embargo, la topología NAT completa también vuelve a escribir la dirección IP de origen, y el servidor puede tener la impresión de que todas las conexiones se originan del equilibrador de carga. NAT permite realizar un seguimiento de las conexiones TCP (es decir, tiene un estado).</p> <p>Ventajas:</p> <ul style="list-style-type: none"> <li>■ Funciona con todos los servidores back-end al cambiar la puerta de enlace predeterminada para que señale al equilibrador de carga.</li> <li>■ Dado que el equilibrador de carga mantiene el estado de conexión, es posible agregar o eliminar servidores sin que se interrumpa la conexión.</li> </ul> <p>Desventajas:</p> <ul style="list-style-type: none"> <li>■ Rendimiento más lento que DSR porque el procesamiento implica la manipulación del encabezado IP y los servidores envían respuestas al equilibrador de carga.</li> <li>■ Todos los servidores back-end deben usar el equilibrador de carga como puerta de enlace predeterminada.</li> </ul> |
| <b>configuración persistente</b>                                                                                                                                                             | En el contexto del ILB, una configuración persistente es una configuración (es decir, un conjunto de reglas de equilibrio de carga) que persiste tras reinicios y actualizaciones de paquetes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>origen de proxy</b>                                                                                                                                                                       | El rango de direcciones IP que pueden actuar como proxies. El rango se limita a 10 direcciones IP. El origen de proxy solamente es necesario en el caso de una implementación NAT completa.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>sesión</b>                                                                                                                                                                                | Está compuesta por un número de paquetes que provienen del mismo cliente durante un período y que pueden tener un significado en conjunto.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>persistencia de sesión</b>     | Permite que todos los paquetes de un cliente se envíen al mismo servidor back-end. También se conoce como permanencia. Puede configurar una persistencia de sesión simple (es decir, persistencia de dirección de origen) para un servicio virtual especificando las opciones <code>pmask=prefix length</code> y <code>persist-timeout=value in seconds</code> . Una vez que se establece la persistencia de sesión entre un cliente y un servidor, todos los paquetes del cliente al servidor virtual se reenvían al mismo servidor back-end mientras exista la persistencia. La longitud del prefijo en notación CIDR es un valor de 0 a 32 para IPv4 y de 0 a 128 para IPv6. |
| <b>grupo de servidores</b>        | Está compuesto por cero o más servidores back-end y debe contener al menos un servidor cuando se utiliza para un servicio virtual. Por ejemplo, si desea equilibrar la carga de solicitudes HTTP, debe configurar el ILB con un grupo de servidores compuesto por uno o más servidores back-end. El ILB equilibrará el tráfico HTTP en todo el conjunto configurado de servidores.                                                                                                                                                                                                                                                                                              |
| <b>ID de servidor</b>             | Un nombre exclusivo para la dirección IP asignada por el sistema cuando el servidor se agrega al grupo de servidores.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>dirección IP virtual (VIP)</b> | La dirección IP de un servicio virtual.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>servicio virtual</b>           | Un servicio que el cliente percibe como <code>VIP:port</code> . Por ejemplo: <code>www.foo.com:80</code> . Aunque el servicio es gestionado por un grupo de servidores compuesto, posiblemente, por más de un servidor, el grupo de servidores aparece para los clientes del servicio virtual como un único <code>IP address:port</code> . Un único servidor puede estar incluido en más de un grupo de servidores y, por lo tanto, puede funcionar en varios servicios virtuales. Además, un único servidor puede mantener varios servicios virtuales.                                                                                                                         |

## Funciones del ILB

En esta sección, se describen las funciones clave del ILB.

## Modos de funcionamiento del ILB

El ILB admite los modos de funcionamiento DSR y NAT sin estado para IPv4 e IPv6 en topologías de segmento único y de segmento doble.

- **Modo DSR sin estado:** en el modo DSR, el ILB equilibra las solicitudes entrantes que se envían a los servidores back-end, pero permite que el tráfico que regresa de los servidores al cliente eluda el equilibrador. Sin embargo, el ILB también se puede configurar para usarlo como enrutador para el servidor back-end. En este caso, la respuesta del servidor back-end al cliente se enruta a través de la máquina que ejecuta el ILB. Con DSR sin estado, el ILB no guarda ninguna información de estado de los paquetes procesados, excepto las estadísticas básicas. Dado que el ILB no guarda ningún estado en este modo, el rendimiento es comparable al rendimiento normal de reenvío de IP. Este modo es más adecuado para protocolos sin conexión.



- Modo NAT (NAT completa y NAT parcial): el ILB utiliza NAT en modo independiente exclusivamente para la funcionalidad de equilibrio de carga. En este modo, el ILB vuelve a escribir la información del encabezado y gestiona el tráfico entrante y el tráfico saliente. El modo NAT proporciona una seguridad adicional y es más adecuado para tráfico HTTP (o SSL).

---

**Nota** – La ruta de código NAT implementada en el ILB difiere de la ruta de código implementada en la función de filtro IP de Oracle Solaris. *No utilice ambas rutas de código simultáneamente.*

---

## Algoritmos del ILB

Los algoritmos del ILB controlan las distribuciones de tráfico y ofrecen diversas características para la distribución de cargas y la selección de servidores. El ILB proporciona los algoritmos siguientes para los dos modos de funcionamiento:

- Round-robin: en un algoritmo round-robin, el equilibrador de carga asigna las solicitudes a una lista de servidores por turnos. Una vez que se asigna una solicitud a un servidor, el servidor se mueve al final de la lista.
- Hash *src IP*: en el método hash de IP de origen, el equilibrador de carga selecciona un servidor según el valor hash de la dirección IP de origen de la solicitud entrante.
- Hash *src-IP, port*: en el método hash de puerto e IP de origen, el equilibrador de carga selecciona un servidor según el valor hash de la dirección IP de origen y el puerto de origen de la solicitud entrante.
- Hash *src-IP, VIP*: en el método hash de IP de origen y VIP, el equilibrador de carga selecciona un servidor según el valor hash de la dirección IP de origen y la dirección IP de destino de la solicitud entrante.

## Interfaz de línea de comandos del ILB

La CLI se encuentra en el directorio `/usr/sbin/ilbadm`. Incluye subcomandos para configurar reglas de equilibrio de carga, grupos de servidores y comprobaciones de estado. También incluye subcomandos para visualizar estadísticas y detalles de configuración. Los subcomandos se pueden dividir en dos categorías:

- Subcomandos de configuración. Estos subcomandos permiten realizar las siguientes tareas:
  - Crear y suprimir reglas de equilibrio de carga
  - Habilitar y deshabilitar reglas de equilibrio de carga
  - Crear y suprimir grupo de servidores
  - Agregar y eliminar servidores de un grupo de servidores
  - Habilitar y deshabilitar servidores back-end

- Crear y suprimir comprobaciones de estado de servidor para un grupo de servidores dentro de una regla de equilibrio de carga

---

**Nota** – Para administrar los subcomandos de configuración, necesita privilegios. Los privilegios se obtienen mediante el control de acceso basado en roles (RBAC). Para crear el rol apropiado y asignarlo a un usuario, consulte [“Configuración inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

---

- Subcomandos de visualización. Estos subcomandos permiten realizar las siguientes tareas:
  - Ver reglas de equilibrio de carga, grupos de servidores y comprobaciones de estado configurados
  - Ver estadísticas de reenvío de paquetes
  - Ver la tabla de conexiones NAT
  - Ver resultados de comprobaciones de estado
  - Ver la tabla de asignación de persistencia de sesión

---

**Nota** – No necesita privilegios para administrar los subcomandos de visualización.

---

Para ver una lista de los subcomandos `ilbadm`, consulte [“Comandos y subcomandos del ILB” en la página 366](#). Para obtener información más detallada sobre los subcomandos `ilbadm`, consulte la página del comando `man ilbadm(1M)`.

## Función de supervisión de servidores del ILB

El ILB ofrece una función opcional de supervisión de servidores que permite realizar comprobaciones de estado de servidor con las capacidades siguientes:

- Sondeos ping integrados
- Sondeos TCP integrados
- Sondeos UDP integrados
- Pruebas proporcionadas por el usuario que se pueden ejecutar como comprobaciones de estado de servidor

De manera predeterminada, el ILB no realiza ninguna comprobación de estado. Puede especificar comprobaciones de estado para cada grupo de servidores al crear una regla de equilibrio de carga. Puede configurar únicamente una comprobación de estado por regla de equilibrio de carga. Siempre que un servicio virtual esté habilitado, las comprobaciones de estado del grupo de servidores asociado con el servicio virtual se inician automáticamente y se

repite periódicamente. Las comprobaciones de estado se detienen cuando se deshabilita el servicio virtual. Los estados de las comprobaciones previas no se conservan cuando se vuelve a habilitar el servicio virtual.

Cuando usted especifica un sondeo de prueba TCP, UDP o personalizado para ejecutar una comprobación de estado, el ILB envía, de manera predeterminada, un sondeo ping para determinar si se puede acceder al servidor antes del envío del sondeo de prueba TCP, UDP o personalizado al servidor. El sondeo ping es un método para supervisar el estado del servidor. Si el sondeo ping falla, se deshabilita el servidor correspondiente y se le asigna el estado de comprobación unreachable. Si el sondeo ping es eficaz, pero el sondeo de prueba TCP, UDP o personalizado falla, se deshabilita el servidor y se le asigna el estado de comprobación dead.

**Nota –**

- Puede deshabilitar el sondeo ping predeterminado.
- El sondeo ping no se puede deshabilitar para el sondeo UDP. Por lo tanto, para la comprobaciones de estado UDP, el sondeo ping es siempre el sondeo predeterminado.

Puede configurar la comprobación de estado para los parámetros que se muestran en la tabla siguiente.

**TABLA 22-1** Configuración de parámetros de comprobación de estado

| Parámetros de comprobación de estado | Descripción                                                                                                                                                                                                                              |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hc-test                              | Especifica el tipo de comprobación de estado que se realizará.                                                                                                                                                                           |
| hc-timeout                           | Inicia un tiempo de espera cuando no se completa una comprobación de estado.                                                                                                                                                             |
| hc-interval                          | Especifica el intervalo entre comprobaciones de estado consecutivas.<br><br><b>Nota –</b> Los intervalos se seleccionan aleatoriamente entre los siguientes valores: $0.5 \times \text{hc-interval}$ y $1.5 \times \text{hc-interval}$ . |
| hc-count                             | Especifica el número de comprobaciones fallidas consecutivas antes de que un servidor se considere defectuoso.                                                                                                                           |

## Funciones adicionales del ILB

En esta sección, se describen las funciones adicionales del ILB.

- **Permite que los clientes hagan ping a direcciones IP virtuales (VIP).** El ILB puede responder a solicitudes de eco del protocolo de mensajes de control de Internet (ICMP) de VIP de los clientes. El ILB proporciona esta capacidad para los modos de funcionamiento DSR y NAT.

- **Permite agregar y eliminar servidores de un grupo de servidores sin interrumpir el servicio.** Puede agregar y eliminar dinámicamente servidores de un grupo de servidores sin interrumpir las conexiones existentes establecidas con los servidores back-end. El ILB proporciona esta capacidad para los modos de funcionamiento NAT.
- **Permite configurar la persistencia (permanencia) de sesión.** Para muchas aplicaciones, es importante que se envíen al mismo servidor back-end una serie de conexiones o paquetes (o ambos) del mismo cliente. Puede configurar la persistencia de sesión para un servicio virtual especificando la máscara de red en el subcomando `create-rule{-m persist=<netmask>}]`. Una vez que se crea una asignación persistente, las solicitudes subsiguientes de paquetes o conexiones (o ambos) que se envían a un servicio virtual con una dirección IP de origen coincidente del cliente se reenvían al mismo servidor back-end. La compatibilidad con el mecanismo de persistencia de sesión está disponible para los modos de funcionamiento DSR y NAT.
- **Permite realizar una purga de conexión.** El ILB admite esta capacidad únicamente para servidores de servicios virtuales basados en NAT. Esta capacidad impide que se envíen conexiones nuevas a un servidor que está deshabilitado. Las conexiones existentes al servidor seguirán funcionando. Después de que finalizan todas las conexiones a ese servidor, el servidor se puede cerrar para realizar el mantenimiento. Una vez que el servidor está listo para gestionar solicitudes, habilite el servidor para que el equilibrador de carga pueda reenviarle las conexiones nuevas. Esta función permite cerrar los servidores para realizar el mantenimiento sin interrumpir las conexiones o sesiones activas.
- **Permite equilibrar la carga de puertos TCP y UDP.** El ILB puede equilibrar la carga de todos los puertos de una dirección IP determinada en diferentes conjuntos de servidores sin que sea necesario configurar reglas explícitas para cada puerto. El ILB proporciona esta capacidad para los modos de funcionamiento DSR y NAT.
- **Permite especificar puertos independientes para servicios virtuales dentro del mismo grupo de servidores.** Con esta función, el ILB permite especificar distintos puertos de destino para distintos servidores en el mismo grupo de servidores para los modos de funcionamiento NAT.
- **Permite equilibrar la carga de un rango de puertos simple.** El ILB puede equilibrar la carga de un rango de puertos en la VIP para un grupo de servidores determinado. Para su comodidad, puede conservar las direcciones IP al equilibrar la carga de distintos rangos de puertos en la misma VIP para distintos conjuntos de servidores back-end. Además, cuando la persistencia de sesión está habilitada para el modo NAT, el ILB envía solicitudes al mismo servidor back-end desde la misma dirección IP del cliente para distintos puertos del rango.
- **Permite el cambio o la reducción del rango de puertos.** El cambio o la reducción del rango de puertos dependen del rango de puertos de un servidor en una regla de equilibrio de carga. Por lo tanto, si el rango de puertos de un servidor es distinto del rango de puertos VIP, se implementa automáticamente el cambio de puertos. Si el rango de puertos del servidor es un puerto único, se implementa la reducción de puertos. Estas funciones se proporcionan para los modos de funcionamiento NAT.

## Procesos del ILB

En esta sección, se describe el funcionamiento de los procesos del ILB, como el procesamiento de paquetes del cliente al servidor y del servidor al cliente.

### Procesamiento de paquetes del cliente al servidor:

1. El ILB recibe una solicitud entrante enviada por el cliente a una dirección VIP y compara la solicitud con una regla de equilibrio de carga.
2. Si el ILB encuentra una regla de equilibrio de carga coincidente, utiliza un algoritmo de equilibrio de carga para reenviar la solicitud al servidor back-end según el modo de funcionamiento.
  - En el modo DSR, el ILB reemplaza el encabezado MAC de la solicitud entrante con el encabezado MAC del servidor back-end seleccionado.
  - En el modo NAT parcial, el ILB reemplaza la dirección IP de destino y el número de puerto del protocolo de transporte de la solicitud entrante con los del servidor back-end seleccionado.
  - En el modo NAT completa, el ILB reemplaza la dirección IP de origen y el número de puerto del protocolo de transporte de la solicitud entrante con la dirección de origen NAT de la regla de equilibrio de carga. El ILB también reemplaza la dirección IP de destino y el número de puerto del protocolo de transporte de la solicitud entrante con los del servidor back-end seleccionado.
3. El ILB reenvía la solicitud entrante modificada al servidor back-end seleccionado.

### Procesamiento de paquetes del servidor al cliente:

1. El servidor back-end envía una respuesta al ILB para responder a la solicitud entrante del cliente.
2. Después de recibir la respuesta del servidor back-end, la acción del ILB se basa en el modo de funcionamiento, de la siguiente manera:
  - En el modo DSR normal, la respuesta del servidor back-end elude el ILB y pasa directamente al cliente. Sin embargo, si el ILB también se utiliza como enrutador para el servidor back-end, la respuesta del servidor back-end al cliente se enruta a través de la máquina que ejecuta el ILB.
  - En el modo NAT parcial y el modo NAT completa, el ILB compara la respuesta del servidor back-end con la solicitud entrante y reemplaza la dirección IP y el número de puerto del protocolo de transporte modificados con los de la solicitud entrante original. Luego, el ILB reenvía la respuesta al cliente.

## Directrices para utilizar el ILB

Las directrices siguientes describen cómo utilizar el ILB:

- Para administrar el ILB, debe asumir un rol que incluya el perfil de derechos de gestión del ILB o convertirse en superusuario. Puede asignar el perfil de derechos de gestión del ILB a un rol creado por usted. Para crear el rol y asignarlo a un usuario, consulte [“Configuración inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).
- Para habilitar la auditoría de los comandos de configuración del ILB, debe preseleccionar la clase de auditoría de administración de todo el sistema. Para ello, consulte [“Configuración del servicio de auditoría \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).
- Los componentes del espacio de usuario del ILB se suministran como un paquete IPS separado en el repositorio de Oracle Solaris, con nombres de paquetes que comienzan con `SUNwilib`. Debe descargar estos paquetes del depósito de Oracle Solaris con el comando `pkg install`. Para obtener instrucciones sobre cómo instalar el ILB, consulte [“Instalación del equilibrador de carga integrado” en la página 369](#).
- La implementación NAT del ILB en modo independiente se limita únicamente a la funcionalidad de equilibrio de carga.
- El ILB proporciona redundancia únicamente para errores de la máquina y no gestiona errores de conmutación. A partir de ahora, el ILB no proporciona sincronización entre distintas máquinas con ILB.

## ILB y la utilidad de gestión de servicios

ILB es gestionado por el servicio `svc:/network/loadbalancer/ilb:default` de la utilidad de gestión de servicios (SMF). Para obtener una descripción general sobre SMF, consulte el [Capítulo 6, “Gestión de servicios \(descripción general\)” de Administración de Oracle Solaris: tareas comunes](#). Para obtener información detallada sobre los procedimientos asociados con SMF, consulte el [Capítulo 7, “Gestión de servicios \(tareas\)” de Administración de Oracle Solaris: tareas comunes](#).

## Comandos y subcomandos del ILB

Puede utilizar `ilbadm` y sus subcomandos para manipular las reglas de equilibrio de carga. Para obtener información más detallada sobre los subcomandos `ilbadm`, consulte la página del comando `man ilbadm(1M)`.

TABLA 22-2 Comandos y subcomandos del ILB utilizados para manipular las reglas de equilibrio de carga

| Comando del ILB                                            | Descripción                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ilbadm create-rule</code>                            | Crea un <code>rule name</code> con las características determinadas.                                                                                                                                                                                                                                |
| <code>ilbadm show-rule</code>                              | Muestra las características de las reglas especificadas o muestra todas las reglas si no se especifica ninguna regla.                                                                                                                                                                               |
| <code>ilbadm delete-rule</code>                            | Elimina toda la información relativa a un <code>rule name</code> . Si el nombre no existe, este subcomando falla.                                                                                                                                                                                   |
| <code>ilbadm enable-rule</code>                            | Habilita una regla designada o todas las reglas si no se especifica ningún nombre.                                                                                                                                                                                                                  |
| <code>ilbadm disable-rule</code>                           | Deshabilita una regla designada o todas las reglas si no se especifica ningún nombre.                                                                                                                                                                                                               |
| <code>ilbadm show-statistics</code>                        | Muestra estadísticas. Por ejemplo, <code>-t</code> con este subcomando incluye un indicador de fecha y hora con cada encabezado.                                                                                                                                                                    |
| <code>ilbadm show-hc-result</code>                         | Muestra los resultados de comprobación de estado para los servidores que están asociados con el nombre especificado de la regla <code>rule-name</code> . Si no se especifica <code>rule-name</code> , se muestran los resultados de comprobación de estado de los servidores para todas las reglas. |
| <code>ilbadm show-nat</code>                               | Muestra la información de la tabla NAT.                                                                                                                                                                                                                                                             |
| <code>ilbadm create-servergroup</code>                     | Crea un grupo de servidores. Se pueden agregar servidores adicionales con <code>ilbadm add-server</code> .                                                                                                                                                                                          |
| <code>ilbadm delete-servergroup</code>                     | Suprime un grupo de servidores.                                                                                                                                                                                                                                                                     |
| <code>ilbadm show-servergroup</code>                       | Enumera un grupo de servidores o enumera todos los grupos de servidores si no se especifica ningún grupo de servidores.                                                                                                                                                                             |
| <code>ilbadm enable-server</code>                          | Habilita un servidor deshabilitado.                                                                                                                                                                                                                                                                 |
| <code>ilbadm disable-server</code>                         | Habilita los servidores especificados.                                                                                                                                                                                                                                                              |
| <code>ilbadm add-server</code>                             | Agrega los servidores especificados a grupos de servidores.                                                                                                                                                                                                                                         |
| <code>ilbadm show-server</code>                            | Muestra los servidores asociados con las reglas designadas o muestra todos los servidores si no se especifica un nombre de regla.                                                                                                                                                                   |
| <code>ilbadm remove-server</code>                          | Elimina servidores de un grupo de servidores.                                                                                                                                                                                                                                                       |
| <code>ilbadm create-healthcheck</code>                     | Configura información de comprobación de estado que se puede utilizar para configurar reglas.                                                                                                                                                                                                       |
| <code>ilbadm show-persist</code>                           | Muestra la tabla de asignación de persistencia de sesión.                                                                                                                                                                                                                                           |
| <code>ilbadm export-config</code><br><i>nombre_archivo</i> | Utiliza el comando <code>ilbadm import</code> para exportar el archivo de configuración existente en un formato adecuado para importar. Si no se especifica <i>nombre_archivo</i> , <code>ilbadm export</code> escribe en <code>stdout</code> .                                                     |

**TABLA 22-2** Comandos y subcomandos del ILB utilizados para manipular las reglas de equilibrio de carga  
*(Continuación)*

| Comando del ILB                                     | Descripción                                                                                                                                                                                              |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ilbadm import-config -p nombre_archivo</code> | Importa un archivo y reemplaza la configuración existente con el contenido de este archivo importado. Si no se especifica <i>nombre_archivo</i> , <code>ilbadm import</code> lee de <code>stdin</code> . |



## Configuración del equilibrador de carga integrado (tarefas)

---

En este capítulo, se describe la instalación y configuración del equilibrador de carga integrado (ILB) y se incluyen las secciones siguientes:

- “Instalación del equilibrador de carga integrado” en la página 369
- “Habilitación y deshabilitación del ILB” en la página 370
- “Configuración del ILB” en la página 371
- “Configuración del ILB de alta disponibilidad (únicamente modo activo-pasivo)” en la página 375
- “Configuración de la autorización del usuario para los subcomandos de configuración del ILB” en la página 380
- “Administración de grupos de servidores del ILB” en la página 381
- “Administración de servidores back-end en el ILB” en la página 382
- “Administración de comprobaciones de estado en el ILB” en la página 385
- “Administración de reglas del ILB” en la página 388
- “Visualización de estadísticas del ILB” en la página 389
- “Uso de los subcomandos `import` y `export`” en la página 391

### Instalación del equilibrador de carga integrado

En esta sección, se describe la instalación del ILB.

El ILB tiene dos partes, el núcleo y el espacio de usuario. El núcleo se instala automáticamente como parte de la instalación de Oracle Solaris 11. Sin embargo, para obtener el espacio de usuario del ILB, el usuario debe instalar manualmente `ilb` que se encuentra en el paquete `service/network/load-balancer/ilb`.

# Habilitación y deshabilitación del ILB

En esta sección, se describen los procedimientos para habilitar y deshabilitar el ILB.

## ▼ Cómo habilitar el ILB

### Antes de empezar

Asegúrese de que los archivos de atributos de control de acceso basado en roles (RBAC) del sistema tengan las entradas siguientes (si no se incluyen las entradas, agréguelas manualmente):

- Nombre del archivo: `/etc/security/auth_attr`
  - `solaris.network.ilb.config::Network ILB Configuration::help=NetworkILBconf.html`
  - `solaris.network.ilb.enable::Network ILB Enable Configuration::help=NetworkILBenable.html`
  - `solaris.smf.manage.ilb::Manage Integrated Load Balancer Service States::help=SmfILBStates.html`
- Nombre del archivo: `/etc/security/prof_attr`
  - `Network ILB::Manage ILB configuration via ilbadm:auths=solaris.network.ilb.config,solaris.network.ilb.enable;help=RtNetILB.htm`
  - La entrada de gestión de red del archivo debe incluir `solaris.smf.manage.ilb`
- Nombre del archivo: `/etc/user_attr`
  - `daemon:::auths=solaris.smf.manage.ilb,solaris.smf.modify.application`

### 1 Asuma un rol que incluya el perfil con derechos de gestión de ILB, o conviértase en superusuario.

Puede asignar el perfil de derechos de gestión del ILB a un rol creado por usted. Para crear el rol y asignarlo a un usuario, consulte [“Configuración inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

### 2 Habilite el servicio de reenvío adecuado, IPv4 o IPv6, o ambos.

```
#svcadm enable svc:/network/ipv4-forwarding
svcadm enable svc:/network/ipv6-forwarding
```

### 3 Habilite el servicio ILB.

```
svcadm enable ilb
```

### 4 Verifique que el servicio ILB esté habilitado.

```
svcs ilb
```

## ▼ Cómo deshabilitar el ILB

- 1 **Asuma un rol que incluya el perfil de derechos de gestión del ILB en un rol creado por usted o conviértase en superusuario.**

Puede asignar el perfil de derechos de gestión del ILB a un rol creado por usted. Para crear el rol y asignarlo a un usuario, consulte [“Configuración inicial de RBAC \(mapa de tareas\)” de Administración de Oracle Solaris: servicios de seguridad](#).

- 2 **Deshabilite el servicio ILB.**

```
svcadm disable ilb
```

- 3 **Verifique que el servicio ILB esté deshabilitado.**

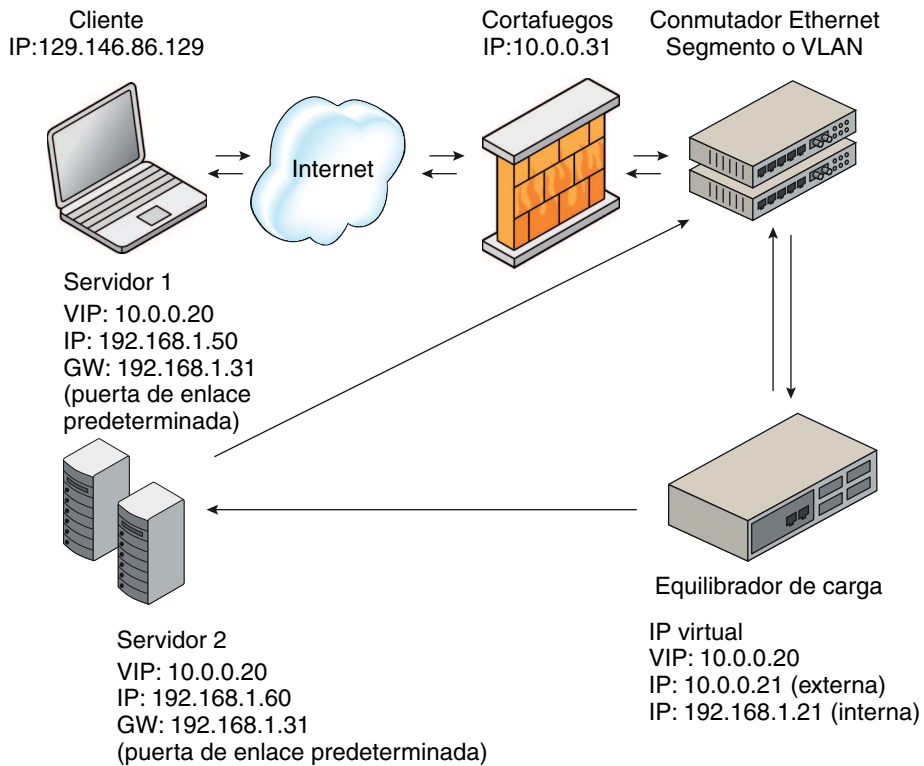
```
svcs ilb
```

## Configuración del ILB

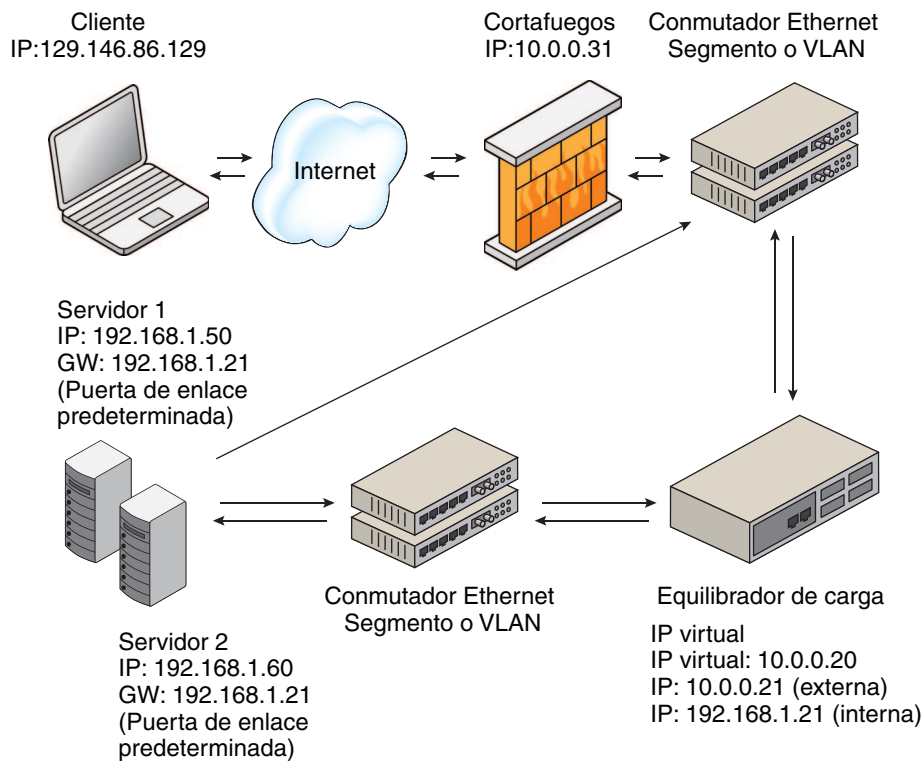
En esta sección, se describe la implementación del ILB con topologías DSR, NAT parcial y NAT completa.

### Topologías DSR, NAT parcial y NAT completa

En la figura siguiente, se muestra la implementación del ILB mediante la topología DSR.



ILB funciona en el modo NAT parcial y en el modo NAT completa. La implementación general de la topología NAT se muestra en la figura siguiente.



## Topología NAT parcial de equilibrio de carga

En el modo NAT parcial de funcionamiento del ILB, el ILB vuelve a escribir únicamente la dirección IP de destino en el encabezado de los paquetes. Si está utilizando la implementación NAT parcial, no puede conectarse a una dirección IP virtual (VIP) del servicio desde la misma subred en la que reside el servidor.

TABLA 23-1 Flujo de solicitud y flujo de respuesta para la implementación NAT parcial

| Flujo de solicitud |                                   | Dirección IP de origen        | Dirección IP de destino       |
|--------------------|-----------------------------------|-------------------------------|-------------------------------|
| 1.                 | Cliente -> Equilibrador de carga  | Cliente                       | VIP del equilibrador de carga |
| 2.                 | Equilibrador de carga -> Servidor | Cliente                       | Servidor                      |
| Flujo de respuesta |                                   |                               |                               |
| 3.                 | Servidor -> Equilibrador de carga | Servidor                      | Cliente                       |
| 4.                 | Equilibrador de carga -> Cliente  | VIP del equilibrador de carga | Cliente                       |

Si conecta la PC cliente a la misma red que los servidores, el servidor en cuestión responde directamente al cliente. El cuarto paso no se produce y, por lo tanto, la dirección IP de origen para la respuesta del servidor al cliente no es válida. Cuando el cliente envía una solicitud de conexión al equilibrador de carga, la respuesta se produce desde el servidor en cuestión. De ahora en adelante, la pila IP del cliente descartará correctamente todas las respuestas.

En ese caso, el flujo de solicitud y el flujo de respuesta continúan como se muestra en la tabla siguiente.

TABLA 23-2 Flujo de solicitud y flujo de respuesta para la implementación NAT parcial

| Flujo de solicitud                   | Dirección IP de origen | Dirección IP de destino       |
|--------------------------------------|------------------------|-------------------------------|
| 1. Cliente -> Equilibrador de carga  | Cliente                | VIP del equilibrador de carga |
| 2. Equilibrador de carga -> Servidor | Cliente                | Servidor                      |
| Flujo de respuesta                   |                        |                               |
| 3. Servidor -> Cliente               | Servidor               | Cliente                       |

## Topología NAT completa de equilibrio de carga

En la implementación NAT completa, se vuelven a escribir las direcciones IP de origen y de destino para garantizar que el tráfico pase por el equilibrador de carga en ambas direcciones. La topología NAT completa posibilita la conexión a la VIP desde la misma subred en la que se encuentran los servidores. En la tabla siguiente, se muestra la topología NAT completa para el ILB. No se requiere ninguna ruta predeterminada que pase a través de los servidores. La ruta predeterminada que pasa a través del equilibrador de carga es la dirección del enrutador en la subred C. En este escenario, el equilibrador de carga se comporta como un proxy.

TABLA 23-3 Flujo de solicitud y flujo de respuesta para la implementación NAT completa

| Flujo de solicitud                   | Dirección IP de origen                                     | Dirección IP de destino                                    |
|--------------------------------------|------------------------------------------------------------|------------------------------------------------------------|
| 1. Cliente -> Equilibrador de carga  | Cliente                                                    | VIP del equilibrador de carga                              |
| 2. Equilibrador de carga -> Servidor | Dirección de interfaz del equilibrador de carga (subred C) | Servidor                                                   |
| Flujo de respuesta                   |                                                            |                                                            |
| 3. Servidor -> Equilibrador de carga | Servidor                                                   | Dirección de interfaz del equilibrador de carga (subred C) |
| 4. Equilibrador de carga -> Cliente  | VIP del equilibrador de carga                              | Cliente                                                    |

## Configuración del ILB de alta disponibilidad (únicamente modo activo-pasivo)

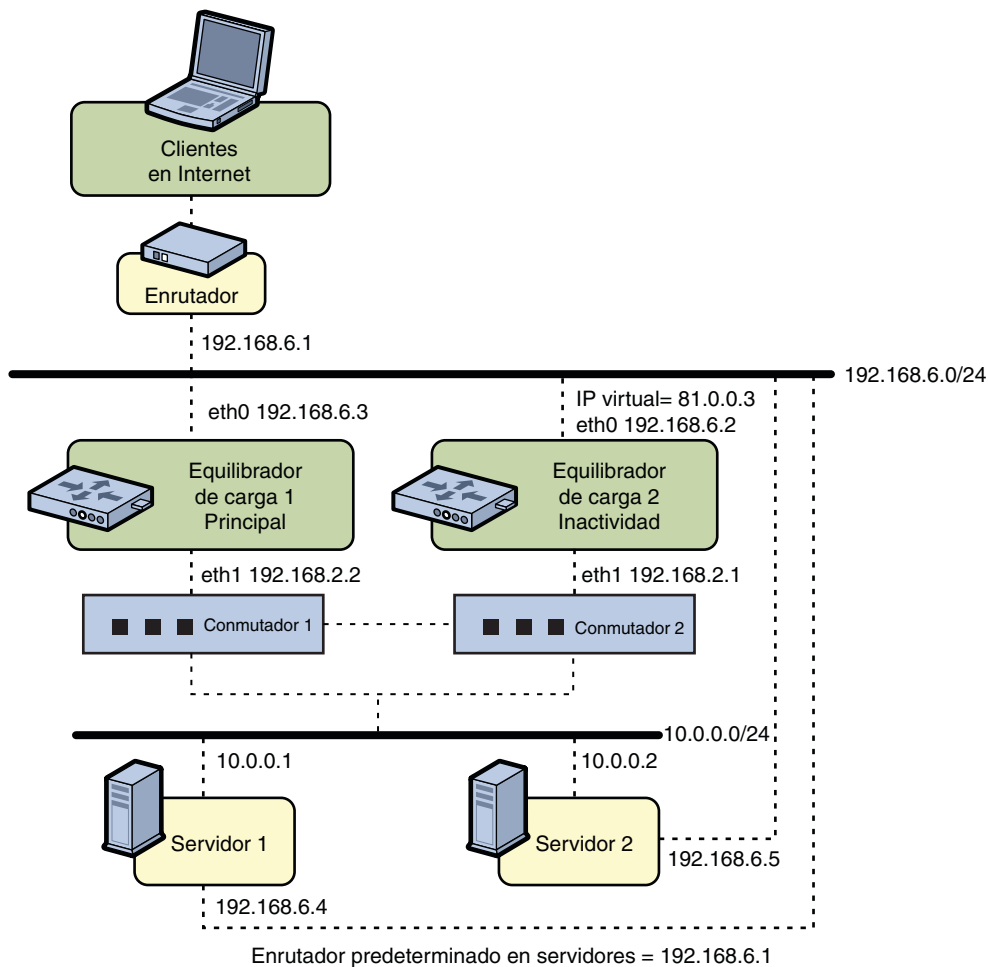
En esta sección, se describe la configuración del ILB de alta disponibilidad mediante las topologías DSR, NAT parcial y NAT completa.

### Configuración del ILB de alta disponibilidad mediante la topología DSR

En esta sección, se describe cómo configurar las conexiones del ILB para lograr alta disponibilidad mediante la topología DSR. Debe configurar dos equilibradores de carga, uno como el equilibrador de carga principal y el otro como el equilibrador de carga de reserva. Si el equilibrador de carga principal falla, el equilibrador de carga de reserva asume el rol del equilibrador de carga principal.

En la figura siguiente, se muestra la topología DSR para configurar las conexiones del ILB para lograr alta disponibilidad.

## Topología DSR



Todas las IP virtuales en los equilibradores de carga están configuradas en interfaces dirigidas a la subred 192.168.6.0/24.

## ▼ Cómo configurar el ILB para lograr alta disponibilidad mediante la topología DSR

- 1 Configure los equilibradores de carga principal y de reserva mediante los siguientes comandos del equilibrador de carga:

```
ilbadm create-servergroup -s server=10.0.0.1,10.0.0.2 sg1
ilbadm create-rule -i vip=81.0.0.3,port=9001 \
-m lbalg=hash-ip-port,type=DSR -o servergroup=sg1 rule1
```



**2 Asegúrese de que todos los servidores tengan configurada la VIP en la interfaz lo0.**

```
Server1# ipadm create-addr -T static -d -a 81.0.0.3/24 lo0/server1
Server2# ipadm create-addr -T static -d -a 81.0.0.3/24 lo0/server2
```

**3 Configure el equilibrador de carga 1 como el equilibrador de carga principal.**

```
LB1# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB1# vrrpadm create-router -V 1 -A inet -l eth0 -p 255 vrrp1
LB1# ipadm create-addr -T static -d -a 81.0.0.3/24 vnic1/lb1
```

**4 Configure el equilibrador de carga 2 como el equilibrador de carga de reserva.**

```
LB2# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB2# vrrpadm create-router -V 1 -A inet -l eth0 -p 100 vrrp1
LB2# ipadm create-addr -T static -d -a 81.0.0.3/24 vnic1/lb2
```

La configuración anterior proporciona protección contra los escenarios de fallo siguientes:

- Si el equilibrador de carga 1 falla, el equilibrador de carga 2 se convierte en el equilibrador de carga principal, asume la resolución de direcciones para la VIP 81.0.0.3 y gestiona todos los paquetes de los clientes con la dirección IP de destino 81.0.0.3.

Cuando el equilibrador de carga 1 se recupera, el equilibrador de carga 2 vuelve al modo de reserva.

- Si una o ambas interfaces del equilibrador de carga 1 fallan, el equilibrador de carga 2 asume el rol de equilibrador principal. De esta manera, el equilibrador de carga 2 asume la resolución de direcciones para la VIP 81.0.0.3 y gestiona todos los paquetes de los clientes con la dirección IP de destino 81.0.0.3.

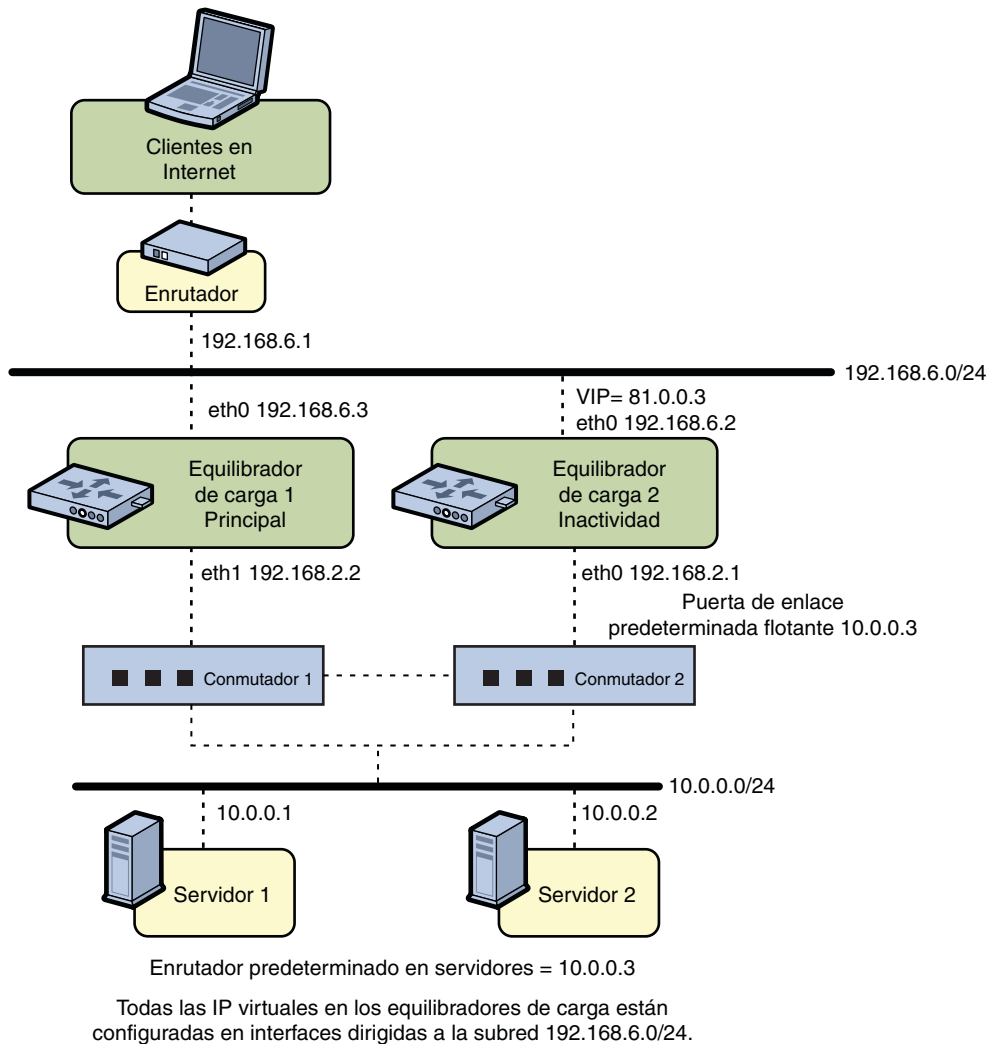
Cuando ambas interfaces del equilibrador de carga 1 funcionan correctamente, el equilibrador de carga 2 vuelve al modo de reserva.

## Configuración del ILB de alta disponibilidad mediante la topología NAT parcial

En esta sección, se describe cómo configurar las conexiones del ILB para lograr alta disponibilidad mediante la topología NAT parcial. Debe configurar dos equilibradores de carga, uno como el equilibrador de carga principal y el otro como el equilibrador de carga de reserva. Si el equilibrador de carga principal falla, el equilibrador de carga de reserva asume el rol del equilibrador de carga principal.

En la figura siguiente, se muestra la topología NAT parcial para configurar las conexiones del ILB para lograr alta disponibilidad.

## Topología NAT parcial



## ▼ Cómo configurar el ILB para lograr alta disponibilidad mediante la topología NAT parcial

### 1 Configure los equilibradores de carga principal y de reserva.

```
ilbadm create servergroup -s server=10.0.0.1,10.0.0.2 sg1
ilbadm create-rule -ep -i vip=81.0.0.3,port=9001-9006,protocol=udp \
-m lbalg=roundrobin,type=HALF-NAT,pmask=24 \
-h hc-name=hc1,hc-port=9006 \
-t conn-drain=70,nat-timeout=70,persist-timeout=70 -o servergroup=sg1 rule1
```

**2 Configure el equilibrador de carga 1 como el equilibrador de carga principal.**

```
LB1# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB1# ipadm create-addr -T static -d -a 81.0.0.3/24 vnic1/lb1
LB1# vrrpadm create-router -V 1 -A inet -l eth0 -p 255 vrrp1
LB1# dladm create-vnic -m vrrp -V 2 -A inet -l eth1 vnic2
LB1# ipadm create-addr -T static -d -a 10.0.0.3/24 vnic2/lb1
LB1# vrrpadm create-router -V 2 -A inet -l eth1 -p 255 vrrp2
```

**3 Configure el equilibrador de carga 2 como el equilibrador de carga de reserva.**

```
LB2# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB2# ipadm create-addr -T static -d -a 81.0.0.3/24 vnic1/lb2
LB2# vrrpadm create-router -V 1 -A inet -l eth0 -p 100 vrrp1
LB2# dladm create-vnic -m vrrp -V 2 -A inet -l eth1 vnic2
LB2# ipadm create-addr -T static -d -a 10.0.0.3/24 vnic2/lb2
LB2# vrrpadm create-router -V 2 -A inet -l eth1 -p 100 vrrp2
```

**4 Agregue la dirección IP de la puerta de enlace móvil predeterminada para ambos servidores.**

```
route add net 192.168.6.0/24 10.0.0.3
```

La configuración anterior proporciona protección contra los escenarios de fallo siguientes:

- Si el equilibrador de carga 1 falla, el equilibrador de carga 2 se convierte en el equilibrador de carga principal, asume la resolución de direcciones para la VIP 81.0.0.3 y gestiona todos los paquetes de los clientes con la dirección IP de destino 81.0.0.3. También debe gestionar todos los paquetes que se envían a la dirección de la puerta de enlace móvil 10.0.0.3.

Cuando el equilibrador de carga 1 se recupera, el equilibrador de carga 2 vuelve al modo de reserva.

- Si una o ambas interfaces del equilibrador de carga 1 fallan, el equilibrador de carga 2 asume el rol de equilibrador principal. De esta manera, el equilibrador de carga 2 asume la resolución de direcciones para la VIP 81.0.0.3 y gestiona todos los paquetes de los clientes con la dirección IP de destino 81.0.0.3. También debe gestionar todos los paquetes destinados a la dirección de la puerta de enlace móvil 10.0.0.3.

Cuando ambas interfaces del equilibrador de carga 1 funcionan correctamente, el equilibrador de carga 2 vuelve al modo de reserva.

---

**Nota** – La implementación actual del ILB no sincroniza los equilibradores de carga principal y de reserva. Cuando el equilibrador de carga principal falla y el equilibrador de carga de reserva asume su rol, fallarán las conexiones existentes. Sin embargo, una alta disponibilidad sin sincronización sigue siendo valiosa en circunstancias en las que falla el equilibrador de carga principal.

---

## Configuración de la autorización del usuario para los subcomandos de configuración del ILB

Debe contar con la autorización RBAC `solaris.network.ilb.config` para ejecutar los siguientes subcomandos de configuración del ILB:

```
create-servergroup
delete-servergroup groupname
show-servergroup
add-server
remove-server
enable-server
disable-server
show-server
create-healthcheck
show-healthcheck
delete-healthcheck
show-rule
delete-rule
enable-rule
disable-rule
show-statistics
show-hc-result
show-nat
show-persist
export-config
import-config
```

Para asignar la autorización a un usuario existente, consulte el [Capítulo 9, “Uso del control de acceso basado en roles \(tarear\)” de \*Administración de Oracle Solaris: servicios de seguridad\*](#)

También puede proporcionar la autorización al crear una cuenta de usuario nueva en el sistema. Por ejemplo:

```
useradd -g 10 -u 1210 -A solaris.network.ilb.config ilbadmin
```

El comando `useradd` agrega un usuario nuevo a los archivos `/etc/passwd`, `/etc/shadow` y `/etc/user_attr`. La opción `-A` asigna la autorización al usuario.

# Administración de grupos de servidores del ILB

Puede utilizar el comando `ilbadm` para crear, suprimir y enumerar grupos de servidores del ILB. Para conocer la definición de un grupo de servidores, consulte [“Terminología del ILB” en la página 358](#).

## ▼ Cómo crear un grupo de servidores

- 1 Seleccione un nombre para el grupo de servidores que está por crear.
- 2 Seleccione los servidores que se deberán incluir en el grupo de servidores.  
Los servidores se pueden especificar por su nombre de host o dirección IP y puerto opcional.

- 3 Cree el grupo de servidores.

```
ilbadm create-servergroup -s servers=webserv1,webserv2,webserv3 webgroup
```

### Ejemplo 23–1 Creación de un grupo de servidores

En el ejemplo siguiente, se crea un grupo de servidores denominado `webgroup`, que está compuesto por tres servidores:

```
ilbadm create-servergroup -s servers=webserv1,webserv2,webserv3 webgroup
```

## ▼ Cómo suprimir un grupo de servidores

- 1 Seleccione el grupo de servidores que desea eliminar.  
El grupo de servidores no debe estar siendo utilizado por una regla activa. De lo contrario, fallará la supresión.

- 2 En la ventana de terminal, suprima el grupo de servidores.

```
ilbadm delete-servergroup webgroup
```

### Ejemplo 23–2 Supresión de un grupo de servidores

En el ejemplo siguiente, se elimina el grupo de servidores denominado `webgroup`:

```
ilbadm delete-servergroup webgroup
```

## Visualización de un grupo de servidores

En una ventana de terminal, escriba el subcomando `show-servergroup` para obtener información sobre un grupo de servidores específicos o sobre todos los grupos de servidores.

En el ejemplo siguiente, se presenta información detallada sobre todos los grupos de servidores:

```
ilbadm show-servergroup -o all
```

| sname     | serverID     | minport | maxport | IP_address    |
|-----------|--------------|---------|---------|---------------|
| specgroup | _specgroup.0 | 7001    | 7001    | 199.199.67.18 |
| specgroup | _specgroup.1 | 7001    | 7001    | 199.199.67.19 |
| test123   | _test123.0   | 7001    | 7001    | 199.199.67.18 |
| test123   | _test123.1   | 7001    | 7001    | 199.199.67.19 |

## Administración de servidores back-end en el ILB

Puede utilizar `ilbadm` para agregar, eliminar, habilitar y deshabilitar uno o más servidores back-end dentro de grupos de servidores. Para ver una lista de definiciones, consulte [“Terminología del ILB” en la página 358](#).

### ▼ Cómo agregar un servidor back-end a un grupo de servidores

- **Agregue un servidor back-end a un grupo de servidores.**

Las especificaciones del servidor deben incluir un nombre de host o una dirección IP, y también pueden incluir un puerto opcional o un rango de puertos. Dentro de un grupo de servidores, no se permiten entradas de servidor con la misma dirección IP.

```
ilbadm add-server -e -s server=192.168.89.1,192.168.89.2 ftpgroup
ilbadm add-server -e -s server=[2001:7::feed:6]:8080 sgrp
```

La opción `-e` habilita los servidores, además de agregarlos al grupo.

---

**Nota** – Las direcciones IPv6 deben escribirse entre corchetes.

---

### Ejemplo 23–3    Cómo agregar un servidor back-end a un grupo de servidores

En el ejemplo siguiente, se agregan servidores a los grupos de servidores `ftpgroup` y `sgrp`, y se los habilita.

```
ilbadm add-server -e -s \
server=192.168.89.1,192.168.89.2 ftpgroup
ilbadm add-server -e -s server=[2001:7::feed:6]:8080 sgrp
```

## ▼ Cómo eliminar un servidor back-end de un grupo de servidores

- 1 Para eliminar un servidor de un grupo de servidores específico, siga estos pasos:
  - a. Identifique el ID del servidor que desea eliminar de un grupo de servidores. El ID del servidor se puede obtener de la salida del subcomando `show-servergroup -o all`.
  - b. Elimine el servidor.
 

```
ilbadm remove-server -s server=_specgroup.0 specgroup
```
- 2 Para eliminar un servidor de todos los grupos de servidores, siga los pasos que se describen a continuación:
  - a. Identifique la dirección IP y el nombre de host del servidor que desea eliminar.
  - b. Utilice la salida del comando `ilbadm show-servergroup -o all` para identificar los grupos de servidores que incluyen el servidor.
  - c. Para cada grupo de servidores, ejecute el siguiente subcomando para eliminar el servidor del grupo de servidores.

### Ejemplo 23–4 Eliminación de un servidor back-end de un grupo de servidores

En el ejemplo siguiente, se elimina el servidor con el ID 10.1.1.2 del grupo de servidores `websg`:

```
ilbadm remove-server -s server=_specgroup.0 specgroup
```

Tenga en cuenta lo siguiente:

- Si el servidor está siendo utilizado por una regla NAT o NAT parcial, deshabilite el servidor con el subcomando `disable-server` antes de eliminarlo. Cuando se deshabilita un servidor, entra en el estado de purga de conexión. Una vez que se purgan todas las conexiones, el servidor puede eliminarse con el subcomando `remove-server`. Después de emitir el comando `disable-server`, compruebe periódicamente la tabla NAT (con el comando `show-nat`) para ver si el servidor en cuestión aún tiene conexiones. Después de purgar todas las conexiones (el servidor no se visualiza en la salida del comando `show-nat`), el servidor puede eliminarse con el comando `remove-server`.
- Si se establece el valor de tiempo de espera de purga de conexión, el estado de purga de conexión se completará una vez que concluya el período de tiempo de espera. El valor predeterminado de tiempo de espera de purga de conexión es 0, lo cual significa que seguirá esperando hasta que se cierre correctamente una conexión.

## ▼ Cómo volver a habilitar o deshabilitar un servidor back-end

- 1 **Identifique la dirección IP, el nombre de host o el ID del servidor que desea volver a habilitar o deshabilitar. Si se especifica una dirección IP o un nombre de host, el servidor se volverá a habilitar o se deshabilitará para todas las reglas asociadas. Si se especifica un ID de servidor, el servidor se volverá a habilitar o se deshabilitará para las reglas específicas asociadas con el ID del servidor.**

---

**Nota** – Un servidor puede tener varios ID si pertenece a varios grupos de servidores.

---

- 2 **Vuelva a habilitar o deshabilite un servidor.**

```
ilbadm enable-server server
ilbadm disable-server server
```

### Ejemplo 23–5 Cómo volver a habilitar o deshabilitar un servidor back-end

En el ejemplo siguiente, se habilita y, luego, se deshabilita un servidor con el ID `websg.1`.

```
ilbadm enable-server websg.1
ilbadm disable-server websg.1
```



# Administración de comprobaciones de estado en el ILB

El usuario puede elegir entre los siguientes tipos opcionales de comprobaciones de estado de servidor proporcionados por el ILB:

- Sondeos ping integrados
- Sondeos TCP integrados
- Sondeos UDP integrados
- Pruebas proporcionadas por el usuario que se pueden ejecutar como comprobaciones de estado

De manera predeterminada, el ILB no realiza ninguna comprobación de estado. Puede especificar comprobaciones de estado para cada grupo de servidores al crear una regla de equilibrio de carga. Puede configurar únicamente una comprobación de estado por regla de equilibrio de carga. Siempre que un servicio virtual esté habilitado, las comprobaciones de estado del grupo de servidores asociado con el servicio virtual se inician automáticamente y se repiten periódicamente. Las comprobaciones de estado se detienen cuando se deshabilita el servicio virtual. Los estados de las comprobaciones previas no se conservan cuando se vuelve a habilitar el servicio virtual.

Cuando usted especifica un sondeo de prueba TCP, UDP o personalizado para ejecutar una comprobación de estado, el ILB envía, de manera predeterminada, un sondeo ping para determinar si se puede acceder al servidor antes del envío del sondeo de prueba TCP, UDP o personalizado al servidor. El sondeo ping es un método para supervisar el estado del servidor. Si el sondeo ping falla, se deshabilita el servidor correspondiente y se le asigna el estado de comprobación `unreachable`. Si el sondeo ping es eficaz, pero el sondeo de prueba TCP, UDP o personalizado falla, se deshabilita el servidor y se le asigna el estado de comprobación `dead`.

Puede utilizar el comando `ilbadm` para crear, suprimir y enumerar las comprobaciones de estado. Para ver una lista de definiciones, consulte [“Terminología del ILB” en la página 358](#).

## Creación de una comprobación de estado

En el ejemplo siguiente, se crean dos comprobaciones de estado: *objetos*, *cel* y *ce*, *mi\_secuencia\_comandos*. La primera comprobación de estado utiliza el sondeo TCP integrado. La segunda comprobación de estado utiliza una prueba personalizada: `/var/tmp/my-script`.

```
ilbadm create-healthcheck \
-h hc-timeout=3,hc-count=2,hc-interval=8,hc-test=tcp hc1
ilbadm create-healthcheck \
-h hc-timeout=3,hc-count=2,hc-interval=8,hc-test=/var/tmp/my-script hc-myscript
```

`hc-test` especifica el tipo de comprobación de estado.

`hc - interval` especifica el intervalo entre comprobaciones de estado consecutivas. Para evitar la sincronización, el intervalo real se selecciona aleatoriamente entre  $0.5 * hc - interval$  y  $1.5 * hc - interval$ .

`hc - timeout` especifica el tiempo de espera tras el cual se considera que la comprobación de estado falló si no se completa.

`hc - count` especifica el número de intentos para ejecutar la comprobación de estado `hc - test`.

---

**Nota** – Para especificar un puerto para `hc - test`, se utiliza la palabra clave `hc - port` en el subcomando `create - rule`. Para obtener detalles, consulte la página del comando [`man ilbadm\(1M\)`](#).

---

## Detalles de la prueba proporcionada por el usuario

La prueba proporcionada por el usuario debe cumplir con los siguientes criterios:

- La prueba puede ser binaria o una secuencia de comandos.
- La prueba puede residir en cualquier parte del sistema y usted debe especificar la ruta absoluta al utilizar el subcomando `create - healthcheck`.

Cuando especifica la prueba (por ejemplo, `/var/tmp/my-script`) como parte de la especificación de la comprobación de estado en el subcomando `create - rule`, el daemon `ilbd` bifurca un proceso y ejecuta la prueba, de la siguiente manera:

```
/var/tmp/my-script $1 $2 $3 $4 $5
```

A continuación, se describen los argumentos:

\$1 VIP (dirección IPv4 o IPv6 literal).

\$2 IP del servidor (dirección IPv4 o IPv6 literal).

\$3 Protocolo (UDP, TCP como una cadena).

\$4 Rango de puertos numérico (el valor especificado por el usuario para `hc - port`).

\$5 Tiempo máximo (en segundos) que la prueba debe esperar antes de devolver un error. Si la prueba se ejecuta más allá del tiempo especificado, es posible que se detenga, y se considerará que falló. Este valor es definido por el usuario y se especifica en `hc - timeout`.

La prueba proporcionada por el usuario, *my-script*, puede o no utilizar todos los argumentos, pero *debe* devolver uno de los siguientes valores:

- Tiempo de ida y vuelta (RTT) en microsegundos
- 0 si la prueba no calcula el RTT
- -1 en caso de error

De manera predeterminada, la prueba de comprobación de estado se ejecuta con los siguientes privilegios: `PRIV_PROC_FORK`, `RIV_PROC_EXEC`, `RIV_NET_ICMPACCESS`.

Si se necesita un conjunto de privilegios más amplio, se debe implementar `setuid` en la prueba. Para obtener más detalles sobre los privilegios, consulte la página del comando `man privileges(5)`.

## Supresión de una comprobación de estado

En el ejemplo siguiente, se suprime una comprobación de estado denominada `cel`:

```
ilbadm destroy-healthcheck hc1
```

## Enumeración de comprobaciones de estado

Puede utilizar el subcomando `list-healthcheck` para obtener información detallada sobre las comprobaciones de estado configuradas. En el ejemplo siguiente, se presentan dos comprobaciones de estado configuradas:

```
ilbadm list-healthcheck
```

| NAME | TIMEOUT | COUNT | INTERVAL | DEF_PING | TEST            |
|------|---------|-------|----------|----------|-----------------|
| hc1  | 3       | 2     | 8        | Y        | tcp             |
| hc2  | 3       | 2     | 8        | N        | /var/usr-script |

## Visualización de resultados de comprobaciones de estado

Puede utilizar el subcomando `list-hc-result` para ver los resultados de las comprobaciones de estado. Si no se especifica una regla o una comprobación de estado, el subcomando enumera todas las comprobaciones de estado.

En el ejemplo siguiente, se muestran los resultados de las comprobaciones de estado asociados con una regla denominada `rule1`:

```
ilbadm list-hc-result rule1
```

| RULE  | HC  | SERVERID | TEST | STATUS        | FAIL | LAST     | NEXT     |
|-------|-----|----------|------|---------------|------|----------|----------|
| rule1 | hc1 | sg1:0    | tcp  | server-alive3 |      | 11:23:30 | 11:23:40 |

| RULE  | HC  | SERVERID | TEST | STATUS      | FAIL | LAST     | NEXT     |
|-------|-----|----------|------|-------------|------|----------|----------|
| rule1 | hc1 | sg1:1    | tcp  | server-dead | 4    | 11:23:30 | 11:23:40 |

# Administración de reglas del ILB

Puede utilizar `ilbadm` para crear, suprimir y enumerar las reglas de equilibrio de carga. Para conocer la definición de una regla de equilibrio de carga y los parámetros necesarios para crear una regla, consulte [“Terminología del ILB” en la página 358](#).

## ▼ Cómo crear una regla

- 1 Cree un grupo de servidores que incluya los servidores back-end adecuados.  
`# ilbadm create-servergroup -s server=60.0.0.10:6000-6009,60.0.0.11:7000-7009 sg1`
- 2 Si desea asociar comprobaciones de estado de servidor con una regla, cree un objeto de comprobación de estado.  
`# ilbadm create-healthcheck -h hc-test=tc, hc-timeout=2, hc-count=3, hc-interval=10 hc1`
- 3 Identifique la VIP, el puerto y el protocolo opcional que se asociarán con la regla.
- 4 Seleccione el funcionamiento que desea utilizar (DSR, NAT completa o NAT parcial). Si selecciona NAT, debe especificar el rango de direcciones IP que se utilizará como la dirección `proxy-src`.
- 5 Seleccione el algoritmo de equilibrio de carga que se utilizará.
- 6 Seleccione otras funciones opcionales (consulte la página del comando `man ilbadm(1M)` para obtener detalles).
- 7 Seleccione un nombre de regla.
- 8 Cree y habilite la regla.

```
ilbadm create-rule -e -i vip=81.0.0.10,port=5000-5009,protocol=tcp\
-m lbalg=rr,type=NAT,proxy-src=60.0.0.101-60.0.0.104,persist=24 -h hc-name=hc1 -o servergroup=sg1 rule1
```

### Ejemplo 23–6 Creación de una regla NAT completa con persistencia de sesión de comprobación de estado

En este ejemplo, se crea una comprobación de estado denominada `hc1` y un grupo de servidores denominado `sg1` (compuesto por dos servidores, cada uno con rango de puertos). El último comando crea y habilita una regla denominada `rule1` con modo NAT completa y asocia la regla

con el grupo de servidores y la comprobación de estado. Tenga en cuenta que la creación del grupo de servidores y la comprobación de estado deben preceder a la creación de la regla.

```
ilbadm create-healthcheck -h hc-test=tcp,hc-timeout=2,hc-count=3,hc-interval=10 hc1
ilbadm create-servergroup -s server=60.0.0.10:6000-6009,60.0.0.11:7000-7009 sg1
ilbadm create-rule -e -i vip=81.0.0.10,port=5000-5009,protocol=tcp \
-m lbalg=rr,type=NAT,proxy-src=60.0.0.101-60.0.0.104,persist=/24
-h hc-name=hc1 -o servergroup=sg1 rule1
```

Al crear una regla NAT/NAT parcial, se recomienda especificar el valor de tiempo de espera de purga de conexión. El valor predeterminado de tiempo de espera de purga de conexión es 0, lo cual significa que seguirá esperando hasta que se cierre correctamente una conexión.

## Supresión de una regla

Para suprimir una regla, utilice el subcomando `delete-rule`. Si desea eliminar todas las reglas, utilice la opción `-a`. En el ejemplo siguiente, se suprime la regla denominada `rule1`:

```
ilbadm delete-rule rule1
```

## Enumeración de reglas

Para enumerar los detalles de configuración de una regla, utilice el subcomando `list-rule`. Si no se especifica ningún nombre de regla, se proporciona información para todas las reglas.

```
ilbadm list-rule
```

| RuleName (+ = enabled) | LB-alg | Type  | Proto | VIP/port          |
|------------------------|--------|-------|-------|-------------------|
| rule-http +            | HIPP   | H-NAT | TCP   | 10.0.0.1/http     |
| rule-dns               | HIP    | DSR   | UDP   | 10.0.0.1/53       |
| rule-abc               | RR     | NAT   | TCP   | 2003::1/1024      |
| rule-xyz +             | HIPV   | NAT   | TCP   | 2003::1/2048-2050 |

## Visualización de estadísticas del ILB

Puede utilizar el comando `ilbadm` para obtener información, como las estadísticas de impresión de un servidor o una regla, o para visualizar información de la tabla NAT y la tabla de asignación de persistencia de sesión. Para ver una lista de definiciones, consulte [“Terminología del ILB” en la página 358](#).

# Obtención de información estadística mediante el subcomando show-statistics

Utilice el subcomando `show-statistics` para ver los detalles de distribución de carga. En el ejemplo siguiente, se muestra el uso del subcomando `show-statistics`:

```
ilbadm show-statistics
PKT_P BYTES_P PKT_U BYTES_U PKT_D BYTES_D
 9 636 0 0 0 0
```

donde

- PKT\_P: paquetes procesados
- BYTES\_P: bytes procesados
- PKT\_U: paquetes no procesados
- BYTES\_U: bytes no procesados

## Visualización de la tabla de conexiones NAT

Utilice el subcomando `show-nat` para ver la tabla de conexiones NAT. No deben realizarse suposiciones sobre las posiciones relativas de los elementos en ejecuciones consecutivas de este comando. Por ejemplo, aunque `{{ ilbadm show-nat 10 }}` se ejecute dos veces, no se garantiza que se muestren los mismos 10 elementos dos veces, en especial, en un sistema ocupado. Si no se especifica un valor de recuento, se muestra toda la tabla de conexiones NAT.

En el ejemplo siguiente, se muestran cinco entradas de la tabla de conexiones NAT.

**EJEMPLO 23-7** Entradas de la tabla de conexiones NAT `ilbadm show-nat 5`

```
UDP: 124.106.235.150.53688 > 85.0.0.1.1024 >>> 82.0.0.39.4127 > 82.0.0.56.1024
UDP: 71.159.95.31.61528 > 85.0.0.1.1024 >>> 82.0.0.39.4146 > 82.0.0.55.1024
UDP: 9.213.106.54.19787 > 85.0.0.1.1024 >>> 82.0.0.40.4114 > 82.0.0.55.1024
UDP: 118.148.25.17.26676 > 85.0.0.1.1024 >>> 82.0.0.40.4112 > 82.0.0.56.1024
UDP: 69.219.132.153.56132 > 85.0.0.1.1024 >>> 82.0.0.39.4134 > 82.0.0.55.1024
```

El formato de las entradas es el siguiente:

```
T: IP1 > IP2 >>> IP3 > IP4
```

T: The transport protocol used in this entry.  
IP1: The client's IP address and port.  
IP2: The VIP and port.  
IP3: If half-NAT mode, the client's IP address and port.  
If full-NAT mode, the client's IP address and port.  
IP4: The back-end server's IP address and port.

## Visualización de la tabla de asignación de persistencia de sesión

Utilice el subcomando `show-persist` para ver la tabla de asignación de persistencia de sesión.

**EJEMPLO 23-8** `ilbadm show-persist 5`

En el ejemplo siguiente, se muestran cinco entradas de la tabla:

```
rule2: 124.106.235.150 --> 82.0.0.56
rule3: 71.159.95.31 --> 82.0.0.55
rule3: 9.213.106.54 --> 82.0.0.55
rule1: 118.148.25.17 --> 82.0.0.56
rule2: 69.219.132.153 --> 82.0.0.55
```

El formato de las entradas es el siguiente:

R: IP1 --> IP2

R: The rule that this persistence entry is tied to.

IP1: The client's IP address.

IP2: The back-end server's IP address.

## Uso de los subcomandos import y export

El subcomando `export` exporta la configuración actual a un archivo especificado por el usuario. Luego, esta información se puede utilizar como entrada para el subcomando `import`. El subcomando `import` suprime la configuración existente antes de la importación, a menos que se indique específicamente lo contrario. La omisión del nombre de un archivo le indica al comando que lea de la entrada estándar o que escriba en la salida estándar.

Para exportar la configuración de un ILB, utilice el comando `export-config`. En el ejemplo siguiente, se utiliza el subcomando `import` para exportar la configuración actual al archivo `/var/tmp/ilb_config` en un formato adecuado para importar:

```
ilbadm export-config /var/tmp/ilb_config
```

Para importar la configuración de un ILB, utilice el comando `import-config`. En el ejemplo siguiente, se lee el contenido de configuración del archivo `/var/tmp/ilb_config` y se sustituye la configuración existente:

```
ilbadm import-config /var/tmp/ilb_config
```





## Protocolo de redundancia de enrutador virtual (descripción general)

---

El protocolo de redundancia de enrutador virtual (VRRP) es un protocolo estándar de Internet especificado en [Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6](#) (protocolo de redundancia de enrutador virtual [versión 3] para IPv4 e IPv6) y se admite en Oracle Solaris para brindar alta disponibilidad. Oracle Solaris proporciona una herramienta administrativa que configura y gestiona el servicio VRRP.

Al configurar una red, como una LAN, es muy importante brindar un servicio de alta disponibilidad. Una manera de aumentar la confiabilidad de la red es realizar copias de seguridad de los componentes críticos. Agregar componentes, como enrutadores, conmutadores y enlaces, a la red garantiza la continuidad del servicio en caso de fallos. Ofrecer redundancia en los puntos finales de una red es una tarea crucial que se puede realizar fácilmente con VRRP. Se pueden agregar enrutadores virtuales a la LAN utilizando VRRP para ofrecer la recuperación tras fallos para un enrutador.

Para obtener más información sobre los términos utilizado en VRRP, consulte [“Terminología de VRRP” en la página 394](#).

En este capítulo, se incluyen las secciones siguientes:

- [“Terminología de VRRP” en la página 394](#)
- [“Descripción general de la arquitectura de VRRP” en la página 395](#)
- [“Limitaciones de VRRP” en la página 397](#)

VRRP es un protocolo de elección que asigna dinámicamente las responsabilidades de un enrutador virtual a uno de los enrutadores VRRP dentro de la LAN. VRRP proporciona uno o más enrutadores de respaldo para un enrutador configurado estáticamente en la LAN.

Un enrutador VRRP denominado enrutador maestro controla las direcciones IPv4 o IPv6 que están asociadas con el enrutador virtual. El enrutador virtual reenvía los paquetes enviados a la dirección IP del enrutador maestro.

El proceso de elección proporciona una conmutación por error dinámica durante el reenvío de paquetes a estas direcciones IP. VRRP elimina el único punto de fallo inherente al entorno enrutado estático predeterminado.

Al utilizar la función VRRP en Oracle Solaris, se puede tener una ruta predeterminada altamente disponible para el proceso de enrutamiento sin tener que configurar protocolos de enrutamiento dinámico o descubrimiento de enrutadores en cada host final.

## Terminología de VRRP

En esta sección, se describen algunos términos que son útiles al implementar VRRP en los sistemas.

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>enrutador de respaldo</b>          | Una instancia de VRRP para un VRID que está activo pero que no tiene el estado maestro. Para un VRID, puede existir cualquier número de copias de seguridad. Un enrutador de respaldo está listo para asumir el rol de enrutador maestro si el enrutador maestro actual falla.                                                                                                                                                                                                |
| <b>enrutador maestro</b>              | Una instancia de VRRP que realiza la función de enrutamiento para el enrutador virtual en un momento determinado. Únicamente hay un enrutador maestro activo a la vez para un VRID determinado.                                                                                                                                                                                                                                                                               |
| <b>dirección IP virtual</b>           | Una dirección IP asociada con un VRID que otros hosts pueden utilizar para obtener el servicio de red. La VRIP es gestionada por las instancias de VRRP que pertenecen a un VRID.                                                                                                                                                                                                                                                                                             |
| <b>dirección MAC virtual</b>          | Una dirección MAC predefinida utilizada por instancias de VRRP durante la ejecución en un medio, como Ethernet que utiliza direcciones MAC. Una dirección MAC virtual aísla el funcionamiento del enrutador virtual del enrutador real que proporciona la función de enrutamiento, y se utiliza en lugar de la dirección MAC real. Una dirección MAC virtual se deriva del VRID.                                                                                              |
| <b>ID de enrutador virtual (VRID)</b> | Un número exclusivo utilizado para identificar un enrutador virtual. Los VRID deben ser exclusivos en un segmento de red determinado.                                                                                                                                                                                                                                                                                                                                         |
| <b>VNIC</b>                           | Una pseudointerfaz de red que está configurada además del adaptador de red física de un sistema; también llamada tarjeta de interfaz de red (NIC). Una interfaz física puede tener más de una VNIC. Las VNIC son componentes fundamentales de la virtualización de red. Para obtener más información, consulte la <a href="#">Parte III, “Virtualización de la red y gestión de los recursos” de Administración de Oracle Solaris: interfaces y virtualización de redes</a> . |
| <b>instancia de VRRP</b>              | Un programa que se ejecuta en un enrutador utilizando la implementación de VRRP. Una única instancia de VRRP puede proporcionar capacidad VRRP para más de un enrutador virtual.                                                                                                                                                                                                                                                                                              |
| <b>enrutador VRRP</b>                 | Una única imagen de enrutador creada por el funcionamiento de uno o más enrutadores que utilizan VRRP.                                                                                                                                                                                                                                                                                                                                                                        |

# Descripción general de la arquitectura de VRRP

## Enrutador VRRP

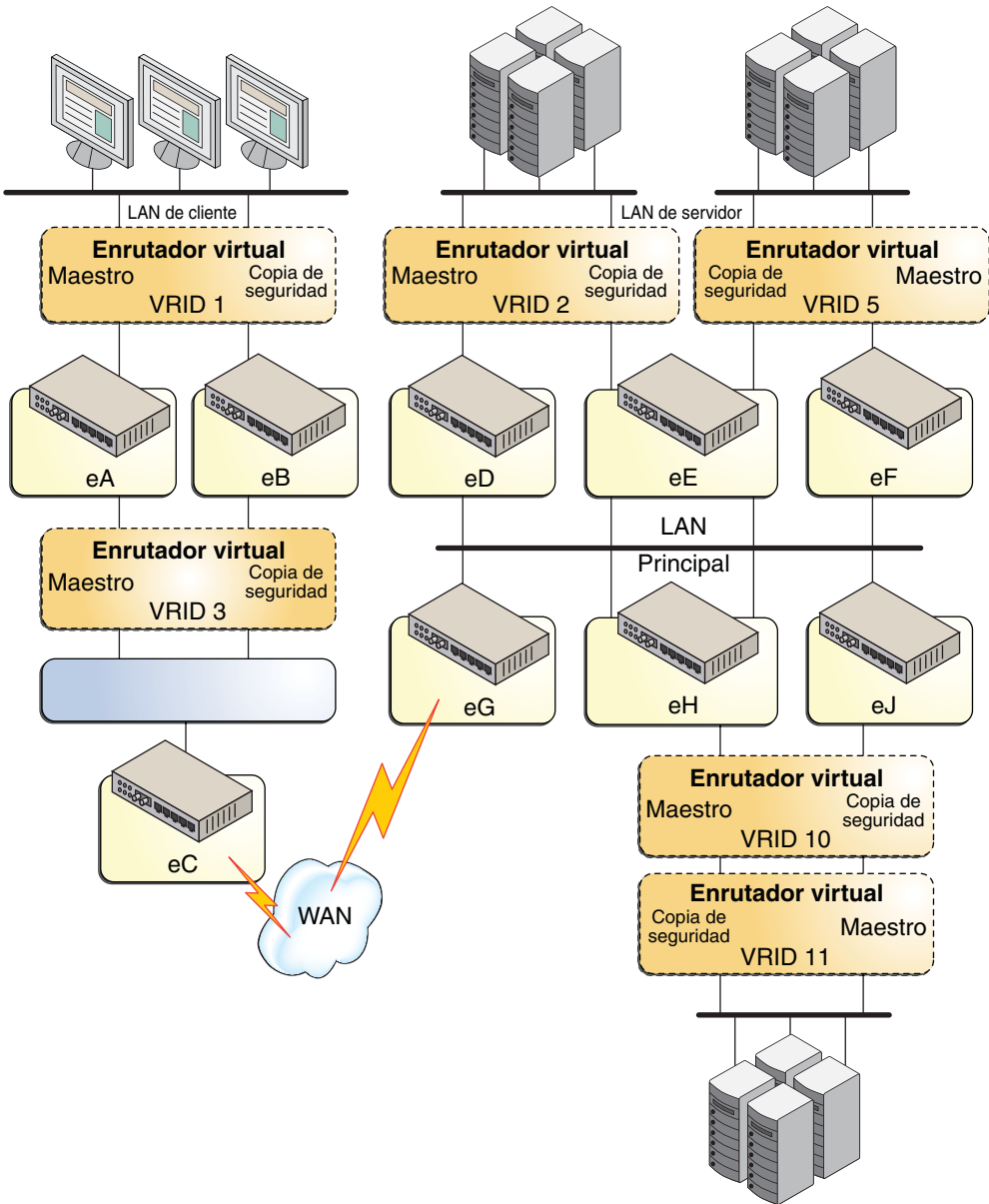
VRRP se ejecuta en cada enrutador VRRP y gestiona el estado del enrutador. Un host puede tener configurados varios enrutadores VRRP, donde cada enrutador VRRP pertenece a un enrutador virtual diferente.

Un enrutador VRRP tiene los atributos siguientes:

- Nombre de enrutador: un identificador exclusivo para todo el sistema
- VRID: identifica el enrutador virtual dentro de una LAN
- Dirección IP principal: utilizada como dirección IP de origen del anuncio VRRP
- Direcciones IP virtuales
- Parámetros VRRP: incluyen la prioridad, el intervalo de anuncio, el modo de cambio y el modo de aceptación
- Estadísticas e información de estado de VRRP

## Procesos de VRRP

En la figura siguiente, se muestra cómo funciona VRRP.



Como se muestra en la figura anterior, VRRP funciona con los siguientes componentes:

- El enrutador rA es el enrutador maestro para el enrutador virtual VRID 1 y el enrutador de respaldo para VRID 3. El enrutador rA gestiona el enrutamiento de paquetes que se envían a la VIP para VRID 1 y está listo para asumir el rol de enrutamiento para VRID 3.
- El enrutador rB es el enrutador maestro para el enrutador virtual VRID 3 y el enrutador de respaldo para VRID 1. El enrutador rB gestiona el enrutamiento de paquetes que se envían a la VIP para VRID 3 y está listo para asumir el rol de enrutamiento para VRID 1.
- El enrutador rC no tiene funciones de VRRP, pero utiliza la VIP para VRID 3 para llegar a la subred LAN del cliente.
- El enrutador rD es el enrutador maestro para VRID 2. El enrutador rF es el enrutador maestro para VRID 5. El enrutador rE es el enrutador maestro ambas VRID. Si rD o rF falla, rE se convierte en el enrutador maestro ese VRID. Tanto rD como rF pueden fallar al mismo tiempo. El hecho de que un enrutador VRRP sea un enrutador maestro para un VRID no impide que sea un enrutador maestro para otro VRID.
- El enrutador rG es la puerta de enlace WAN para la LAN principal. Todos los enrutadores conectados a la red principal comparten información de enrutamiento con los enrutadores de la WAN mediante un protocolo de enrutamiento dinámico, como Abrir primero la ruta más corta (OSPF). VRRP no participa en esto, aunque el enrutador rC anuncia que la ruta hasta la subred LAN del cliente es a través de la VIP de VRID 3.
- El enrutador rH es el enrutador maestro para VRID 10 y el enrutador de respaldo para VRID 11. Del mismo modo, el enrutador rJ es el enrutador maestro para VRID 11 y el enrutador de respaldo para VRID 10. Esta configuración de uso compartido de carga de VRRP ilustra que pueden existir varios VRID en una interfaz de enrutador única.

VRRP se puede utilizar como parte de un diseño de red que proporciona una redundancia casi total para todos los sistemas de la red.

## Limitaciones de VRRP

### Compatibilidad con zonas de IP exclusiva

En cada zona de IP exclusiva, el servicio VRRP `svc:/network/vrrp/default` se habilita automáticamente cuando se crea un enrutador VRRP en la zona determinada. El servicio VRRP gestiona el enrutador VRRP para esa zona específica.

Sin embargo, la compatibilidad con una zona de IP exclusiva es limitada debido a los siguientes motivos:

- VNIC no puede crearse dentro de una zona no global. Por lo tanto, primero cree la VNIC de VRRP en la zona global y, luego, asignar la VNIC a la zona no global donde reside el enrutador VRRP. De esta forma, el enrutador VRRP se puede crear e iniciar en la zona no global con el comando `vrpadm`.
- En un único sistema Oracle Solaris, no es posible crear dos enrutadores VRRP en zonas diferentes para que participen con el mismo enrutador virtual. El motivo es que Oracle Solaris no permite crear dos VNIC con la misma dirección MAC.

## Funcionamiento junto con otras funciones de red

El servicio VRRP no puede funcionar en una interfaz de rutas múltiples de redes IP (IPMP). Esto se debe a que VRRP requiere direcciones MAC VRRP específicas, mientras que IPMP funciona completamente en la capa IP.

Además, las direcciones IP virtuales VRRP únicamente se pueden configurar de manera estática y no pueden configurarse automáticamente con las dos herramientas existentes de configuración automática para direcciones IP: `in.ndpd` para la configuración automática de IPv6 y `dhcpgent` para la configuración DHCP. Dado que los enrutadores VRRP maestro y de respaldo (VNIC) comparten la misma dirección MAC, `in.ndpd` y `dhcpgent` pueden confundirse. Con el tiempo, pueden ocurrir resultados inesperados. Por lo tanto, la configuración automática de IPv6 y las configuraciones DHCP no se admiten en VNIC de VRRP. Si configura IPv6 automáticamente o configura DHCP en una VNIC de VRRP, fallará el intento de mostrar la dirección IP configurada automáticamente, al igual que la operación de configuración automática.

## Configuración VRRP (tareas)

---

Un enrutador VRRP ejecuta VRRP y trabaja con otros enrutadores VRRP que participan con el mismo enrutador virtual. VRRP tiene un conjunto de direcciones IP virtuales.

En este capítulo, se describen las secciones siguientes:

- “Creación de una VNIC de VRRP” en la página 400
- “Configuración vrrpadm” en la página 400
- “Consideraciones de seguridad” en la página 403

Dentro de una LAN, cada enrutador virtual se identifica de manera exclusiva con el VRID y la familia de direcciones, y está asociado con un conjunto de direcciones IP virtuales protegidas.

Cada enrutador VRRP participante tiene parámetros adicionales, como prioridad, intervalo de anuncio y modo de aceptación. Únicamente un enrutador VRRP (el maestro) a la vez asumirá la responsabilidad del enrutador virtual y reenviará los paquetes enviados a las direcciones IP virtuales.

Si falla el enrutador maestro, los otros enrutadores VRRP participantes detectarán su ausencia y otro enrutador VRRP será elegido como enrutador maestro y asumirá esa responsabilidad.

Todos los enrutadores VRRP con el mismo enrutador virtual comparten la misma dirección MAC virtual VRRP. La dirección MAC virtual se calcula según la familia de direcciones y el VRID del enrutador virtual (en formato hexadecimal en orden de bits estándar de Internet). Por ejemplo:

IPv4: 00-00-5E-00-01-{VRID}

IPv6: 00-00-5E-00-02-{VRID}

Por lo tanto, primero debe crearse una VNIC de VRRP con la dirección MAC virtual para que el enrutador VRRP funcione correctamente. Todas las direcciones IP que residen en esta VNIC se consideran direcciones IP virtuales protegidas por el enrutador VRRP. Esas direcciones IP

virtuales residen en el enrutador de respaldo y se muestran cuando el enrutador se convierte en el enrutador maestro; de esta manera, se brinda una alta disponibilidad para estas direcciones IP virtuales.

## Creación de una VNIC de VRRP

El subcomando `dladm create-vnic` existente se amplió para permitir la creación de la VNIC de VRRP. La sintaxis es la siguiente:

```
dladm create-vnic [-t] [-R root-dir] [-l link] [-m vrrp -V VRID -A {inet | inet6}] [-v vlan-id] [-p prop=value[,...]] vnic-link
```

Se agregó un nuevo tipo de dirección VNIC: `vrrp`. Debe especificar el VRID y la familia de direcciones con este nuevo tipo de dirección VNIC.

Como resultado, se creará una VNIC con una dirección MAC de enrutador virtual conocida.

## Configuración `vrrpadm`

En las siguientes secciones, se resumen los subcomandos `vrrpadm`. Consulte la página del comando [man `vrrpadm`\(1M\)](#) para obtener detalles. Todos los subcomandos son persistentes, excepto por el subcomando `vrrpadm show-router`. Por ejemplo, el enrutador VRRP creado con `vrrpadm create-router` persistirá tras los reinicios.

### Subcomando `vrrpadm create-router`

El subcomando `vrrpadm create-router` crea un enrutador VRRP del VRID y la familia de direcciones especificados con los parámetros determinados. Cada enrutador VRRP requiere la creación de una VNIC de VRRP especial, y la VNIC se puede crear con el comando `dladm create-vnic`. Para obtener más información, consulte la página del comando [man `vrrpadm`\(1M\)](#). La sintaxis es la siguiente:

```
vrrpadm create-router -V vrid -l link -A {inet | inet6} [-p \
priority] [-i adv-interval] [-o flags]router-name
```

La opción `-o` se utiliza para configurar los modos de cambio y aceptación del enrutador VRRP. Los valores pueden ser: `preempt`, `un_preempt`, `accept`, `no_accept`. De manera predeterminada, ambos modos se establecen en `true`.

El *nombre\_enrutador* se utiliza como el identificador exclusivo de este enrutador VRRP y se utiliza en los otros subcomandos `vrrpadm`. En el nombre de un enrutador se permiten caracteres alfanuméricos (a-z, A-Z, 0-9) y guión bajo ('\_'). El nombre de un enrutador puede tener una longitud máxima de 31 caracteres.



## Subcomando vrrpadm modify-router

El subcomando `vrrpadm modify-router` cambia la configuración de un enrutador VRRP especificado. La sintaxis es la siguiente:

```
vrrpadm modify-router [-p priority] [-i adv-interval] [-o flags] \
router-name
```

## Subcomando vrrpadm delete-router

El subcomando `vrrpadm delete-router` suprime un enrutador VRRP especificado. La sintaxis es la siguiente:

```
vrrpadm delete-router router-name
```

## Subcomando vrrpadm disable-router

Un enrutador VRRP no funciona hasta que se habilita. De manera predeterminada, un enrutador VRRP se habilita cuando se crea por primera vez. Sin embargo, a veces es útil deshabilitar temporalmente un enrutador VRRP para realizar cambios de configuración y, luego, volver a habilitar el enrutador. La sintaxis es la siguiente:

```
vrrpadm disable-router router-name
```

## Subcomando vrrpadm enable-router

Un enrutador deshabilitado se puede volver a habilitar con el subcomando `enable-router`. Cuando se habilita el enrutador, deben existir el enlace de datos subyacente sobre el cual se crea el enrutador VRRP (especificado con la opción `-l` cuando el enrutador se crea con `vrrpadm create-router`) y la VNIC de VRRP del enrutador. De lo contrario, fallará la habilitación. La sintaxis es la siguiente:

```
vrrpadm enable-router router-name
```

## Subcomando vrrpadm show-router

El subcomando `vrrpadm show-router` muestra la configuración y el estado de un enrutador VRRP especificado. Para obtener más detalles, consulte la página del comando [man vrrpadm\(1M\)](#). La sintaxis es la siguiente:

```
vrrpadm show-router [-P | -x] [-p] [-o field[,...]] [router-name]
```

A continuación, se presentan ejemplos de la salida de `vrrpadm show-router`:

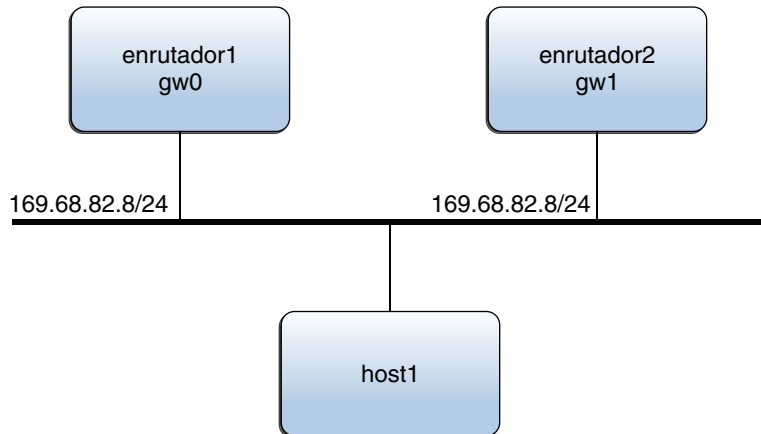
```
vrrpadm show-router vrrp1
NAME VRID LINK AF PRIO ADV_INTV MODE STATE VNIC
vrrp1 1 bge1 IPv4 100 1000 e-pa- BACK vnic1

vrrpadm show-router -x vrrp1
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 BACK MAST 1m17s vnic1 10.0.0.100 10.0.0.1

vrrpadm show-router -P vrrp1
NAME PEER P_PRIO P_INTV P_ADV_LAST M_DOWN_INTV
vrrp1 10.0.0.123 120 1000 0.313s 3609
```

#### EJEMPLO 25-1 Ejemplo de configuración VRRP

En la figura siguiente, se muestra una configuración VRRP típica.



En este ejemplo, la dirección IP 169.68.82.8 está configurada como la puerta de enlace predeterminada para host1. Esta dirección IP es la dirección IP virtual protegida por el enrutador virtual que está compuesto por dos enrutadores VRRP: router1 y router2. Únicamente uno de los dos enrutadores a la vez actúa como enrutador maestro, asume las responsabilidades del enrutador virtual y reenvía los paquetes provenientes de host1.

Suponga que el VRID del enrutador virtual es 12. A continuación, se muestran los pasos que se utilizan para establecer la configuración VRRP anterior en router1 y router2. router1 es el propietario de la dirección IP virtual 169.68.82.8 y su prioridad es el valor predeterminado (255). router2 es el enrutador de respaldo cuya prioridad es 100.

```
router1:
dladm create-vnic -m vrrp -V 12 -A inet -l gw0 vnic1
vrrpadm create-router -V 12 -A inet -l gw0 vrrp1
ipadm create-addr -T static -d -a 169.68.82.8/24 vnic1/router1
```

**EJEMPLO 25-1** Ejemplo de configuración VRRP (Continuación)

```
ipadm create-addr -T static -d -a 169.68.82.100/24 gw0/router1
vrrpadm show-router -x vrrp1
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 MAST BACK 1m17s vnic1 169.68.82.100 169.68.82.8
router2:
dladm create-vnic -m vrrp -V 12 -A inet -l gw1 vnic1
vrrpadm create-router -V 12 -A inet -l gw1 -p 100 vrrp1
ipadm create-addr -T static -d -a 169.68.82.8/24 vnic1/router2
ipadm create-addr -T static -d -a 169.68.82.101/24 gw0/router2
vrrpadm show-router -x vrrp1
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 BACK INIT 2m32s vnic1 169.68.82.101 169.68.82.8
```

Utilizando la configuración de router1 como ejemplo, debe configurar al menos una dirección IP en gw0. En el ejemplo siguiente, esta dirección IP de router1 es la dirección IP principal, que se utiliza para enviar los paquetes de anuncio de VRRP:

```
vrrpadm show-router -x vrrp1
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 MAST BACK 1m17s vnic1 169.68.82.100 169.68.82.8
```

## Consideraciones de seguridad

Se agregó una nueva autorización `solaris.network.vrrp`, que es necesaria para configurar el servicio VRRP. Tenga en cuenta que la operación de sólo lectura, `vrrpadm showrouter`, no necesita esta autorización.

La autorización `solaris.network.vrrp` se agregó al perfil de gestión de red.



# Implementación del control de congestión

En este capítulo, se trata la implementación del control de congestión en Oracle Solaris. Se establecen controles para evitar la congestión de tráfico TCP y SCTP.

## Control de congestión y congestión de red

Por lo general, la congestión de red se manifiesta en forma de desbordamientos de búfer de enrutador, cuando los nodos envían más paquetes de los que la red puede alojar. Varios algoritmos evitan la congestión de tráfico mediante el establecimiento de controles en los sistemas de envío. Estos algoritmos son compatibles con Oracle Solaris y se pueden agregar con facilidad o incorporar directamente al sistema operativo.

En la siguiente tabla, se enumeran y se describen los algoritmos admitidos.

| Algoritmo | Nombre de Oracle Solaris | Descripción                                                                                                                                                       |
|-----------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NewReno   | newreno                  | Algoritmo predeterminado en Oracle Solaris. El mecanismo de control incluye la ventana de congestión del remitente, el arranque lento y la evasión de congestión. |
| HighSpeed | highspeed                | Una de las modificaciones más conocidas y más simples de NewReno para redes de alta velocidad.                                                                    |
| CUBIC     | cubic                    | En la actualidad, el algoritmo predeterminado en Linux 2.6. Cambia la fase de evasión de congestión de un aumento lineal de la ventana a una función cúbica.      |
| Vegas     | vegas                    | Un algoritmo clásico basado en demoras que intenta predecir la congestión sin desencadenar una pérdida real de paquetes.                                          |

En Oracle Solaris, el control de congestión se habilita mediante el establecimiento de las propiedades de TCP relacionadas con el control. Si bien estas propiedades son para TCP, el mecanismo de control habilitado por estas propiedades también se aplica al tráfico SCTP.

- `cong_enabled`: contiene una lista de algoritmos, separados por comas, que, actualmente, se encuentran funcionando en el sistema. Puede agregar o eliminar algoritmos para habilitar solo los que desea usar.
- `cong_default`: el algoritmo que se usa de manera predeterminada cuando las aplicaciones no especifican los algoritmos explícitamente en las opciones del socket. En la actualidad, el valor de la propiedad `cong_default` se aplica tanto para las zonas globales como para las no globales.

Para establecer estas propiedades, use el comando `ipadm set-prop`. Puede usar el modificador `+=` para agregar un algoritmo o el modificador `-=` para eliminar un algoritmo.

## ▼ Cómo implementar el control de congestión de redes TCP y SCTP

### 1 Conviértase en administrador.

Para obtener más información, consulte “[Cómo obtener derechos administrativos](#)” de *Administración de Oracle Solaris: servicios de seguridad*.

### 2 Visualice los valores actuales de las propiedades del control de congestión del protocolo TCP.

```
ipadm show-prop -p cong_enabled,cong_default tcp
```

Si no especifica las propiedades, se muestran todas las propiedades.

El comando muestra tanto los valores actuales como los algoritmos posibles que se pueden asignar a las propiedades.

### 3 Establezca las propiedades del control de congestión del protocolo TCP.

```
ipadm set-prop -p cong-ctrl-property+=algorithm tcp
```

donde

*propiedad\_ctrl\_cong*      Se refiere a la propiedad `cong_enabled` o a la propiedad `cong_default`.

*algoritmo*                Especifica el algoritmo que está estableciendo para la propiedad. Puede especificar cualquier algoritmo que está enumerado en el encabezado del campo POSSIBLE de la salida del comando `ipadm show-prop`.

### 4 (Opcional) Elimine un algoritmo que está habilitado actualmente.

```
ipadm set-prop -p cong-ctrl-property-=algorithm tcp
```

**Nota** – No se siguen reglas de secuencia cuando se agregan o se eliminan algoritmos. Puede eliminar un algoritmo antes de agregar otros algoritmos a una propiedad. Sin embargo, la propiedad `cong_default` siempre debe tener un algoritmo definido.

## 5 (Opcional) Visualice los nuevos valores de las propiedades del control de congestión.

```
ipadm show-prop -p cong_enabled,cong_default tcp
```

### Ejemplo 26-1 Establecimiento de algoritmos para el control de congestión

En este ejemplo, se cambia el algoritmo predeterminado para el protocolo TCP de `newreno` a `cubic`. También elimina `vegas` de la lista de algoritmos permitidos.

```
ipadm show-prop -p cong_default,cong_enabled tcp
```

| PROTO | PROPERTY     | PERM | CURRENT                               | PERSISTENT | DEFAULT | POSSIBLE                          |
|-------|--------------|------|---------------------------------------|------------|---------|-----------------------------------|
| tcp   | cong_default | rw   | newreno                               | --         | newreno | -                                 |
| tcp   | cong_enabled | rw   | newreno,cubic,<br>highspeed,<br>vegas | --         | newreno | newreno,cubic,<br>highspeed,vegas |

```
ipadm set-prop -p cong_enabled==vegas tcp
ipadm set-prop -p cong_default=cubic tcp
```

```
ipadm show-prop -p cong_default,cong_enabled tcp
```

| PROTO | PROPERTY     | PERM | CURRENT                     | PERSISTENT | DEFAULT | POSSIBLE                          |
|-------|--------------|------|-----------------------------|------------|---------|-----------------------------------|
| tcp   | cong_default | rw   | cubic                       | --         | newreno | -                                 |
| tcp   | cong_enabled | rw   | newreno,cubic,<br>highspeed | --         | newreno | newreno,cubic,<br>highspeed,vegas |





## **P A R T E V**

# 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)

---

La calidad de servicio IP (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 411
- “Ofrecimiento de calidad de servicio con IPQoS” en la página 414
- “Mejoramiento de la eficacia de la red con IPQoS” en la página 415
- “Modelo de servicios diferenciados” en la página 417
- “Reenvío del tráfico en una red con IPQoS” en la página 422

## 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:

- Herramienta de línea de comandos `ipqosconf` para configurar la política QoS
- Clasificador que selecciona acciones basadas en filtros que configuran la política 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, Definition of the Differentiated Services Field \(DS Field\) in the IPv4 and IPv6 Headers](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 enlaces 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.

## Ofrecimiento de 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. El resto del tráfico puede recibir prioridad media 24 horas al día.

### Garantía de 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 política de calidad de servicio

Para utilizar la calidad de servicio es necesario definir una *política 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 política 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 política IPQoS se considera un *sistema con IPQoS*.

Normalmente, la política 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 política QoS.

Las tareas para diseñar la política QoS se describen en la sección [“Planificación de la política de calidad de servicio” en la página 431](#).

## Mejoramiento de 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 política 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 política 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 política 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 política QoS. Si necesita información detallada sobre cada módulo, consulte la sección “[Arquitectura IPQoS y el modelo Diffserv](#)” en la página 489.

## 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 clasificador](#)” en la página 489.

## 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 política 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 política QoS” en la página 434](#).

## 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 política QoS.

Si necesita información sobre cómo crear filtros, consulte la sección [“Cómo definir filtros en la política QoS” en la página 437](#).

## 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 política 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 438](#).

## Descripción general de marcadores (`dscpmk` y `dlcosmk`)

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.
- `dlcosmk`: 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.

`dlcosmk` 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 política QoS, consulte [“Cómo planificar el comportamiento de reenvío” en la página 441](#).

## 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

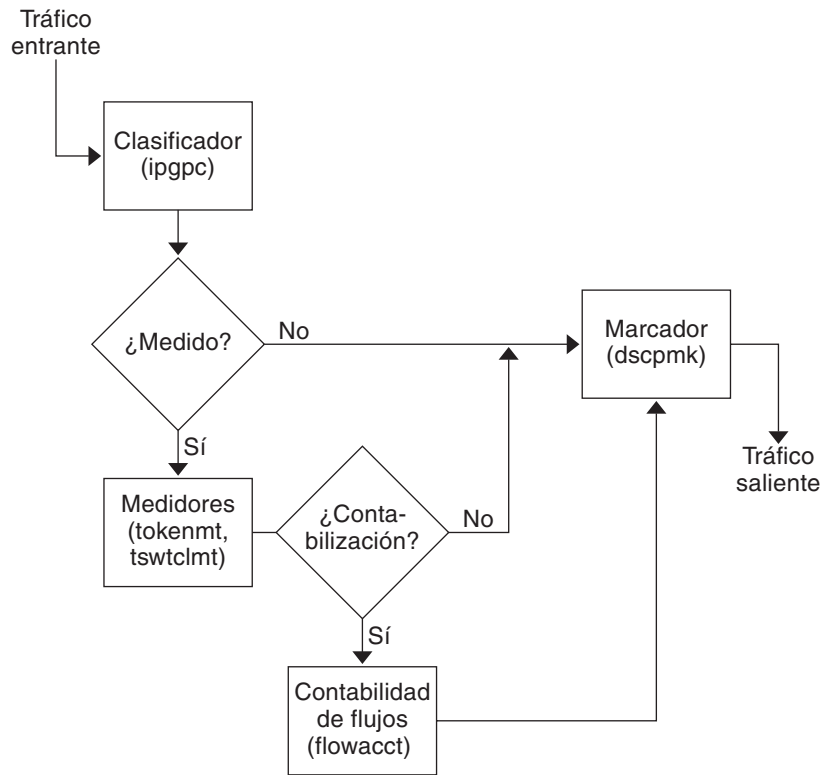
También puede recopilar estadísticas de otros atributos, como se describe en la sección [“Registro de información sobre flujos de tráfico” en la página 484](#), y en las páginas de comando `man flowacct(7ipp)` y `acctadm(1M)`.

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 443](#).

## 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 27-1 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 política 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 política 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 495](#).

---

### 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 495](#).

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 política 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 política 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 política 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

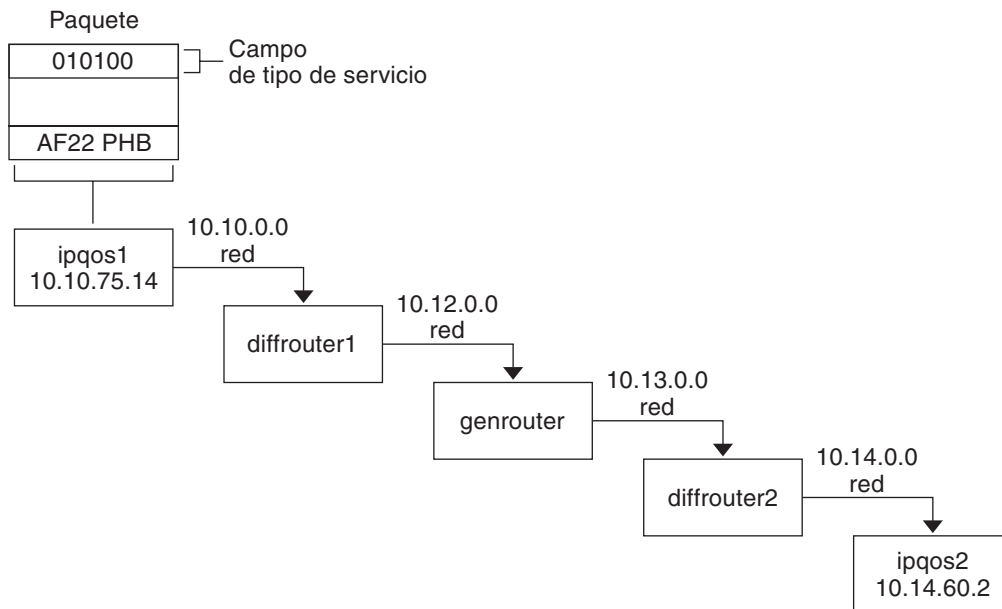
El comportamiento por salto de *reenvío asegurado (AF)* proporciona cuatro clases de reenvío diferentes que se pueden asignar a un paquete. Cada clase de reenvío proporciona tres precedencias de descarte, tal y como se muestra en la [Tabla 32-2](#).

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 política 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 27-2 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 política QoS al flujo de paquetes resultante. Después, ipqos1 clasifica el tráfico `ftp`.

El administrador del sistema creó una clase para todo el tráfico `ftp` saliente que se origina en la red local 10.10.0.0. Al tráfico para la clase `ftp` se le asigna el comportamiento por salto AF22: clase dos, precedencia de descarte media. Se ha asignado una tasa de flujo de tráfico de 2 Mb/s a la clase `ftp`.

3. ipqos - 1 mide el flujo `ftp` para determinar si excede la tasa asignada de 2 Mbit/s.
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 política 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 427
- “Planificación de la distribución de la red Diffserv” en la página 428
- “Planificación de la política de calidad de servicio” en la página 431
- “Planificación de la política QoS (mapa de tareas)” en la página 432
- “Introducción al ejemplo de configuración IPQoS” en la página 444

### 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. | <a href="#">“Planificación de la distribución de la red Diffserv” en la página 428.</a> |

| 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).                     | <a href="#">“Planificación de la política de calidad de servicio” en la página 431.</a>                                |
| 3. Planificar la política QoS para cada sistema IPQoS.                            | Decidir cuáles son las funciones de clases, medición y recopilación de datos necesarias para cada acuerdo SLA.      | <a href="#">“Planificación de la política de calidad de servicio” en la página 431.</a>                                |
| 4. Si procede, planificar la política del enrutador Diffserv.                     | Establecer las políticas de planificación y espera en cola del enrutador Diffserv utilizado con los sistemas IPQoS. | Consulte la documentación del enrutador si necesita información sobre las políticas 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

Por lo general, los clientes ejecutan IPQoS en servidores y consolidaciones de servidores, como los servidores Sun Enterprise™ de Oracle. 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.

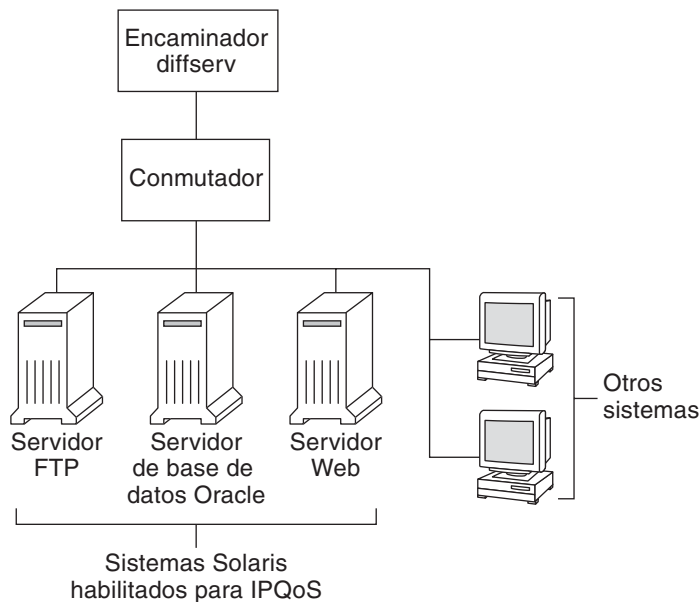
## Distribuciones de red IPQoS

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 28-1 Sistemas IPQoS en un segmento de red

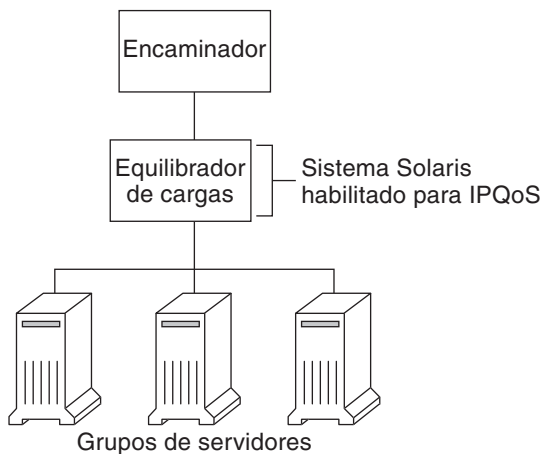


Esta red es sólo un segmento de una intranet empresarial. Activando IPQoS en los servidores de aplicaciones y servidores web, puede controlar la tasa a la que cada sistema IPQoS envía el tráfico saliente. Si configura el enrutador para utilizar Diffserv, puede obtener un mayor grado de control del tráfico entrante y saliente.

El ejemplo de esta guía utiliza una configuración con IPQoS en un único host. Para ver la topología de ejemplo que se utiliza en esta guía, consulte la [Figura 28-4](#).

### IPQoS en una red de conjuntos de servidores

La siguiente figura muestra una red con varios conjuntos de servidores heterogéneos.

**FIGURA 28-2** Red de conjuntos de servidores con IPQoS

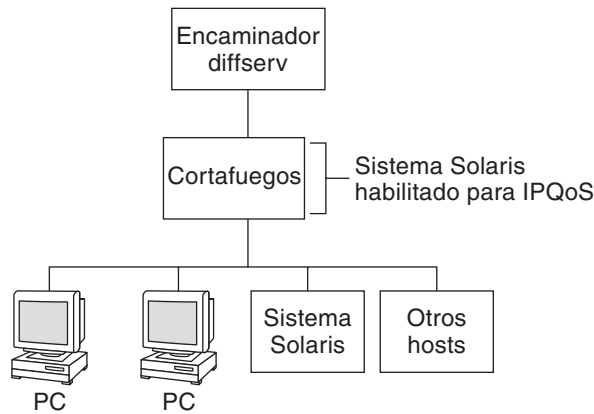
En esta distribución, el enrutador utiliza Diffserv y, por lo tanto, puede poner en cola y tasar el tráfico entrante y saliente. El equilibrador de carga también utiliza Diffserv y los conjuntos de servidores usan IPQoS. El equilibrador de carga permite realizar un filtrado adicional al del enrutador 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 28-3 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 política de seguridad del cortafuegos determina si el tráfico entrante puede entrar o salir de la red interna. La política QoS controla los niveles de servicio para el tráfico entrante que ha pasado el cortafuegos. Según la política QoS, el tráfico saliente también puede marcarse con un comportamiento de reenvío.

## Planificación de la política de calidad de servicio

Al planificar la política 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 política QoS

Recopile información para planificar la política 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 28–1 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 política QoS. En las siguientes secciones se explica cómo obtener información sobre las categorías mostradas en la plantilla.

## Planificación de la política QoS (mapa de tareas)

Este mapa de tareas enumera las tareas principales para planificar una política 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.                                                                       | <a href="#">“Cómo preparar una red para IPQoS” en la página 433</a>           |
| 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. | <a href="#">“Cómo definir las clases de la política QoS” en la página 434</a> |
| 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.                                                         | <a href="#">“Cómo definir filtros en la política QoS” en la página 437</a>    |



| 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.                                                                               | <a href="#">“Cómo planificar el control de flujo” en la página 438</a>               |
| 5. Definir los puntos DSCP o valores de prioridad de usuario que se deben utilizar en la política QoS.  | Planificar un esquema para determinar el comportamiento de reenvío asignado a un flujo de tráfico cuando lo controla el enrutador o nodo.      | <a href="#">“Cómo planificar el comportamiento de reenvío” en la página 441</a>      |
| 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. | <a href="#">“Cómo planificar la recopilación de datos de flujo” en la página 443</a> |

---

**Nota** – En el resto de esta sección se explica cómo planificar la política QoS de un sistema con IPQoS. Para planificar la política 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 política QoS.

### 1 Revise 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 428](#).

### 2 Identifique los hosts de la distribución de red que requieren IPQoS o que pueden ser buenos candidatos para el servicio IPQoS.

### 3 Determine qué sistemas con IPQoS pueden usar la misma política QoS.

Por ejemplo, si piensa activar IPQoS en todos los hosts de la red, identifique los hosts que pueden usar la misma política QoS. Cada sistema con IPQoS debe tener una política 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 política QoS.

### 4 Revise y realice 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 política QoS

El primer paso para definir la política 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 política QoS diferente para cada sistema con IPQoS.

---

**Nota** – Para ver una descripción general de las clases, consulte la sección “[Clases IPQoS](#)” en la [página 417](#).

---

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 433](#).

### 1 Cree una tabla de planificación QoS para organizar la información de política QoS.

Para ver sugerencias, consulte la [Tabla 28–1](#).

### 2 Realice el resto de los pasos para cada política QoS de la red.

### 3 Defina las clases que utilizar en la política 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 de mejor esfuerzo 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 política 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 video y audio.

Definir clases de entrada y clases de salida para estas aplicaciones de alta prioridad. Después, añadir las clases a las políticas QoS del sistema con IPQoS que proporciona las aplicaciones y del enrutador Diffserv.

■ **¿La red tiene flujos de tráfico que deben controlares 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 política QoS del enrutador Diffserv. Después, el enrutador puede poner en cola y planificar los flujos problemáticos de acuerdo con la configuración de la política 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 Enumere las clases definidas en la tabla de planificación QoS creada en el paso 1.**

**5 Asigne 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 política QoS no se utilizan en IPQoS. De hecho, puede asignar la misma prioridad a varias clases, si es apropiado para la política QoS.

**6 Cuando haya terminado de definir las clases, puede definir filtros para cada clase, como se explica en “Cómo definir filtros en la política QoS” en la página 437.**

**Más información** Priorización 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 441](#).

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.

## Definición de 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 418](#).

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 32–1](#).

TABLA 28–2 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 <a href="#">“Cómo definir las clases de la política QoS” en la página 434</a> . |
| 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 28–2 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 política QoS**

**Antes de empezar** Antes de llevar a cabo los siguientes pasos, debe haber completado el procedimiento “[Cómo definir las clases de la política QoS](#)” en la página 434.

- 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 política QoS](#)” en la página 434.**

Considere 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 política 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 28–1](#) para rellenar los filtros de las clases definidas.

**Ejemplo 28–1** Definición de 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<br>daddr 10.100.10.53<br>sport 21<br>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 438.

- Para definir comportamientos de reenvío para flujos que vuelven al flujo de red, consulte [“Cómo planificar el comportamiento de reenvío” en la página 441.](#)
- 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 443.](#)
- Para añadir más clases a la política QoS, consulte la sección [“Cómo definir las clases de la política QoS” en la página 434.](#)
- Para añadir más filtros a la política QoS, consulte la sección [“Cómo definir filtros en la política QoS” en la página 437.](#)

## ▼ 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 418.](#)

En el siguiente procedimiento se asume que ha definido filtros y selectores, como se describe en la sección [“Cómo definir filtros en la política QoS” en la página 437.](#)

- 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 política QoS” en la página 434.](#)**

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 493](#). También puede encontrar información detallada en la página del 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 494](#) y en la página del 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 medidor” en la página 492](#).

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 28-2 Definición de 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/s, o 10000000 bits por segundo. La política 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<br>dport imap<br>direction<br>LOCAL_IN  |                                                                                                                                                                                                                                                  |
| email | 8         | mail_out | saddr10.50.50.5<br>sport imap<br>direction<br>LOCAL_OUT | medidor=tokenmt<br>tasa asignada=5000000<br>ráfaga asignada =5000000<br>tasa máxima =10000000<br>ráfaga máxima=1000000<br>precedencia verde=continuar<br>procesando<br>precedencia amarilla=marcar<br>PHB amarillo<br>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 441.](#)
  - 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 443.](#)
  - Para añadir más clases a la política QoS, consulte la sección [“Cómo definir las clases de la política QoS” en la página 434.](#)
  - Para añadir más filtros a la política QoS, consulte la sección [“Cómo definir filtros en la política QoS” en la página 437.](#)
  - Para definir otro esquema de control de flujo, consulte la sección [“Cómo planificar el control de flujo” en la página 438.](#)
  - 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 452.](#)



## ▼ 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 497](#).

---

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 422](#).

### Antes de empezar

En los siguientes pasos se asume que ha definido clases y filtros para la política 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 496](#).

#### 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 28–3 Política 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 política QoS. Esta política 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<br>tasa asignada=5000000<br>ráfaga asignada=5000000<br>tasa máxima=10000000<br>ráfaga máxima=15000000<br>precedencia verde=continuar procesando<br>precedencia amarilla=marcar PHB amarillo<br>precedencia roja=descartar | verde=AF31<br>amarillo=AF42<br>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 política QoS indica que los paquetes de games\_app deben descartarse. Todos los puntos de código AF se enumeran en la [Tabla 32–2](#).

- 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 443](#).
  - Para añadir más clases a la política QoS, consulte la sección [“Cómo definir las clases de la política QoS” en la página 434](#).
  - Para añadir más filtros a la política QoS, consulte la sección [“Cómo definir filtros en la política QoS” en la página 437](#).
  - Para definir un esquema de control de flujo, consulte la sección [“Cómo planificar el control de flujo” en la página 438](#).
  - 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 441](#).
  - 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 452](#).

## ▼ 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 política 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 política 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 política 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 política QoS, consulte la sección [“Cómo definir las clases de la política QoS” en la página 434](#).
  - Para añadir más filtros a la política QoS, consulte la sección [“Cómo definir filtros en la política QoS” en la página 437](#).
  - Para definir un esquema de control de flujo, consulte la sección [“Cómo planificar el control de flujo” en la página 438](#).

- 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 441](#).
- 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 443](#).
- 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 452](#).

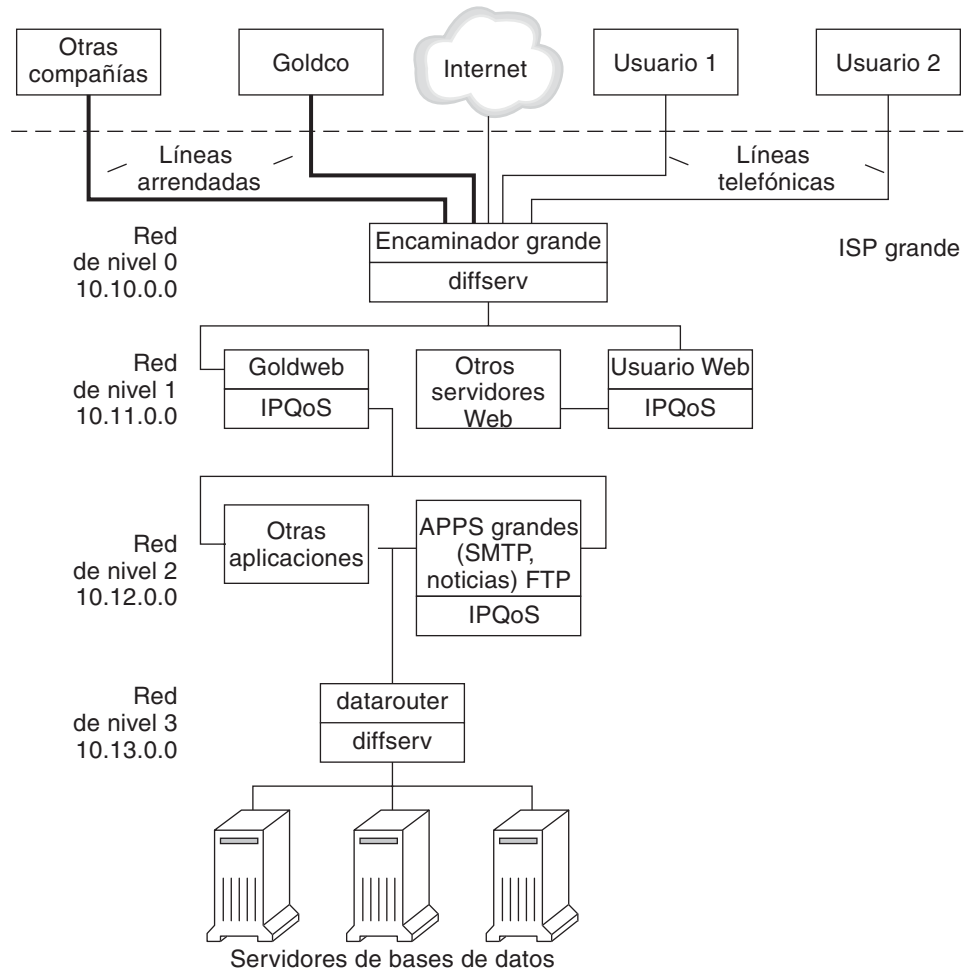
## Introducción al ejemplo de configuración IPQoS

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 28-4 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 política QoS en el archivo de configuración IPQoS (mapa de tareas)” en la página 447
- “Herramientas para crear una política QoS” en la página 449
- “Creación de archivos de configuración IPQoS para servidores web” en la página 450
- “Creación un archivo de configuración IPQoS para un servidor de aplicaciones” en la página 463
- “Suministro de servicios diferenciados en un enrutador” en la página 472

En este capítulo se asume que el usuario ha definido una política QoS completa y que está listo para utilizarla como base para el archivo de configuración IPQoS. Si necesita instrucciones sobre la planificación de políticas QoS, consulte el tema “[Planificación de la política de calidad de servicio](#)” en la página 431.

### Definición de una política QoS en el archivo de configuración IPQoS (mapa de tareas)

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. | Decida qué sistemas de la red local va a utilizar IPQoS. | <a href="#">“Cómo preparar una red para IPQoS” en la página 433</a> |

| Tarea                                                                                                       | Descripción                                                                                                                                                                                | Para obtener instrucciones                                                                                        |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| 2. Planificar la política QoS para sistemas IPQoS de la red.                                                | Identifique flujos de tráfico como diferentes clases de servicio. A continuación, determine qué flujos requieren administración del tráfico.                                               | <a href="#">“Planificación de la política de calidad de servicio” en la página 431</a>                            |
| 3. Crear el archivo de configuración IPQoS y definir la primera acción.                                     | Cree el archivo IPQoS, invoque el clasificador IP y defina una clase para procesar.                                                                                                        | <a href="#">“Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico” en la página 452</a>   |
| 4. Crear filtros para un clase.                                                                             | Añada los filtros que determinan qué tráfico se selecciona y se organiza en una clase.                                                                                                     | <a href="#">“Cómo definir filtros en el archivo de configuración IPQoS” en la página 454</a>                      |
| 5. Añadir más clases y filtros al archivo de configuración IPQoS.                                           | Cree más clases y filtros para que los procese el clasificador IP.                                                                                                                         | <a href="#">“Cómo crear un archivo de configuración IPQoS para un servidor web “best-effort” en la página 460</a> |
| 6. Añadir una instrucción <code>action</code> con parámetros para configurar los módulos de medición.       | Si la política QoS solicita control de flujo, asigne tasas de control de flujo y niveles de cumplimiento al medidor.                                                                       | <a href="#">“Cómo configurar el control de flujo en el archivo de configuración IPQoS” en la página 469</a>       |
| 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.                                                                  | <a href="#">“Cómo definir el reenvío de tráfico en el archivo de configuración IPQoS” en la página 456</a>        |
| 8. Añadir una instrucción <code>action</code> con parámetros para configurar el módulo de control de flujo. | Si la política QoS solicita recopilación de estadísticas sobre flujos de tráfico, defina cómo deben recopilarse las estadísticas de control.                                               | <a href="#">“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 459</a>    |
| 9. Aplicar el archivo de configuración IPQoS.                                                               | Añada el contenido de un archivo de configuración IPQoS especificado a los módulos de núcleo apropiados.                                                                                   | <a href="#">“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 476</a>             |
| 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. | <a href="#">“Cómo configurar un enrutador en una red con IPQoS” en la página 473</a>                              |



# Herramientas para crear una política QoS

La política 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 `ipqosconf`, la herramienta de configuración IPQoS. Al solicitar a `ipqosconf` que aplique la política definida en el archivo de configuración, la política se escribe en el núcleo del sistema IPQoS. Si necesita información detallada sobre el comando `ipqosconf`, consulte la página del comando `man ipqosconf(1M)`. Si necesita instrucciones sobre el uso de `ipqosconf`, consulte la sección “[Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS](#)” en la página 476.

## Archivo de configuración IPQoS básico

Un archivo de configuración IPQoS consiste en un árbol de instrucciones `action` que implementan la política QoS definida en la sección “[Planificación de la política de calidad de servicio](#)” en la página 431. El archivo de configuración IPQoS configura los módulos IPQoS. Cada instrucción `action` contiene un conjunto de *clases*, *filtros* o *parámetros* que procesará el módulo al que llame la instrucción `action`.

Para ver la sintaxis completa del archivo de configuración IPQoS, consulte el [Ejemplo 32-3](#) y la página del comando `man ipqosconf(1M)`.

## Configuración de 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 compañía BigISP, que se presentó en la [Figura 28-4](#).

- 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.

# Creación de 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 28–4](#).

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 29–1** 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
 }
}
```

**EJEMPLO 29-1** Archivo de configuración IPQoS de ejemplo para un servidor web de nivel alto  
(Continuación)

```

action {
 module dscpmk
 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 29-2** 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
 }
}

```

**EJEMPLO 29-2** Configuración de muestra para un servidor web "best-effort" (Continuación)

```

 dscp_map{0-63:12}
 next_action continue
 }
}

```

## ▼ 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 29-1](#).

---

**Nota** – Al crear el archivo de configuración IPQoS, asegúrese de comenzar y finalizar cada instrucción `action` y cláusula con llaves (`{ }`). Para ver un ejemplo del uso de llaves, consulte el [Ejemplo 29-1](#).

---

### 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 `action`, que configura el clasificador IP genérico `ipgpc`.

Esta primera acción inicia el árbol de instrucciones `action` que compone el archivo de configuración IPQoS. Por ejemplo, el archivo `/var/ipqos/Goldweb.qos` comienza con la instrucción `action` 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 `action`.

`module ipgpc`      Configura el clasificador `ipgpc` como la primera acción del archivo de configuración.

`name ipgpc.classify`      Define el nombre de la instrucción `action` 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 503](#) y la página del 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 505](#) y la página del 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 <code>action markAF11</code> . La instrucción <code>action 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 504](#) y la página del comando `man ipqosconf(1M)`.

### 5 Defina una clase que identifique una aplicación que deba tener reenvío de máxima prioridad.

```
class {
 name video
```

|                                                                        |                                                                                                                                                                                                    |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>        next_action marKEF         enable_stats FALSE     }</pre> |                                                                                                                                                                                                    |
| <code>name video</code>                                                | Crea la clase video para identificar el tráfico saliente de video streaming del servidor Goldweb.                                                                                                  |
| <code>next_action marKEF</code>                                        | Indica al módulo ipgpc que debe pasar los paquetes de la clase video a la instrucción marKEF después de que ipgpc haya terminado el procesamiento. La instrucción marKEF llama al marcador dscpmk. |
| <code>enable_stats FALSE</code>                                        | Activa la recopilación de estadísticas de la clase video. Aunque, debido a que el valor de enable_stats es FALSE, 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 454](#).
  - 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 452](#).

## ▼ 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 452](#).

---

**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 29–1](#).

---

### 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 505](#).

## 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 456](#).
  - 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 469](#).
  - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 476](#).

- Para definir filtros adicionales, consulte la sección [“Cómo definir filtros en el archivo de configuración IPQoS”](#) en la página 454.
- 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 465.

## ▼ 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 29-1](#).

---

**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 497.

---

### 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 `action 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 10 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 32-2](#).

### 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 política QoS. Si necesita más información sobre PHB de reenvío acelerado, consulte la sección [“Reenvío acelerado \(EF\) PHB” en la página 496](#).

- 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 473](#).

- 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 459](#).
  - 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 456](#).
  - 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 469](#).
  - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 476](#).
  - Para definir filtros adicionales, consulte la sección [“Cómo definir filtros en el archivo de configuración IPQoS” en la página 454](#).
  - 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 465](#).

## ▼ 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 452](#). 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 29-1](#).

### 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 473.
  - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS”](#) en la página 476.
  - 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 465.

## ▼ **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 29–2](#).

- 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 452](#).

### 3 Defina una clase que identifique el tráfico vinculado con el servidor web "best-effort".

```

class {
 name userweb
 next_action markAF12
 enable_stats FALSE
}

```

`name userweb` Crea una clase llamada `userweb` para reenviar el tráfico web de usuarios.

`next_action markAF1` Indica al módulo `ipgpc` que debe transferir los paquetes de la clase `userweb` a la instrucción `action markAF12` cuando `ipgpc` haya completado el procesamiento. La instrucción `action markAF12` invoca al marcador `dscpmk`.

`enable_stats FALSE` Activa la recopilación de estadísticas para la clase `userweb`. Aunque, debido a que el valor de `enable_stats` es `FALSE`, 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 452](#).

### 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
}

```

`name webout` Asigna el nombre `webout` al filtro.

`sport 80` Selecciona el tráfico con origen en el puerto 80, el puerto de tráfico HTTP (web).

`direction LOCAL_OUT` Selecciona el tráfico saliente del sistema local.

`class userweb` Identifica la clase a la que pertenece el filtro, en este caso, la clase `userweb`.

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 454.](#)

## 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 465.](#)
  - Para configurar comportamientos por salto en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS” en la página 473.](#)

- Para activar el archivo de configuración IPQoS, consulte la sección “[Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS](#)” en la página 476.

## Creación 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 utiliza como ejemplo el servidor BigAPPS de la [Figura 28-4](#).

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 29-3 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 29-3** 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. Empiece 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 452.](#)

- 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 452](#).

### 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 454](#).
  - 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 467](#).
  - 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 469](#).
  - 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 459](#).

## ▼ 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 29–3](#).

**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 32-2](#).

## 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 452](#).
  - 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 469](#).
  - 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 459](#).
  - Para configurar comportamientos de reenvío en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS” en la página 473](#).
  - Para activar el archivo de configuración IPQoS, consulte la sección [“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 476](#).

## ▼ 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.

En el siguiente procedimiento, se continúa con la creación del archivo de configuración IPQoS para el servidor de aplicaciones del [Ejemplo 29-3](#). 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 493](#).

**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 medidor](#)” en la [página 492](#).

## 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 32-2](#).

## 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 32–2](#).

## 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 núcleo IPQoS”](#) en la página 476.
  - 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 452.
  - 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 459.
  - Para configurar comportamientos de reenvío en un enrutador, consulte la sección [“Cómo configurar un enrutador en una red con IPQoS”](#) en la página 473.

# 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 428. 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 28–4](#).

**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 políticas 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 475
- “Aplicación de una configuración IPQoS” en la página 476
- “Activación del registro `sys log` para mensajes IPQoS” en la página 477
- “Resolución de problemas con mensajes de error IPQoS” en la página 478

### 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 política QoS en el archivo de configuración IPQoS (mapa de tareas)” en la página 447.

La tabla siguiente enumera y describe esas tareas y contiene vínculos a las secciones que describen cómo realizarlas.

| Tarea                                                                                                                                        | Descripción                                                                                             | Para obtener instrucciones                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| 1. Configurar IPQoS en un sistema.                                                                                                           | Utilice el comando <code>ipqosconf</code> para activar el archivo de configuración IPQoS en un sistema. | <a href="#">“Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS” en la página 476</a>            |
| 2. Hacer 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.                  | <a href="#">“Cómo garantizar que la configuración IPQoS se aplica cada vez que se reinicia” en la página 477</a> |
| 3. Activar el registro <code>sys log</code> para IPQoS.                                                                                      | Añada una entrada para activar el registro <code>sys log</code> de mensajes IPQoS.                      | <a href="#">“Cómo activar el registro de mensajes IPQoS durante el inicio” en la página 477</a>                  |

| Tarea                                             | Descripción                                                 | Para obtener instrucciones                                      |
|---------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------|
| 4. Solucionar cualquier problema IPQoS que surja. | Solucione los problemas IPQoS utilizando mensajes de error. | Consulte los mensajes de error de la <a href="#">Tabla 30–1</a> |

# 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 núcleo IPQoS

Se utiliza el comando `ipqosconf` para leer el archivo de configuración IPQoS y para configurar los módulos IPQoS del núcleo UNIX. En el siguiente procedimiento se utiliza como ejemplo el archivo `/var/ipqos/Goldweb.qos`, creado en la sección “[Creación de archivos de configuración IPQoS para servidores web](#)” en la [página 450](#). Si necesita información detallada, consulte la página del comando `man ipqosconf(1M)`.

### 1 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 núcleo de Oracle Solaris. En este ejemplo, el contenido de `/var/ipqos/Goldweb.qos` se aplica al núcleo 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.

### 2 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 486](#).
  - Para registrar los mensajes `ipqosconf`, consulte la sección “[Activación del registro `syslog` para mensajes IPQoS](#)” en la [página 477](#).
  - 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 477](#).

## ▼ 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 Compruebe que existe una configuración IPQoS en los módulos de núcleo.

```
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 núcleo IPQoS” en la página 476](#).

- 2 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 Abra el archivo `/etc/syslog.conf`.

- 2 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`.

- 3 Reinicie el sistema para aplicar los mensajes.

Ejemplo 30–1 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 30–1](#).

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 30–1 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 ipgpc 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 452. |

TABLA 30-1 Mensajes de error IPQoS (Continuación)

| Mensaje de error                                                                    | Descripción                                                                                                                                         | Solución                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 a <code>fmt_version 1.0</code> , que se requiere a partir de la versión Solaris 9 9/02 de IPQoS.                                                                                                                |
| No ipgpc action defined.                                                            | No ha definido una acción para el clasificador ipgpc en el archivo de configuración, como requiere IPQoS.                                           | Defina una acción para ipgpc, como se muestra en la sección “ <a href="#">Cómo crear el archivo de configuración IPQoS y definir las clases de tráfico</a> ” en la página 452.                                                               |
| Can't commit a null configuration                                                   | Cuando ejecutó <code>ipqosconf -c</code> 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 “ <a href="#">Cómo aplicar una nueva configuración a los módulos de núcleo IPQoS</a> ” en la página 476. |
| 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.                                                                                                                                                                          |
| Invalid module name line <i>número de línea</i>                                     | En el archivo de configuración, el nombre de módulo que ha especificado en una instrucción action no es válido.                                     | Compruebe que el nombre de módulo esté bien escrito. Para ver una lista de módulos IPQoS, consulte la <a href="#">Tabla 32-5</a> .                                                                                                           |
| 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 <code>ipgpc.classify</code> requerido.                          | Cambie el nombre de la acción <code>ipgpc.classify</code> .                                                                                                                                                                                  |
| 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</i> in action <i>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.                                                                                                                                                                      |

TABLA 30-1 Mensajes de error IPQoS (Continuación)

| Mensaje de error                                                                    | Descripción                                                                                                                        | Solución                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Undefined action in class<br><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<br>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 <a href="#">“Arquitectura IPQoS y el modelo Diffserv” en la página 489</a> . También puede consultar la página del comando <code>man ipqosconf(1M)</code> .                                                      |
| Mandatory parameter missing<br>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 <a href="#">“Arquitectura IPQoS y el modelo Diffserv” en la página 489</a> . También puede consultar la página del comando <code>man ipqosconf(1M)</code> .                                                      |
| Max number of classes<br>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> .                                                                            |
| Max number of filters<br>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> <i>número de filtros</i> .                                                                         |
| Invalid/missing parameters<br>for filter <i>nombre de filtro</i> in<br>action ipgpc | En el archivo de configuración, el filtro <i>nombre de filtro</i> tiene parámetros no válidos o no especificados.                  | Consulte la página del comando <code>man ipqosconf(1M)</code> para ver una lista de parámetros válidos.                                                                                                                                                                                                              |
| Name not allowed to start<br>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<br>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<br><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 <code>action</code> con la matriz no válida, consulte la sección <a href="#">“Arquitectura IPQoS y el modelo Diffserv” en la página 489</a> . También puede consultar la página del comando <code>man ipqosconf(1M)</code> . |



TABLA 30-1 Mensajes de error IPQoS (Continuación)

| Mensaje de error                                                                                | Descripción                                                                                                                                                               | Solución                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <code>action</code> , consulte la descripción del módulo en la sección “ <a href="#">Arquitectura IPQoS y el modelo Diffserv</a> ” en la página 489. También puede consultar la página del 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 <code>action</code> con el número de línea no reconocido, consulte la sección “ <a href="#">Arquitectura IPQoS y el modelo Diffserv</a> ” en la página 489. También puede consultar la página del 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 <code>action</code> con la lista de valores mal formada, consulte la descripción del módulo en la sección “ <a href="#">Arquitectura IPQoS y el modelo Diffserv</a> ” en la página 489. También puede consultar la página del comando <code>man ipqosconf(1M)</code> .                                     |
| 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 | <code>ipqosconf</code> 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 <code>ip_version</code> . | Cambie las dos entradas en conflicto para que sean compatibles.                                                                                                                                                                                                                                                                                                                 |

TABLA 30-1 Mensajes de error IPQoS (Continuación)

| Mensaje de error                                                                                                     | Descripción                                                                                                                 | Solución                                                               |
|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 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 483
- “Registro de información sobre flujos de tráfico” en la página 484
- “Recopilación de estadísticas” en la página 486

### 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. Crear 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> . | <a href="#">“Cómo crear un archivo para datos de control de flujo” en la página 484</a>                        |
| 2. Definir 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> .                                            | <a href="#">“Cómo activar el control para una clase en el archivo de configuración IPQoS” en la página 459</a> |

# 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 32–4](#).

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 `action` para `flowacct` en el archivo de configuración IPQoS, consulte “[Cómo configurar el control de flujo en el archivo de configuración IPQoS](#)” en la página 469.
- Para aprender cómo funciona `flowacct`, consulte “[Módulo clasificador](#)” en la página 489.
- Si necesita información técnica, consulte la página del 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 32–4](#). Si necesita información detallada sobre `acctadm`, consulte la página del comando `man acctadm(1M)`.

### 1 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 29–1](#).

```
/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.                          |

`/var/ipqos/goldweb/account.info`      Especifica el nombre de ruta completo del archivo que contendrá los registros de flujo de `flowacct`.

`flow`      Indica a `acctadm` que debe activar el control de flujo.

**2 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, se deben utilizar con la función Oracle Solaris Resource Manager. En la siguiente tabla se explican las entras específicas de IPQoS.

| Entrada                                                     | Descripción                                                                     |
|-------------------------------------------------------------|---------------------------------------------------------------------------------|
| Flow accounting: active                                     | Indica que el control de flujo está activado.                                   |
| Flow accounting file:<br>/var/ipqos/goldweb/account.info    | Da el nombre del archivo de control de flujo actual.                            |
| Tracked flow resources: basic                               | Indica que sólo se supervisan los atributos de flujo básicos.                   |
| Untracked flow resources:<br>dsfield,ctime,lseen,projid,uid | Enumera los atributos <code>flowacct</code> que no se supervisan en el archivo. |

**3 (Optativo) Añada los atributos ampliados al archivo de control.**

```
acctadm -e extended -f /var/ipqos/goldweb/account.info flow
```

**4 (Optativo) Vuelva 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.

**5 Ve el contenido de un archivo de control de flujo.**

Para obtener instrucciones para ver el contenido de un archivo de control de flujo, consulte [“Interfaz Perl para libexacct” de Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#).

- Véase también**
- Para obtener información detallada sobre la función de control ampliada, consulte el [Capítulo 4, “Contabilidad ampliada \(descripción general\)” de \*Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos\*](#).
  - 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 459](#).
  - Para imprimir los datos en el archivo creado con el comando `acctadm`, consulte [“Interfaz Perl para libexacct” de \*Administración de Oracle Solaris: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos\*](#).

## 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 32–5](#). Por ejemplo, para ver estadísticas generadas por el marcador `ds cpmk`, utilice el siguiente comando de `kstat`:

```
/bin/kstat -m ds cpmk
```

Si necesita información técnica, consulte la página del comando `man kstat(1M)`.

### EJEMPLO 31–1 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
```

`class: flacct` Da el nombre de la clase a la que pertenecen los flujos de tráfico, en este caso `flacct`.

`bytes_in_tbl` 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 `bytes_in_tbl` es 0.

**EJEMPLO 31-1** Estadísticas kstat de IPQoS (Continuación)

|                           |                                                                                                                                                                                                                                                                                                                |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>crtime</code>       | La última vez que se creó esta salida de <code>kstat</code> .                                                                                                                                                                                                                                                  |
| <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 489
- “Archivo de configuración IPQoS” en la página 502
- “Herramienta de configuración `ipqosconf`” en la página 506

Para obtener una descripción general, consulte el [Capítulo 27, “Introducción a IPQoS \(descripción general\)”](#). Si necesita información sobre la planificación, consulte el [Capítulo 28, “Planificación para una red con IPQoS \(tareas\)”](#). Para ver los procedimientos para configurar IPQoS, consulte el [Capítulo 29, “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>). 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 clasificador

En el modelo Diffserv, el módulo *clasificador* 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 del 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 política 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 417](#). Si necesita información sobre cómo invocar al clasificador en el archivo de configuración IPQoS, consulte [“Archivo de configuración IPQoS” en la página 502](#).

### 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 32-1 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 32-1 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 medidor

El *medidor* controla la tasa de transmisión de flujos por paquete. Después, determina si el paquete cumple los parámetros configurados. El módulo medidor 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.

El medidor 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 del 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 un ejemplo de `tokenmt` de tasa única con dos resultados, consulte el [Ejemplo 29-3](#).

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 `action` que configura `tokenmt` para que reconozca colores.

**EJEMPLO 32-1** 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}
 }
}
```

**EJEMPLO 32-1** Acción tokenmt de reconocimiento de color para el archivo de configuración IPQoS  
(Continuación)

```
}
```

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 del 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 `dscpmk`, consulte la página del comando `man dscpmk(7ipp)`. Si necesita información técnica sobre `dlcosmk`, consulte la página del comando `man dlcosmk(7ipp)`.

### Utilización del marcador `dscpmk` 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 422](#).

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 422](#).

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 32-2 Puntos de código de reenvío asegurado

|                                                       | Clase 1               | Clase 2               | Clase 3               | Clase 4               |
|-------------------------------------------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| <b>Precedencia con baja probabilidad de descarte</b>  | AF11 =<br>10 (001010) | AF21 =<br>18 (010010) | AF31 =<br>26 (011010) | AF41 =<br>34 (100010) |
| <b>Precedencia con probabilidad de descarte media</b> | AF12 =<br>12 (001100) | AF22 =<br>20 (010100) | AF32 =<br>28 (011100) | AF42 =<br>36 (100100) |
| <b>Precedencia con alta probabilidad de descarte</b>  | AF13 =<br>14 (001110) | AF23 =<br>22 (010110) | AF33 =<br>30 (011110) | AF43 =<br>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.

## Suministro de 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 *action* 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 `dscpmk`.

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 32-2](#) a notación decimal para usarlos con `dscp_map`.

## Uso del marcador `dlcosmk` con dispositivos VLAN

El módulo de marcador `dlcosmk` marca un comportamiento de reenvío en el encabezado MAC de un datagrama. `dlcosmk` sólo se puede usar en un sistema IPQoS con una interfaz VLAN.

`dlcosmk` 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 `dlcosmk` definiendo la clase de marcas de servicio de la siguiente tabla.

**TABLA 32-3** Valores de prioridad de usuario 801.D

| Clase de servicio | Definición    |
|-------------------|---------------|
| 0                 | Mejor posible |
| 1                 | Segundo plano |

TABLA 32-3    Valores de prioridad de usuario 801.D    (Continuación)

| Clase de servicio | Definición                        |
|-------------------|-----------------------------------|
| 2                 | Momentos libres                   |
| 3                 | Excelente                         |
| 4                 | Carga controlada                  |
| 5                 | Video, latencia de menos de 100ms |
| 6                 | Video, latencia de menos de 10ms  |
| 7                 | Control de red                    |

Si necesita más información sobre `dlcosmk`, consulte la página del 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 32-2    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
}
```

### EJEMPLO 32-2 Archivo de configuración IPQoS para un sistema con un dispositivo VLAN (Continuación)

```
}
}
```

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 posición de `flowacct` en el modelo Diffserv, consulte la [Figura 27-1](#). Para ver información técnica detallada sobre `flowacct`, consulte la página del comando `man flowacct(7ipp)`.

Para habilitar el control de flujo, debe emplear la utilidad de control `exacct` de Oracle Solaris y el comando `acctadm`, además del comando `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 483](#).

## 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 469](#).

**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 32-4 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 |

TABLA 32-4 Atributos de un registro flowacct (Continuación)

| Nombre de atributo          | Contenido de atributo                                                                                                                                | Tipo          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| dest-addr-tipo de dirección | 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        |
| src-port                    | Puerto de origen del que proviene el flujo.                                                                                                          | Básico        |
| dest-port                   | Número de puerto de destino al que está vinculado el flujo.                                                                                          | Básico        |
| protocol                    | Número de protocolo del flujo.                                                                                                                       | Básico        |
| total-packets               | Número de paquetes del flujo.                                                                                                                        | Básico        |
| 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 del 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
```

|                                   |                                                                                                                                                                                                                                              |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>acctadm -e</code>           | Invoca a <code>acctadm</code> con la opción <code>-e</code> . "-e" indica que a continuación hay una lista de recursos.                                                                                                                      |
| <i>tipo de archivo</i>            | Especifica los atributos que se deben recopilar. <i>tipo de archivo</i> debe reemplazarse por <code>basic</code> o <code>extended</code> . Para ver una lista de atributos de cada tipo de archivo, consulte la <a href="#">Tabla 32-4</a> . |
| <code>-f nombre de archivo</code> | Crea el archivo <i>nombre de archivo</i> que contendrá los registros de flujo.                                                                                                                                                               |
| <code>flow</code>                 | Indica que <code>acctadm</code> debe ejecutarse con IPQoS.                                                                                                                                                                                   |

## Archivo de configuración IPQoS

Esta sección contiene información detallada sobre las secciones del archivo de configuración IPQoS. La política 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 29](#), “Creación del archivo de configuración IPQoS (tareas)”.

La sintaxis del archivo de configuración IPQoS se muestra en el [Ejemplo 32-3](#). 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 32-3 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 | ""
}
```

**EJEMPLO 32-3** Sintaxis del archivo de configuración IPQoS (Continuación)

```

 }
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 | ""
}
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 489](#).

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

```

|                                                                                                                 |                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <code>module module-name</code><br><code>params-clause   ""</code><br><code>cf-clauses</code><br><code>}</code> |                                                                                                                          |
| <code>name nombre de acción</code>                                                                              | Asigna un nombre a la acción.                                                                                            |
| <code>module nombre de módulo</code>                                                                            | Identifica el módulo IPQoS que se debe invocar, que debe ser uno de los módulos de la <a href="#">Tabla 32–5</a> .       |
| <code>cláusula params</code>                                                                                    | Pueden ser parámetros que debe procesar el clasificador, como estadísticas globales, o la siguiente acción que procesar. |
| <code>cláusulas cf</code>                                                                                       | Conjunto de cero o más cláusulas <code>class</code> o <code>filter</code> .                                              |

## 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 32–5 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 503](#).

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 32–1](#).

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 `action`. 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 núcleo UNIX. `ipqosconf` realiza las siguientes acciones:

- Aplica el archivo de configuración a los módulos de núcleo IPQoS (`ipqosconf -a nombre de archivo`)
- Indica el archivo de configuración IPQoS actual del núcleo (`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 núcleo IPQoS actuales (`ipqosconf -f`)

Si necesita información técnica, consulte la página del comando `man ipqosconf(1M)`.

# Glosario

---

|                                                      |                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>3DES</b>                                          | Consulte <a href="#">Triple-DES</a> .                                                                                                                                                                                                                                                                                                         |
| <b>AES</b>                                           | Advanced Encryption Standard. Una técnica de cifrado de datos en bloques de 128 bits simétricos. En octubre de 2000, el gobierno de los Estados Unidos adoptó la variante Rijndael del algoritmo como estándar de cifrado. AES sustituye al cifrado <a href="#">DES</a> como estándar gubernamental.                                          |
| <b>algoritmo Diffie-Hellman</b>                      | 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. |
| <b>anuncio de enrutador</b>                          | 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.                                                                                                                                                        |
| <b>anuncio de vecinos</b>                            | 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.                                                                                                                                                                          |
| <b>ataque smurf</b>                                  | Uso de paquetes de solicitud de ICMP echo dirigidos a una <a href="#">dirección de difusión</a> IP o a varias direcciones de difusión desde ubicaciones remotas para crear interrupciones o congestiones graves de la red.                                                                                                                    |
| <b>autoconfiguración</b>                             | Proceso mediante el cual un host configura automáticamente su dirección IPv6 a partir del prefijo del sitio y la dirección MAC local.                                                                                                                                                                                                         |
| <b>autoconfiguración sin estado</b>                  | 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.                                                                                                                                                                                  |
| <b>autoridad de certificación</b>                    | 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.                                                       |
| <b>base de datos de políticas de seguridad (SPD)</b> | 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.                                                                                                                               |
| <b>Blowfish</b>                                      | 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.                                                                                                     |
| <b>CA</b>                                            | Consulte <a href="#">autoridad de certificación</a> .                                                                                                                                                                                                                                                                                         |

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>capa de vínculo</b>                        | Capa inmediatamente inferior a <a href="#">IPv4/IPv6</a> .                                                                                                                                                                                                                                                                                                                                        |
| <b>carga de seguridad encapsuladora (ESP)</b> | 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).                                                                                                                                                                                                                         |
| <b>carga útil</b>                             | 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.                                                                                                                                                                                                                                        |
| <b>cifrado de claves asimétricas</b>          | 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. El <a href="#">algoritmo Diffie-Hellman</a> es un ejemplo de protocolo de claves asimétricas. Se contrapone a <a href="#">criptografía de clave simétrica</a> . |
| <b>clase</b>                                  | En IPQoS, grupo de flujos de datos de red que comparten características similares. Las clases se definen en el archivo de configuración de IPQoS.                                                                                                                                                                                                                                                 |
| <b>contabilidad de flujos</b>                 | 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.                                                                                                                                                          |
| <b>cortafuegos</b>                            | 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).                                                                                          |
| <b>criptografía de clave simétrica</b>        | 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. <a href="#">DES</a> constituye un ejemplo de sistema de claves simétricas.                                                         |
| <b>criptografía por clave pública</b>         | 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.                                                                                                                                                                                                      |
| <b>datagrama</b>                              | Consulte <a href="#">datagrama IP</a> .                                                                                                                                                                                                                                                                                                                                                           |
| <b>datagrama IP</b>                           | 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.                                                                                        |
| <b>DES</b>                                    | Siglas en inglés de Data Encryption Standard, estándar de cifrado de datos. Método de cifrado de clave simétrica que se desarrolló en 1975 y que ANSI estandarizó en 1981 como ANSI X.3.92. DES utiliza una clave de 56 bits.                                                                                                                                                                     |
| <b>descubrimiento de enrutadores</b>          | Proceso de los hosts que buscan enrutadores residentes en un vínculo conectado.                                                                                                                                                                                                                                                                                                                   |
| <b>descubrimiento de vecinos</b>              | Mecanismo de IP que permite a los host encontrar otros host que residen en un vínculo conectado.                                                                                                                                                                                                                                                                                                  |
| <b>detección de reparaciones</b>              | 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.                                                                                                                                                                                                                      |

|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dirección de difusión</b>                                     | 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.                                                                                                                                             |
| <b>dirección de difusión por proximidad</b>                      | 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 enrutamiento.                                                                     |
| <b>dirección de enrutamiento entre dominios sin clase (CIDR)</b> | 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.                                                                                                                                       |
| <b>dirección de multidifusión</b>                                | 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.                                                                                                                               |
| <b>dirección de unidifusión</b>                                  | 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.                                                                                                                                                                                                                                  |
| <b>dirección de uso local</b>                                    | Dirección de unidifusión que sólo tiene un ámbito de enrutamiento local (dentro de una subred o una red de suscriptores). Esta dirección puede tener también un ámbito de exclusividad local o global.                                                                                                                                                                                                       |
| <b>dirección de uso local de sitio</b>                           | Designación que se usa para dirección en un solo sitio.                                                                                                                                                                                                                                                                                                                                                      |
| <b>dirección local de vínculo</b>                                | 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.                                                                                                                                                         |
| <b>dirección privada</b>                                         | Dirección IP que no se puede enrutar por Internet. Las redes internas utilizan las direcciones privadas en los host que no necesitan conexión con Internet. Las direcciones están definidas en <a href="http://www.ietf.org/rfc/rfc1918.txt?number=1918">Address Allocation for Private Internets (http://www.ietf.org/rfc/rfc1918.txt?number=1918)</a> y con frecuencia se las denomina direcciones “1918”. |
| <b>dispositivo LAN virtual (VLAN)</b>                            | Interfaces de red que proporcionan reenvío de tráfico en el nivel de Ethernet (vínculo de datos) del protocolo de pila IP.                                                                                                                                                                                                                                                                                   |
| <b>dominio de interpretación</b>                                 | 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.                                                                                    |
| <b>DSA</b>                                                       | 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 los Estados Unidos, llega hasta los 1024 bits. DSA se basa en el algoritmo <a href="#">SHA-1</a> para las entradas.                                                                                      |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>encabezado de autenticación</b>      | Encabezado de extensión que proporciona autenticación e integridad, sin confidencialidad, a datagramas IP.                                                                                                                                                                                                                                                                                                                    |
| <b>encabezado de paquete</b>            | Consulte <a href="#">encabezado IP</a> .                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>encabezado IP</b>                    | 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.                                                                                                                                                                                                                     |
| <b>encapsulado</b>                      | Proceso de colocación de un encabezado y carga útil en el primer paquete, que posteriormente se coloca en la carga útil del segundo paquete.                                                                                                                                                                                                                                                                                  |
| <b>encapsulado mínimo</b>               | 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.                                                                                                                                                                                                                             |
| <b>enrutador</b>                        | Sistema que en general tiene más de una interfaz, ejecuta protocolos de enrutamiento 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.                                                                                                                                                                                               |
| <b>expansión de carga</b>               | 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. |
| <b>filtro</b>                           | 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 <a href="#">filtro de paquetes</a> .                                                                                                                  |
| <b>filtro de paquetes</b>               | Función de cortafuegos que se puede configurar para permitir o denegar el paso de determinados paquetes a través de un cortafuegos.                                                                                                                                                                                                                                                                                           |
| <b>filtro de paquetes con estado</b>    | Un <a href="#">filtro de paquetes</a> 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 <a href="#">cortafuegos</a> . Al efectuar el seguimiento y relacionar solicitudes y respuestas, un filtro de paquetes con estado puede detectar respuestas que no coincidan con una consulta.                           |
| <b>filtro de paquetes dinámico</b>      | Consulte <a href="#">filtro de paquetes con estado</a> .                                                                                                                                                                                                                                                                                                                                                                      |
| <b>firma digital</b>                    | Código digital que se vincula con un mensaje transmitido electrónicamente y que identifica al remitente de forma exclusiva.                                                                                                                                                                                                                                                                                                   |
| <b>gestión de claves</b>                | El modo en que puede gestionar asociaciones de seguridad (SA).                                                                                                                                                                                                                                                                                                                                                                |
| <b>grupo de difusión por proximidad</b> | 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.                                                                                                                    |
| <b>header</b>                           | Consulte <a href="#">encabezado IP</a> .                                                                                                                                                                                                                                                                                                                                                                                      |

|                                          |                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HMAC</b>                              | 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. |
| <b>host</b>                              | 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.                                                                                               |
| <b>host multired</b>                     | Sistema con más de una interfaz física y que no reenvía paquetes. Un host multired puede ejecutar protocolos de enrutamiento.                                                                                                                                                                                                                                          |
| <b>ICMP</b>                              | Siglas inglesas de Internet Control Message Protocol (protocolo de mensajes de control de Internet). Se utiliza para administrar e intercambiar mensajes de control.                                                                                                                                                                                                   |
| <b>IKE</b>                               | 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.                                                                                                                                                                        |
| <b>inactividad</b>                       | Interfaz física que no se emplea para transportar tráfico de datos a menos que otra interfaz física haya sufrido algún problema.                                                                                                                                                                                                                                       |
| <b>índice de parámetros de seguridad</b> | 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.                                                                                                                                                                                                          |
| <b>interfaz de red virtual (VNIC)</b>    | 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 zonas IP exclusivas, se configuran conforme a interfaces de red virtual (VNIC) para formar una red virtual.                                                                                              |
| <b>interfaz física</b>                   | 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.                                                                                                                      |
| <b>IP</b>                                | Consulte <a href="#">protocolo de Internet (IP)</a> , <a href="#">IPv4</a> , <a href="#">IPv6</a> .                                                                                                                                                                                                                                                                    |
| <b>IP en encapsulado IP</b>              | Mecanismo para colocar en túneles paquetes IP dentro de paquetes IP.                                                                                                                                                                                                                                                                                                   |
| <b>IPQoS</b>                             | Función de software que permite la implementación del estándar <a href="#">modelo DiffServ</a> , 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.                       |
| <b>IPsec</b>                             | Seguridad IP. Arquitectura de seguridad que proporciona protección a los datagramas IP.                                                                                                                                                                                                                                                                                |
| <b>IPv4</b>                              | Internet Protocol version 4. IPv4 en ocasiones se denomina IP. Esta versión admite un espacio de direcciones de 32 bits.                                                                                                                                                                                                                                               |
| <b>IPv6</b>                              | Internet Protocol version 6. IPv6 admite espacio de direcciones de 128 bits.                                                                                                                                                                                                                                                                                           |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>lista de revocación de certificados (CRL)</b> | 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.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>lista de visitantes</b>                       | La lista de nodos móviles que visitan a un agente externo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>MAC (Message Authentication Code)</b>         | MAC proporciona seguridad en la integridad de los datos y autentica el origen de los datos. MAC no proporciona protección contra intromisiones externas.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>marcador</b>                                  | <p>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 dscpmk.</p> <p>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 dltcosmk.</p> |
| <b>MD5</b>                                       | Una función de hash criptográfica iterativa utilizada para autenticar mensajes, incluso las firmas digitales. Rivest desarrolló esta función en 1991.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>medidor</b>                                   | 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.                                                                                                                                                                                                                                                                                                                                                          |
| <b>modelo DiffServ</b>                           | Estándar de arquitectura de Internet Engineering Task Force para implementar distintas clases de servicios en redes IP. Los módulos principales son clasificador, medidor, marcador, programador y descartador. IPQoS implementa los módulos clasificador, medidor y marcador. El modelo DiffServ se describe en RFC 2475, <i>An Architecture for Differentiated Services</i> .                                                                                                                                                         |
| <b>MTU</b>                                       | 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.                                                                                                                                                                                                                                                                                                                                 |
| <b>NAT</b>                                       | Consulte <a href="#">traducción de la dirección de red</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>nodo</b>                                      | En IPv6, cualquier sistema compatible con IPv6, ya sea host o enrutador.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>nombre de keystore</b>                        | Nombre que un administrador asigna a un área de almacenamiento o keystore, en una <a href="#">tarjeta de interfaz de red</a> . El nombre de keystore también se denomina token o ID de token.                                                                                                                                                                                                                                                                                                                                           |
| <b>paquete</b>                                   | Grupo de información que se transmite como una unidad a través de líneas de comunicaciones. Contiene un <a href="#">encabezado IP</a> y una <a href="#">carga útil</a> .                                                                                                                                                                                                                                                                                                                                                                |
| <b>paquete icmp echo request</b>                 | Paquete que se envía a un sistema en Internet para solicitar una respuesta. Esta clase de paquetes suelen denominarse “ping”.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>PFS (Perfect Forward Secrecy)</b>             | <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 <a href="#">algoritmo Diffie-Hellman</a>.</p>                                                                                                                                        |



|                                                                         |                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PHB<br/>(Per-Hop<br/>Behavior,<br/>comportamiento<br/>por salto)</b> | 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.                                                                                                                                                                       |
| <b>pila</b>                                                             | Consulte <a href="#">pila de IP</a> .                                                                                                                                                                                                                                                                                         |
| <b>pila de IP</b>                                                       | 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.                                                                                                       |
| <b>pila de protocolos</b>                                               | Consulte <a href="#">pila de IP</a> .                                                                                                                                                                                                                                                                                         |
| <b>pila doble</b>                                                       | 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.                                                                                                                     |
| <b>PKI</b>                                                              | 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.                                          |
| <b>prioridad de<br/>usuario</b>                                         | 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.                                                                                                                                       |
| <b>protocolo de<br/>Internet<br/>(IP)</b>                               | Método o protocolo con el cual se envían datos de un sistema a otro por Internet.                                                                                                                                                                                                                                             |
| <b>punto de código<br/>DS</b>                                           | Valor de 6 bits que, al incluirse en el campo DS o un encabezado IP, indica la manera en que se reenvía un paquete.                                                                                                                                                                                                           |
| <b>reconfiguración<br/>dinámica<br/>(DR)</b>                            | 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 Sun de Oracle admiten DR. Es posible que algunas plataformas Sun de Oracle sólo admitan DR de determinados tipos de hardware, como NIC. |
| <b>red privada virtual<br/>(VPN)</b>                                    | Una sola red lógica y segura que emplea túneles en una red pública como Internet.                                                                                                                                                                                                                                             |
| <b>red virtual</b>                                                      | 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”.                          |
| <b>red visitada</b>                                                     | Una red que no es la red doméstica de un nodo móvil, a la cual el nodo móvil se encuentra actualmente conectado.                                                                                                                                                                                                              |
| <b>redireccionar</b>                                                    | En un enrutador, proceso para informar a un host sobre un primer salto más apropiado para llegar a un determinado destino.                                                                                                                                                                                                    |
| <b>repetición de<br/>ataque</b>                                         | 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.                             |

|                                          |                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>resultado</b>                         | 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.                                                                                                                                                             |
| <b>RSA</b>                               | Método para la obtención de firmas digitales y criptosistemas de claves públicas. Dicho método lo describieron sus creadores, Rivest, Shamir y Adleman, en 1978.                                                                                                                                                                                               |
| <b>SA</b>                                | Consulte <a href="#">SA (Security Association)</a> .                                                                                                                                                                                                                                                                                                           |
| <b>SA<br/>(Security<br/>Association)</b> | Asociación que establece las propiedades de seguridad entre un primer host y un segundo.                                                                                                                                                                                                                                                                       |
| <b>SADB</b>                              | 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.                                                                                                                  |
| <b>salto</b>                             | 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.                                                                                                                                         |
| <b>SCTP</b>                              | Consulte protocolo SCTP (Streams Control Transport Protocol).                                                                                                                                                                                                                                                                                                  |
| <b>SCTP</b>                              | 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. |
| <b>selector</b>                          | 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.                                                                                                         |
| <b>servidor proxy</b>                    | 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.                                                                                                                                                    |
| <b>SHA-1</b>                             | 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.                                                                                                                       |
| <b>sniff</b>                             | 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.                                                                                                                                                                   |
| <b>solicitud de<br/>enrutador</b>        | 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.                                                                                                                                                                                            |
| <b>solicitud de vecino</b>               | 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.                                                                                                                     |
| <b>SPD</b>                               | Consulte <a href="#">base de datos de políticas de seguridad (SPD)</a> .                                                                                                                                                                                                                                                                                       |
| <b>SPI</b>                               | Consulte <a href="#">índice de parámetros de seguridad</a> .                                                                                                                                                                                                                                                                                                   |

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>spoof</b>                             | 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.                                                                      |
| <b>tarjeta de interfaz de red</b>        | 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 igb.                                                                                                                                                                                                                                                                                                                                       |
| <b>TCP/IP</b>                            | 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).                                                                                                                                                                                                                                                                                 |
| <b>traducción de la dirección de red</b> | También se conoce como NAT (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.                                                                                                                                                                                                                                                                 |
| <b>Triple-DES</b>                        | 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.                                                                                                                                                                                                                                                                                                                        |
| <b>túnel</b>                             | La ruta a la que sigue un <a href="#">datagrama</a> cuando se encapsula. Consulte <a href="#">encapsulado</a> .                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>túnel bidireccional</b>               | Túnel capaz de transmitir datagramas en ambos sentidos.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>túnel inverso</b>                     | Túnel que comienza en la dirección de auxilio del nodo móvil y termina en el agente interno.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>valor hash</b>                        | 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. <a href="#">MD5</a> y <a href="#">SHA-1</a> son ejemplos de funciones hash de una dirección.                                                                                                                                                                                                                                                                 |
| <b>vínculo IP</b>                        | 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

---

## A

### opción -A

- comando `ikecert`, 305

- comando `ikecert certlocal`, 275

acceso http a CRL, palabra clave `use_http`, 289

acctadm comando, para el control de flujo, 485

aceleración, cálculos IKE, 298

actualizar, claves previamente compartidas (IKE), 270–271

acuerdo de nivel de servicio (SLA), 414

- clases de servicio, 417

- facturación a clientes, según el control de flujo, 484

- proporcionar diferentes clases de servicio, 416

administración de red

- diseño de la red, 25

- nombres de host, 30

administración del tráfico

- control del flujo, 418

- planificar distribuciones de red, 429

- priorizar los flujos de tráfico, 416

- reenvío del tráfico, 422, 423, 424

- regulación del ancho de banda, 415

admisión de ATM, IPv6, en, 172

agregar

- asociaciones de seguridad de IPsec, 232

- certificados autofirmados (IKE), 275

- certificados de autoridad de certificación (IKE), 279–284

- certificados de clave pública (IKE), 279–284

- claves manualmente (IPsec), 243–245

- claves previamente compartidas (IKE), 271–272

- SA IPsec, 243–245

agrupaciones de direcciones

- anexar, 340–341

- configuración, 318–320

- descripción general, 318–320

- eliminar, 340

- ver estadísticas, 344

- vista, 339–340

AH, *Ver* encabezado de autenticación (AH)

algoritmo de autenticación DSS, 306

algoritmo de cifrado 3DES, IPsec y, 221

algoritmo de cifrado AES, IPsec y, 221

algoritmo de cifrado Blowfish, IPsec y, 221

algoritmo de cifrado DES, IPsec y, 221

algoritmo de cifrado RSA, 306

algoritmo de cifrado Triple-DES, IPsec y, 221

algoritmos de autenticación

- certificados IKE, 306

- claves IKE previamente compartidas, 265–267

algoritmos de cifrado

- claves IKE previamente compartidas, 265–267

- IPsec

  - 3DES, 221

  - AES, 221

  - Blowfish, 221

  - DES, 221

almacén de claves softtoken, almacenamiento de claves con metarranura, 305

almacenamiento, claves IKE en hardware, 298–299

almacenamiento de claves

- almacenamiento de claves softtoken, 299

- asociaciones de seguridad de ISAKMP, 304

- ID de señal a partir de metarranura, 299

- almacenamiento de claves (*Continuación*)
  - SA de IPsec, 227
  - softtoken, 305
- almacenamiento de claves softtoken, almacenamiento de claves con metarranura, 299
- almacenar
  - claves IKE en disco, 281, 306, 307
- anuncio de 6to4, 132
- anuncio de enrutador, 192
  - IPv6, 164, 165, 168, 171
  - prefijo, 165
- archivo /etc/bootparams, descripción, 143
- archivo /etc/default/dhcpagent, 198
- archivo /etc/default/dhcpagent, descripción, 207
- archivo /etc/default/inet\_type, 103–104
  - valor DEFAULT\_IP, 158
- archivo /etc/defaultrouter
  - configuración de modo de archivos locales, 54
  - descripción, 143
- archivo /etc/dhcp/dhcptags, descripción, 208
- archivo /etc/dhcp/eventhook, 204
  - descripción, 207
- archivo /etc/dhcp/inittab, descripción, 208
- archivo /etc/dhcp/interfaz.dh\*, descripción, 207
- archivo /etc/ethers, descripción, 143
- archivo /etc/inet/dhcpd4.conf, descripción, 207
- archivo /etc/inet/dhcpd6.conf, descripción, 207
- archivo /etc/inet/dhcpsvc.conf, descripción, 207
- archivo /etc/inet/hosts, 231
  - configuración de modo de archivos locales, 53
  - configuración de modo de cliente de red, 54
  - descripción, 143
- archivo /etc/inet/ike/config
  - certificados autofirmados, 278
  - certificados de clave pública, 282, 287
  - claves previamente compartidas, 269
  - colocar certificados en hardware, 286
  - comando ikercert, 305
  - consideraciones de seguridad, 303
  - descripción, 261, 303
  - ejemplo, 269
- archivo /etc/inet/ike/config, entrada de biblioteca PKCS #11, 305
- archivo /etc/inet/ike/config
  - palabra clave cert\_root, 282, 287
  - palabra clave cert\_trust, 278, 286
  - palabra clave ignore\_crls, 283
  - palabra clave ldap-list, 290
  - palabra clave pkcs11\_path, 285, 305
  - palabra clave use\_http, 289
  - palabra claveproxy, 290
  - resumen, 263
- archivo /etc/inet/ipaddrsel.conf, 114, 155
- archivo /etc/inet/ipsecinit.conf, 252–254
- archivo /etc/inet/ndpd.conf, 81, 160
  - anuncio de enrutador 6to4, 132
  - configuración de direcciones temporales, 84
  - crear, 81
  - palabras clave, 152–155, 161
  - variables de configuración de interfaz, 152
  - variables de configuración de prefijo, 154
- 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/netmasks, descripción, 143
- archivo /etc/networks, descripción, 143
- archivo /etc/protocols, descripción, 143
- archivo /etc/services, descripción, 143
- archivo /var/inet/ndpd\_state.interface, 160
- archivo de registro, vaciar en filtro IP, 347
- archivo de zona, 89
- archivo de zona inversa, 89
- archivo defaultrouter, configuración de modo de archivos locales, 54
- archivo dhcpagent, descripción, 207
- archivo dhcpd4.conf, descripción, 207
- archivo dhcpd6.conf, descripción, 207
- archivo dhcpsvc.conf, 207
- archivo eventhook, 204
- archivo hosts, 231
- archivo ike.preshared, 270, 304
- archivo Ike.preshared, ejemplo, 272
- archivo inet\_type, 103–104
- archivo ipaddrsel.conf, 114, 155
- archivo ipf.conf, 314–317
  - Ver filtro IP
- archivo ipnat.conf, 317–318

- archivo `ipnat.conf` (*Continuación*)
  - Ver filtro IP
- archivo `ippool.conf`, 318–320
  - Ver filtro IP
- archivo `ipsecinit.conf`
  - comprobar sintaxis, 232
  - consideraciones de seguridad, 253–254
  - descripción, 227
  - ejemplo, 253
  - objetivo, 221
  - omisión de LAN, 240
  - proteger servidor web, 234
  - ubicación y alcance, 226
  - verificación de la sintaxis, 241
- archivo `ipseckey`s
  - almacenamiento de claves IPsec, 227
  - verificación de sintaxis, 245
- archivo `ndpd.conf`
  - anuncio 6to4, 132
  - configuración de direcciones temporales, 84
  - crear, en un enrutador IPv6, 81
- archivo `ndpd.conf`
  - lista de palabras clave, 152–155
  - variables de configuración de interfaz, 152
  - variables de configuración de prefijo, 154
- archivo `ike/config`, Ver `archivo/etc/inet/ike/config`
- archivos
  - IKE
    - archivo `ike/config`, 227, 261, 263, 303
    - archivo `ike.preshared`, 263, 304
    - directorio `crls`, 264, 307
    - directorio `ike.privatekeys`, 264, 307
    - directorio `publickeys`, 264, 307
  - IPsec
    - archivo `ipsecinit.conf`, 227, 252–254
    - archivo `ipsecinit.conf`, 227
    - archivo `ipseckey`s, 227
- archivos de configuración
  - creación para filtro IP, 349–350
  - ejemplos de filtro IP, 314
  - IPv6
    - archivo `/etc/inet/ipaddrsel.conf`, 155
    - archivo `/etc/inet/ndpd.conf`, 152, 154
    - archivo `/etc/inet/ndpd.conf`, 152–155
  - archivos de configuración IPQoS de ejemplo
    - configuración de dispositivo VLAN, 498
    - segmento de reconocimiento de colores, 493
    - servidor de aplicaciones, 463
    - servidor web "best-effort", 451
    - servidor web de nivel alto, 450
  - archivos de política
    - archivo `ike/config`, 227, 263, 303
    - archivo `ipsecinit.conf`, 252–254
    - consideraciones de seguridad, 253–254
  - archivos de registro
    - creación para filtro IP, 345–346
    - ver para filtro IP, 346–347
  - archivos locales, selección como servicio de nombres, 31
  - argumento `tokens`, comando `ikecert`, 305
  - arquitectura de seguridad IP, Ver IPsec
  - asociación de identidad, 190
  - asociaciones de seguridad
    - generación de números aleatorios, 261
    - IKE, 302
    - ISAKMP, 260
  - asociaciones de seguridad (SA)
    - agregar IPsec, 232, 241
    - base de datos IPsec, 255
    - crear manualmente, 243–245
    - definición, 212
    - IPsec, 217–218, 232, 241
  - asociaciones de seguridad del protocolo de gestión de claves y asociaciones de seguridad de Internet (ISAKMP), ubicación de almacenamiento, 304
  - aspectos sobre la seguridad, redes habilitadas para IPv6, 41–42
- B**
  - base de datos de asociaciones de seguridad (SADB), 255
    - IPsec, 212
  - base de datos de política de seguridad (SPD), configuración, 252
  - base de datos de políticas de seguridad (SPD)
    - IPsec, 212, 214

- base de datos de red, servicio SMF
  - name-service/switch, 145
- base de datos ethers, comprobar entradas, 140
- base de datos hosts
  - archivo /etc/inet/hosts
    - configuración de modo de archivos locales, 53
  - comprobación de entradas, 140
- base de datos ike.privatekeys, 307
- base de datos netmasks, agregar subredes, 54
- base de datos publickeys, 307
- base de datos services, actualizar, para SCTP, 72
- bases de datos
  - base de datos de asociaciones de seguridad (SADB), 255
  - base de datos de políticas de seguridad (SPD), 212
  - base de datos ike/crls, 307
  - base de datos ike.privatekeys, 305, 307
  - base de datos ike/publickeys, 306
  - base de datos ike/publickeys, 307
  - IKE, 304–307
- bases de datos de red
  - base de datos ethers
    - comprobar entradas, 140
  - base de datos hosts
    - comprobación de entradas, 140
  - servicios de nombres, 147
  - servicios SMF name-service/switch y, 145
- biblioteca PKCS #11, en archivo ike/config, 305
- borradores de Internet, SCTP con IPsec, 213

## C

- cálculos, aceleración de IKE en hardware, 298–299
- calidad de servicio (QoS), política QoS, 414
- calidad del servicio (QoS), tareas, 411
- cambio de dirección de capa de vínculo, 168
- capa de transporte
  - obtener estado del protocolo de transporte, 96–97
  - TCP/IP
    - protocolo SCTP, 71–74
- carga de seguridad encapsuladora (ESP)
  - consideraciones de seguridad, 219
  - descripción, 219–220
  - proteger paquetes IP, 211

- carga de seguridad encapsuladora(ESP), mecanismo de protección IPsec, 218–221
- certificados
  - agregar a base de datos, 281
  - almacenamiento
    - en hardware, 298
  - almacenar
    - IKE, 306
  - creación de autofirmados (IKE), 275
  - de autoridad de certificación, 281
  - de autoridad de certificación en hardware, 288
  - descripción, 280
  - en archivo ike/config, 286
  - enumeración, 277
  - guardar
    - en equipo, 274
  - IKE, 262
  - omitir CRL, 283
  - solicitar
    - de autoridad de certificación, 280
    - en hardware, 285
- certificados de claves públicas, *Ver* certificados
- cifrado, *Ver* algoritmos de cifrado
- clases, 417
  - definir, en el archivo de configuración IPQoS, 461, 465
  - selectores, lista de, 490
  - sintaxis de la cláusula class, 504
- clases de servicio, *Ver* clases
- clasificador ipgpc, *Ver* módulo clasificador
- cláusula class, del archivo de configuración IPQoS, 453
- cláusula class, en el archivo de configuración IPQoS, 504
- cláusula filter, del archivo de configuración IPQoS, 455
- cláusula filter, en el archivo de configuración IPQoS, 505
- cláusula params
  - de un marcador action, 457
  - de una acción flowacct, 459
  - definir estadísticas globales, 453, 505
  - para una instrucción action de medición, 470
  - sintaxis, 505



- claves
  - almacenar (IKE)
    - certificados, 306
    - claves públicas, 306
    - privadas, 305
  - base de datos `ike.privatekeys`, 307
  - base de datos `ike/publickeys`, 307
  - gestión automática, 260
  - gestión manual, 255–256
  - gestionar IPsec, 217–218
  - previamente compartidas (IKE), 262
- claves previamente compartidas (IKE)
  - almacenar, 304
  - descripción, 262
  - mapa de tareas, 268
  - reemplazar, 270–271
  - visualización de algoritmos y grupos de fase 1, 265–267
- claves previamente compartidas (IPsec),
  - crear, 243–245
- claves privadas, almacenar (IKE), 305
- claves públicas, almacenar (IKE), 306
- cliente DHCP
  - abandono de dirección IP, 197
  - administración, 196
  - cierre, 194
  - definición, 181
  - desactivar, 196
  - desconfigurar, 196
  - ejecutar programas con, 203–204
  - extensión de permiso, 197
  - habilitar, 195–196
  - información de red sin permiso, 197
  - inicio, 192, 197
  - interfaces lógicas, 199
  - liberación de dirección IP, 197
  - nombre de host
    - especificar, 200
  - parámetros, 198
  - secuencias de eventos, 203–204
  - varias interfaces de red, 199
- cliente DHCPv4, gestión de interfaz de red, 193
- cliente DHCPv6, gestión de la interfaz de red, 193
- comando `command`, verificar protección de paquetes, 248–249
- comando `/usr/lib/inet/dhcrelay`, descripción, 205
- comando `/usr/sadm/admin/bin/dhcpmgr`, descripción, 206
- comando `/usr/sbin/6to4relay`, 133
- comando `/usr/sbin/dhcpagent`, descripción, 206
- comando `/usr/sbin/dhcpconfig`, descripción, 206
- comando `/usr/sbin/dhcpinfo`, descripción, 206
- comando `/usr/sbin/dhtadm`, descripción, 206
- comando `/usr/sbin/ipdam`, DHCP y, 206
- comando `/usr/sbin/omshell`, descripción, 206
- comando `/usr/sbin/ping`, 102
  - descripción, 101
  - ejecución, 102
  - sintaxis, 101
- comando `/usr/sbin/pntadm`, descripción, 206
- comando `/usr/sbin/snoop`, DHCP y, 206
- comando `6to4relay`, 133
  - definición, 157
  - ejemplos, 158
  - sintaxis, 157
  - tareas de configuración de túnel, 133
- comando `acctadm`, para control de flujo, 419, 501
- comando `dhcpagent`, descripción, 206
- comando `dhcpconfig`, descripción, 206
- comando `dhcpinfo`, descripción, 206
- comando `dhcpmgr`, descripción, 206
- comando `dhcrelay`, descripción, 205
- comando `dhtadm`, descripción, 206
- comando `dladm`
  - creación de túneles, 127–131
  - modificación de la configuración de túnel, 135–136
  - supresión de túneles IP, 138
  - visualización de información de túnel, 136–137
- comando `ikeadm`
  - descripción, 302, 303–304
  - subcomando `dump`, 265–267
- comando `ikecert`
  - descripción, 302, 304
  - opción `-A`, 305
  - opción `-a`, 285
  - opción `-T`, 285
  - opción `-t`, 306

- comando `ikecert certdb`
  - opción -a, 276, 281
- comando `ikecert certlocal`
  - opción -kc, 280
  - opción -ks, 275
- comando `ikecert certrldb`, opción -a, 290
- comando `ikecert tokens`, 298
- comando `ipaddrsel`, 114, 156–157
- comando `ipadm`, 313
  - control del cliente DHCP, 197
  - función estricta de hosts múltiples, 240
  - hosts múltiples, 63
  - parámetro `hostmodel`, 240
  - sondeo de una interfaz, 48
  - uso como herramienta de resolución de problemas, 139
- comando `ipdam`, DHCP y, 206
- comando `ipf`
  - Ver también* filtro IP
  - anexar reglas de línea de comandos, 334
  - opción -a, 332–333
  - opción -D, 328–329
  - opción -E, 325–326
  - opción -F, 327–328, 332–333, 333–334, 336–337
  - opción -f, 325–326, 332–333, 334, 335
  - opción -I, 335, 336–337
  - opción -s, 335–336
  - opción -6, 320–321
- comando `ipfstat`, 342
  - Ver también* filtro IP
  - opción -i, 331
  - opción -o, 331
  - opción -6, 320–321
  - opción -I, 331
  - opción -i, 331
  - opción -o, 331
  - opción -s, 342–343
  - opción -t, 342
- comando `ipmon`
  - Ver también* filtro IP
  - IPv6 y, 320–321
  - opción -a, 346–347
  - opción -F, 347
  - opción -o, 346–347
- comando `ipnat`
  - Ver también* filtro IP
  - opción -C, 328
  - opción -F, 328, 338
  - opción -f, 325–326
  - opción -f, 338–339
  - opción -l, 337–338
  - opción -s, 343–344
- comando `ippool`
  - Ver también* filtro IP
  - anexar reglas de línea de comandos, 340–341
  - IPv6 y, 320–321
  - opción -l, 339–340
  - opción -F, 340
  - opción -f, 340–341
  - opciones -s, 344
- comando `ipqos conf`
  - aplicar una configuración, 476, 477
  - listado de la configuración actual, 477
  - opciones de comando, 506
- comando `ipsec conf`
  - configuración de política IPsec, 252
  - configuración de túneles, 222
  - consideraciones de seguridad, 253–254
  - descripción, 227
  - objetivo, 221
  - visualización de política IPsec, 252–254
  - visualizar política IPsec, 233–235, 235
- comando `ipseckey`
  - consideraciones de seguridad, 256
  - descripción, 227, 255–256
  - finalidad, 218
- comando `ks stat`, usado con IPQoS, 486
- comando `netstat`
  - descripción, 95
  - ejecutar comprobaciones de software, 140
  - extensiones de IPv6, 158
  - opción -a, 98
  - opción -f, 98
  - opción -r, 100–101
  - opción `inet`, 98
  - opción `inet6`, 98
  - sintaxis, 95
  - visualizar estadísticas por protocolo, 95

- comando netstat (*Continuación*)
  - visualizar estado de rutas conocidas, 100–101
- comando nslookup, 172
  - IPv6, 91
- comando omshell, descripción, 206
- comando ping, 102
  - descripción, 101
  - ejecución, 102
  - extensiones de IPv6, 159
  - opción -s, 102
  - sintaxis, 101
- comando pntadm, descripción, 206
- comando route
  - IPsec, 242
  - opción inet6, 159
- comando routeadm
  - configuración de enrutador IPv6, 80
  - reenvío de IP, 239, 240
- comando snoop
  - comprobación de paquetes en la capa IP, 110–113
  - comprobar flujo de paquetes, 107
  - comprobar paquetes entre servidor y cliente, 109
  - DHCP y, 206
  - extensiones de IPv6, 159
  - palabra clave de protocolo ip6, 159
  - supervisar tráfico de IPv6, 109–110
  - visualizar contenido de paquetes, 107
  - visualizar paquetes protegidos, 257
- comando traceroute
  - definición, 105–107
  - extensiones de IPv6, 159
  - seguimiento de rutas, 106–107
- comando ipnat, anexas reglas de línea de
  - comandos, 338–339
- comandos
  - IKE, 304–307
    - comando ikeadm, 263, 302, 303–304
    - comando ikecert, 263, 302, 304
    - daemon in.iked, 302
  - IPsec
    - comando in.iked, 218
    - comando ipsecalg, 220, 254
    - comando ipsecconf, 227, 252
    - comando ipseckey, 227, 255–256
  - comandos, IPsec (*Continuación*)
    - comando snoop, 257
    - consideraciones de seguridad, 256
    - lista de, 226–227
- comportamiento por salto (PHB), 422
  - definir, en el archivo de configuración IPQoS, 471
  - reenvío AF, 423
  - reenvío EF, 423
  - utilizar, con el marcador dscpmk, 495
- confidencialidad directa perfecta (PFS)
  - descripción, 260
  - IKE, 260
- configuración
  - agrupaciones de direcciones, 318–320
  - archivo ike/config, 303
  - archivo ipsecinit.conf, 252–254
  - archivos de configuración TCP/IP, 143
  - enrutadores, 56
    - descripción general, 57
  - enrutadores habilitados para IPv6, 80
  - IPsec, 252
  - manual de interfaces, para IPv6, 78–79
  - redes TCP/IP
    - servicio SMF name-service/switch, 145
  - reglas de filtros de paquetes, 314–317
  - reglas NAT, 317–318
  - túneles
    - Ver túneles
- configuración automática de direcciones
  - IPv6, 160, 164
- configuración automática de direcciones sin
  - estado, 165
- configuración de cliente, 188
- configuración de enrutadores, enrutador IPv4, 56
- configuración de IKE (mapa de tareas), 267
- configuración de IKE con certificados de clave pública
  - (mapa de tareas), 273
- configuración de IKE con claves previamente
  - compartidas (mapa de tareas), 268
- configuración de IKE para sistemas portátiles (mapa de
  - tareas), 290
- configuración de red
  - configuración de servidor de configuración de
    - red, 55

configuración de red (*Continuación*)

- configurar
    - servicios, 70
  - configurar seguridad, 209
  - enrutador, 57
  - enrutador IPv6, 80
  - hosts múltiples habilitados para IPv6, 78–79
  - tareas de configuración de red IPv4, 45
- configuración de redes, habilitar IPv6 en un host, 82–89
- configuración de vínculo persistente, creación, 50
- configurar
  - cliente DHCP, 187
  - enrutadores, 147
  - IKE, 267
  - IKE con certificados autofirmados, 274–279
  - IKE con certificados de autoridad de certificación, 279–284
  - IKE con certificados de clave pública, 273, 274–279
  - IKE con certificados en hardware, 284–288
  - IKE con sistemas portátiles, 291–297
- redes TCP/IP
  - servicios TCP/IP estándar, 70
- seguridad de red con un rol, 245–246
- VPN en modo túnel con IPsec, 239–242
- VPN protegida con IPsec, 239–242
- conjunto de protocolos TCP/IP, visualizar estadísticas, 95
- conjuntos de reglas
  - Ver consulte filtro IP
  - filtros de paquetes, 314–320
  - inactivos
    - Ver también filtro IP
  - NAT, 317–318
- conjuntos de reglas activos, Ver filtro IP
- conjuntos de reglas inactivos, Ver filtro IP
- consideraciones de seguridad
  - archivo ike/config, 303
  - archivo ipsecinit.conf, 253–254
  - archivo ipseckeys file, 244
  - carga de seguridad encapsuladora (ESP), 219
  - claves precompartidas, 262
  - comando ipsecconf, 253–254
  - comando ipseckey, 256

consideraciones de seguridad (*Continuación*)

- configuración
  - IPsec, 231
  - encabezado de autenticación (AH), 219
  - problemas de enrutador de relé de 6to4, 142
  - protocolos de seguridad, 219
  - sockets bloqueados, 253
- control de flujo, 484, 499
  - tabla de registro de flujo, 500
- control del flujo, mediante los módulos de medición, 418
- creación
  - asociaciones de seguridad de IPsec, 232
  - certificados autofirmados (IKE), 275
- creación de directorio /tftboot, 55
- crear
  - rol relativo a seguridad, 245–246
  - SA IPsec, 243–245
  - solicitudes de certificados, 280
- crear archivo, ipsecinit.conf, 231
- CRL
  - acceder desde ubicación central, 288
  - base de datos ike/crls, 307
  - comando ikecert certrldb, 307
  - enumeración, 289
  - omitir, 283
- cumplimiento del tráfico
  - definir, 470
  - parámetros de tasa, 492
  - parámetros de tasas, 492
  - planificación
    - tasas en la política QoS, 439
  - planificar
    - resultados en la política QoS, 439
  - resultados, 418, 492

**D**

- daemon /usr/lib/inet/dhcpd, descripción, 205
- daemon /usr/lib/inet/in.dhcpd, descripción, 205
- daemon /usr/sbin/in.routed
  - descripción, 147
  - modo de ahorro de espacio, 148

- daemon /usr/sbin/inetd
  - comprobar el estado de inetd, 140
  - servicios iniciados por, 70
- daemon dhcpagent, archivo de parámetros, 207
- daemon dhcpcd, descripción, 205
- daemon in.dhcpcd, descripción, 205
- daemon in.iked
  - activar, 302
  - descripción, 260
  - opción -c, 270
  - opción -f, 270
- daemon in.ndpd
  - comprobar el estado, 140
  - crear un registro, 105
  - opciones, 160
- daemon in.ripngd, 80, 161
- daemon in.routed
  - crear un registro, 104
  - descripción, 147
  - modo de ahorro de espacio, 148
- daemon in.tftpd, 55
- daemon in.tftpd, activación, 55
- daemon inetd
  - administrar servicios, 145
- daemon inetd, comprobar el estado, 140
- daemon inetd
  - servicios de IPv6, 161–163
  - servicios iniciados por, 70
- daemons
  - daemon in.iked, 260, 263
  - daemon in.ndpd, 160
  - daemon in.ripngd, 80, 161
  - in.iked daemon, 302
  - servicios de Internet inetd, 145
- datagramas, IP, 211
- datagramas IP, proteger con IPsec, 211
- descubrimiento de enrutador, en IPv6, 165, 168
- descubrimiento de enrutadores, en IPv6, 160
- deshabilitar filtro IP, 328–329
- detección de direcciones duplicadas, algoritmo, 167
- detección de inasequibilidad de vecinos
  - IPv6, 166, 169
- dhcpagent daemon, 192
- DHCPv4 en comparación con DHCPv6, 188
- DHCPv6, nombre de cliente, 189
- DHCPv6 en comparación con DHCPv4, 188
- dirección local de vínculo, configuración manual, con un token, 88
- dirección MAC, 189
- dirección temporal, en IPv6
  - configurar, 84–86
  - definición, 83–86
- direcciones
  - selección de direcciones predeterminadas, 113–115
  - temporales, en IPv6, 83–86
- direcciones de difusión por proximidad, 133
- direcciones IP
  - clases de red
    - administración de número de red, 27
    - diseño de un esquema de direcciones, 27
    - notación CIDR, 27
- direcciones IPv6, exclusividad, 166
- direcciones locales de vínculo
  - IPv6, 166, 169
- direcciones multidifusión, IPv6, comparación con direcciones de emisión, 169
- directorio /etc/inet/ike/crls, 307
- directorio /etc/inet/ike/publickeys, 307
- directorio /etc/inet/secret/ike.privatekeys, 307
- directorios
  - certificados (IKE), 306
  - claves previamente compartidas (IKE), 304
  - claves privadas (IKE), 305
  - claves públicas (IKE), 306
  - directorios /etc/inet/publickeys, 306
  - /etc/inet, 263
  - /etc/inet/ike, 264
  - /etc/inet/secret, 263
  - /etc/inet/secret/ike.privatekeys, 305
- diseño de la red
  - denominación de hosts, 30
  - descripción general, 25
  - esquema de direcciones IP, 27
  - selección de nombres de dominio, 31
- dispositivos de LAN virtual (VLAN) en una red IPQoS, 497
- distribuciones de red para IPQoS
  - ejemplo de configuración, 444

distribuciones de red para IPQoS (*Continuación*)

- Red LAN con conjuntos de servidores con IPQoS, 429
  - red LAN con cortafuegos con IPQoS, 430
  - Red LAN con hosts con IPQoS, 429
- dominios lógicos, IPsec, 226

**E**

- ejemplo de red de IPQoS, 449
- encabezado de autenticación (AH)
  - consideraciones de seguridad, 219
  - mecanismo de protección IPsec, 218–221
  - proteger datagrama IP, 218
  - proteger paquetes IP, 211
- enlaces de filtros de paquetes, 320
- enrutador con Diffserv
  - evaluación de puntos de código DS, 496
  - planificar, 433
- enrutador de límite, 47
- enrutador de límite de sistema, en ubicación 6to4, 121
- enrutador de reenvío, configuración de túnel 6to4, 133, 134
- enrutador de reenvío 6to4
  - cuestiones de seguridad, 122–124
  - tareas de configuración de túnel, 133, 134
- enrutador de reenvío de paquetes, 47
- enrutador de relé 6to4, topología de túnel, 123
- enrutador de relé de 6to4
  - en un túnel de 6to4, 157
  - problemas de seguridad, 142
- enrutador predeterminado, definición, 47
- enrutadores
  - configuración
    - IPv6, 80
  - configuración de modo de archivos locales, 54
  - configurar, 147
  - definición, 57, 147
  - enrutador de reenvío de paquetes, 47
  - función, en topología 6to4, 120
  - problemas al actualizar a IPv6, 141
  - protocolos de enrutamiento
    - descripción, 147, 148

- enrutamiento
  - configuración estática, 65
  - en hosts de interfaz única, 65
  - enrutamiento dinámico, 59
  - enrutamiento estático, 59
  - IPv6, 170
  - puerta de enlace, 59
- enrutamiento dinámico, uso recomendado, 60
- enrutamiento estático
  - agregar una ruta estática, 61–62
  - configuración manual en un host, 65
  - ejemplo de configuración, 61–62
  - uso recomendado, 60
- entrada /opt/SUNWconn/lib/libpkcs11.so, en archivo ike/config, 305
- enumeración
  - certificados (IPsec), 277
  - CRL (IPsec), 289
  - hardware (IPsec), 298
  - ID de token (IPsec), 298
- enumerar
  - algoritmos (IPsec), 220
  - certificados (IPsec), 288
  - ID de señal a partir de metarranura, 299
- envoltorios, TCP, 74
- envoltorios TCP, activar, 74
- equilibrio de carga, en una red habilitada para IPv6, 168
- equilibrio de la carga, en una red con IPQoS, 429
- equilibrio de la carga entrante, 168
- equipos, proteger comunicación, 230–233
- ESP, *Ver* carga de seguridad encapsuladora (ESP)
- estadísticas
  - por protocolo (netstat), 95
  - transmisión de paquetes (ping), 102
- estadísticas de estado, *ver*, 342–343
- estadísticas de IPQoS
  - activación de las estadísticas globales, 505
  - activar estadísticas basadas en clases, 505
  - activar estadísticas globales, 453
  - generar, con el comando kstat, 486
- estructura criptográfica, IPsec y, 254
- eventos DHCP, 203–204
- extensión de permiso DHCP, 197

**F**

## filtro IP

- administrar conjuntos de reglas de filtros de paquetes, 330–337
- agrupaciones de direcciones
  - anexar, 340–341
  - eliminar, 340
  - vista, 339–340
- agrupaciones de direcciones y, 318–320
- archivo `/etc/ipf/ipf.conf`, 349–350
- archivo `/etc/ipf/ipf6.conf`, 320–321
- archivo `/etc/ipf/ipnat.conf`, 349–350
- archivo `/etc/ipf/ippool.conf`, 349–350
- archivo `ipf.conf`, 314–317
- archivo `ipf6.conf`, 320–321
- archivo `ipnat.conf`, 317–318
- archivo `ippool.conf`, 318–320
- código abierto, 310
- comando `ipadm`, 313
- comando `ipf`, 325–326
  - opción `-6`, 320–321
- comando `ipfstat`
  - opción `-6`, 320–321
- comando `ipmon`
  - IPv6 y, 320–321
- comando `ipnat`, 325–326
- comando `ippool`, 339–340
  - IPv6 y, 320–321
- conjunto de reglas
  - activación de otro, 332–333
- conjuntos de reglas
  - activos, 331
  - alternar, 335–336
  - anexar a activos, 334
  - anexar a inactivos, 335
  - eliminar, 333–334
  - eliminar inactivos, 336–337
  - inactivos, 331
- conjuntos de reglas y, 314–320
- creación
  - archivos de registro, 345–346
- creación de archivos de configuración, 349–350
- desactivar
  - NAT, 328

filtro IP (*Continuación*)

- descripción general, 309–310
  - descripción general de filtros de paquetes, 314–317
  - deshabilitar, 328–329
  - directrices de uso, 313
  - ejemplos de archivos de configuración, 314
  - eliminación
    - reglas NAT, 338
  - en IPMP, 313
  - enlaces de filtros de paquetes, 320, 324–325
  - filtros en bucle de retorno, 326–327
  - guardar paquetes registrados en un
    - archivo, 347–348
  - IPv6, 320–321
  - NAT y, 317–318
  - reactivar, 325–326
  - reglas NAT
    - anexar, 338–339
    - ver, 337–338
  - vaciar archivo de registro, 347
  - ver
    - archivos de registro, 346–347
    - estadísticas de agrupación de direcciones, 344
    - estadísticas de estado, 342–343
    - estadísticas NAT, 343–344
    - tablas de estado, 342
- filtros, 418
- crear, en el archivo de configuración IPQoS, 461, 466
  - planificar, en la política QoS, 436
  - selectores, lista de, 490
  - sintaxis de la cláusula `filter`, 505
- filtros de paquetes
- activación de otro conjunto de reglas, 332–333
  - administrar conjuntos de reglas, 330–337
  - alternar entre conjuntos de reglas, 335–336
  - anexar
    - reglas a conjunto activo, 334
    - reglas a conjunto inactivo, 335
  - configuración, 314–317
  - desactivar, 327–328
  - eliminar
    - conjunto de reglas activo, 333–334
    - conjunto de reglas inactivo, 336–337

filtros de paquetes (*Continuación*)

- volver a cargar tras actualizar el conjunto de reglas actual, 332–333

## firmas digitales

- DSA, 306
- RSA, 306

## flujo de paquetes

- a través de túnel, 121
- enrutador de reenvío, 123

## flujo de paquetes, IPv6

- 6to4 e IPv6 nativo, 123
- a través de túnel 6to4, 121

**G**

## gestión de claves

- automática, 260
- IKE, 260
- IPsec, 217–218
- manual, 255–256
- servicio ike, 218
- servicio manual-key, 218
- zonas y, 229

## grupos de difusión por proximidad, enrutador de reenvío 6to4, 133

## grupos Diffie-Hellman, claves IKE previamente compartidas, 265–267

**H**

## hardware

- aceleración de cálculos IKE, 298
- almacenamiento de claves IKE, 298–299
- buscar conectado, 298

## hardware para redes con IPQoS, 428

## hosts

- comprobación de conectividad IP, 102
- comprobar conectividad de host con ping, 101
- configurar para IPv6, 82–89
- direcciones IPv6 temporales, 83–86
- hosts múltiples
  - configuración, 62

hosts (*Continuación*)

- nombre de host
  - administración, 30
  - resolución de problemas generales, 139

## hosts múltiples

- definición, 62
- habilitación para IPv6, 78–79

**I**

## ID de cliente, 189

## ID de interfaz, utilizar un token configurado manualmente, 88

## ID de token, del hardware, 307

## IKE

- agregar certificados autofirmados, 275
- archivo ike.preshared, 304
- archivos de configuración, 263–264
- asociaciones de seguridad, 302
- asociaciones de seguridad de ISAKMP, 260, 261
- base de datos crls, 307
- base de datos ike.privatekeys, 307
- base de datos publickeys, 307
- bases de datos, 304–307
- cambiar
  - nivel de privilegios, 304
- certificados, 262
- claves previamente compartidas, 262
  - visualización de algoritmos y grupos de fase 1, 265–267
- comando ikeadm, 303–304
- comando ikecert, 304
- comando ikecert certtdb, 281
- comando ikecert certrldb, 290
- comando ikecert tokens, 298
- comprobación de configuración válida, 270
- confidencialidad directa perfecta (PFS), 260
- configurar
  - con certificados de autoridad de certificación, 279–284
  - con certificados de clave pública, 273
  - con claves previamente compartidas, 268
  - para sistemas portátiles, 291–297
- creación de certificados autofirmados, 275



IKE (*Continuación*)

- daemon, 302
- daemon `in.iked`, 302
- descripción de servicios SMF, 263–264
- descripción general, 259
- descripciones de comandos, 263–264
- generar solicitudes de certificación, 280
- gestión con SMF, 247–248
- gestión de claves, 260
- implementar, 267
- intercambio de fase 1, 260
- intercambio de fase 2, 261
- mediante una placa Crypto Accelerator de Sun, 307
- NAT y, 294–295, 296–297
- nivel de privilegios
  - cambiar, 304
  - descripción, 303
- referencia, 301
- RFC, 213
- servicio SMF, 301–302
- sistemas portátiles, 291–297
- ubicaciones de almacenamiento para
  - claves, 263–264
- uso de la placa Sun Crypto Accelerator
  - 6000, 298–299
- utilizar una placa Crypto Accelerator de Sun, 305
- visualización
  - algoritmos y grupos de fase 1, 265–267
  - visualización de algoritmos disponibles, 265–267
  - visualización de algoritmos y grupos de fase 1, 265–267
- indicador de recursos uniforme (URI), para acceder a
  - CRL, 288
- índice de parámetros de seguridad (SPI),
  - descripción, 217–218
- instrucción `action`, 503
- interfaces
  - comprobar paquetes, 107–108
  - configuración
    - desde un vínculo de datos, 48
    - manual, para IPv6, 78–79
  - configurar
    - direcciones temporales, 83–86
  - creación de configuración persistente, 50

## interfaces IP

- configuradas en túneles, 125, 129, 132
- interfaces lógicas, sistemas cliente DHCP, 199
- interfaz de socket `PF_KEY`
  - IPsec, 217, 227
- interfaz lógica, 190
- IPMP, activación de filtrado de paquetes, 313
- IPQoS, 411
  - archivo de configuración, 449, 502
    - cláusula `class`, 453
    - cláusula `filter`, 455
    - instrucción `action` de marcador, 456
    - instrucción `action` inicial, 503
    - instrucción `action` inicial, 452
    - lista de módulos IPQoS, 504
    - sintaxis, 502
    - sintaxis de instrucción `action`, 503
  - compatibilidad con dispositivos VLAN, 497
  - directrices en redes habilitadas para IPv6, 40
  - distribuciones de red admitidas, 428
  - distribuciones de red compatibles, 429, 430
  - ejemplo de configuración, 444–446
  - ejemplo de red, 449
  - enrutadores en una red IPQoS, 472
  - funciones, 412
  - funciones de administración del tráfico, 415, 416
  - generación de estadísticas, 486
  - implementación del modelo Diffserv, 417
  - mensajes de error, 478
  - páginas de comando `man`, 413
  - peticiones de comentarios relacionadas, 413
  - planificar la configuración, 427
  - planificar la política QoS, 431
  - registro de mensajes, 477
- `ipqosconf`, 449
- IPsec
  - activar, 227
  - agregar asociaciones de seguridad (SA), 232, 241
  - algoritmos de autenticación, 220
  - algoritmos de cifrado, 221
  - archivo `/etc/hosts`, 231
  - archivo `ipsecinit.conf`
    - archivo de política, 221
    - configurar, 231

IPsec, archivo ipsecinit.conf (*Continuación*)

- descripción, 252–254
- omisión de LAN, 240
- proteger servidor web, 234
- archivos de configuración, 226–227
- archivos de política, 252–254
- asociaciones de seguridad (SA), 212, 217–218
- base de datos de asociaciones de seguridad (SADB), 212, 255
- base de datos de política de seguridad (SPD), 252
- base de datos de políticas de seguridad (SPD), 212, 214
- carga de seguridad encapsuladora (ESP), 218–221
- comando de política
  - ipseconf, 252
- comando ipsecalgs, 220, 254
- comando ipsecconf, 221, 252
- comando ipseckey, 218, 255–256
- comando route, 242
- comando snoop, 257
- comandos, lista de, 226–227
- componentes, 212
- configuración, 252
- configuración de política
  - permanente, 252–254
  - temporal, 252
- configurar, 221
- crear manualmente SA, 243–245
- daemon in.iked, 218
- datos de encapsulación, 219
- descripción general, 211
- dominios lógicos, 226
- estructura criptográfica y, 254
- etiquetas Trusted Extensions y, 230
- extensiones para utilidades
  - comando snoop, 257
- fuentes de algoritmo, 254
- gestión con SMF, 247–248
- gestión de claves, 217–218
- implementar, 230
- índice de parámetros de seguridad (SPI), 217–218
- mecanismos de protección, 218–221
- mecanismos de seguridad, 212
- modo de transporte, 221–223

IPsec (*Continuación*)

- modo de túnel, 221–223
- NAT y, 224–225
- omitir, 221, 234
- paquetes etiquetados y, 230
- política de protección, 221
- proceso de paquetes entrantes, 214
- proceso de paquetes salientes, 214
- protección del inicio de sesión remoto, 231
- proteger
  - paquetes, 211
  - servidores web, 233–235
  - sistemas portátiles, 291–297
  - VPN, 239–242
- proteger tráfico, 230–233
- proteger una VPN, 236–242
- protocolo SCTP y, 225, 230
- protocolos de seguridad, 212, 217–218
- RBAC y, 229
- redes privadas virtuales (VPN), 224, 239–242
- RFC, 213
- roles de seguridad, 245–246
- servicios
  - manual-key, 227
  - policy, 227
- servicios, lista de, 226–227
- servicios SMF, 251–252
- terminología, 213–214
- túneles, 224
- uso de ssh para inicio de sesión remoto seguro, 233
- utilidades de claves
  - comando ipseckey, 255–256
  - IKE, 260
- verificar protección de paquetes, 248–249
- visualizar políticas, 235
- VPN IPv4 y, 239–242
- zonas y, 226
- zones y, 229

IPv6

- admisión de ATM, 172
- agregar
  - compatibilidad con DNS, 89
- anuncio de enrutador, 164, 165, 168, 171
- aspectos sobre la seguridad, 41–42

**IPv6 (Continuación)**

- comando `nslookup`, 91
- comparación con IPv4, 168–170
- comprobar el estado de `in.ndpd`, 140
- configuración automática de direcciones, 160, 164
- configuración automática de direcciones sin estado, 165, 166
- configuración de direcciones temporales, 83–86
- daemon `in.ndpd`, 160
- daemon `in.ripngd`, 161
- descripción general de protocolo, 164
- descubrimiento de enrutador, 168
- descubrimiento de enrutadores, 160
- detección de inasequibilidad de vecinos, 169
- direcciones locales de vínculo, 166, 169
- direcciones multidifusión, 169
- enrutamiento, 170
- habilitar, en un servidor, 88–89
- plan de direcciones, 37–38
- preparación para admitir DNS, 40
- protocolo ND (Neighbor Discovery), 163–170
- redirección, 164, 169
- registros AAAA de DNS, 90
- resolución de problemas IPv6 comunes, 141
- resolver problemas IPv6 comunes, 140–142
- solicitud de enrutador, 164, 165
- solicitud de vecino, 164
- solicitud e inasequibilidad de vecinos, 166
- supervisar tráfico, 109–110
- tabla de directrices de selección de direcciones predeterminada, 156
- y filtro IP, 320–321

**K**

- keys, crear para SA IPsec, 243–245

**L**

- listas de revocación de certificados, *Ver* CRL

**M**

- mapa de tareas
  - IPQoS
    - planificar la configuración, 427
- mapas de tareas
  - configuración de IKE (mapa de tareas), 267
  - configuración de IKE con certificados de clave pública (mapa de tareas), 273
  - configuración de IKE con claves previamente compartidas (mapa de tareas), 268
  - configuración de IKE para sistemas portátiles (mapa de tareas), 290
- IPQoS
  - configuración de control de flujo, 483
  - creación de archivo de configuración, 447
  - planificación de política QoS, 432
- IPv6
  - planificar, 33–34
- Protección del tráfico con IPsec (mapa de tareas), 230
- tareas de administración de red, 94
- marca de clase de servicio (CoS), 419
- marcador `d\cosmk`, 419
  - etiquetas VLAN, 497
  - planificar el reenvío de datagramas, 441
  - valores de prioridad de usuario, tabla de, 497
- marcador `dscpmk`, 419
  - comportamientos PHB para el reenvío de paquetes, 495
  - invocar, en una instrucción `action de` marcador, 456, 462, 468, 471
  - planificar el reenvío de paquetes, 441
- mecanismos de protección, IPsec, 218–221
- medidor `tokenmt`, 418
  - configuración de presencia de color, 419
  - configuración de reconocimiento de colores, 493
  - medición de tasas, 492
- medidor de doble tasa, 493
- medidor de tasa única, 493
- parámetros de tasas, 492
- medidor `tswtclmt`, 418, 494
  - medición de tasas, 494
- mensajes, anuncio de enrutador, 171
- mensajes de error de IPQoS, 478

- metarranura, almacenamiento de claves, 299
- modelo administrativo, 188
- modelo administrativo de DHCPv6, 188
- modelo Diffserv
  - ejemplo de flujo, 420
  - implementación de IPQoS, 417
  - implementación IPQoS, 418, 419, 420
  - módulo clasificador, 417
  - módulos de marcador, 419
- módulo Diffserv, módulos de medidor, 418
- modo de ahorro de espacio, opción de daemon
  - in.routed, 148
- modo de transporte
  - datos protegidos con ESP, 222
  - IPsec, 221–223
- modo de túnel, IPsec, 221–223
- modo transporte, proteger datos con AH, 223
- modo túnel, proteger paquete IP interior
  - completo, 223
- módulo clasificador, 417
  - funciones de clasificador, 490
  - instrucción action, 452
- módulo flowacct, 419, 499
  - atributos de registros de flujo, 500
  - comando acctadm, para crear un archivo de control de flujo, 501
  - instrucción action de flowacct, 459
  - parámetros, 499
  - registros de flujo, 484
  - tabla de registro de flujo, 500
- módulos de marcado
  - Ver también* marcador dlcosmk
- módulos de marcador, 419
  - Ver también* marcador dlcosmk
  - Ver también* marcador dscpmk
  - compatibilidad con dispositivos VLAN, 497
  - especificar un punto de código DS, 497
  - PHB, para el reenvío de paquetes IP, 422
- módulos de medición
  - Ver también* medidor tokenmt
  - Ver también* medidor tswtclmt
  - introducción, 418
  - invocar, en el archivo de configuración IPQoS, 470
  - resultados de la medición, 418, 492

## N

### NAT

- configuración de reglas para, 317–318
- desactivar, 328
- descripción general, 317–318
- eliminación de reglas NAT, 338
- limitaciones con IPsec, 224–225
- reglas NAT
  - anexar, 338–339
  - ver, 337–338
- uso de IPsec e IKE, 294–295, 296–297
- ver estadísticas, 343–344

NIS, selección como servicio de nombres, 31

nombre de almacén de claves, *Ver* ID de token

nombre de directorio (DN), para acceder a CRL, 288

nombre de host, activar solicitud de cliente de, 200

nombres de dominio

- selección, 31
- servicio SMF nis/domain, 54, 55

nombres/denominación

- nombre de nodo
  - host local, 54

notación CIDR, 27

novedades

- protocolo SCTP, 71–74
- utilidad de gestión de servicios (SMF), 56

nuevas funciones

- comando inetconv, 56
- comando routeadm, 80
- configurar manualmente una dirección local de vínculo, 86–88
- DHCP en interfaces lógicas, 199
- direcciones temporales en IPv6, 83–86
- secuencias de eventos DHCP, 203–204
- selección de direcciones predeterminadas, 113–115

números de red de clase A, B y C, 27

## O

- omisión, IPsec en LAN, 240
- omitir, política IPsec, 221
- opción -a
  - comando ikecert, 285
  - comando ikecert certdb, 276, 281

- opción -a (*Continuación*)
    - comando `ikecert certrlb`, 290
  - opción -c
    - comando `ipseckey`, 255
    - daemon `in.iked`, 270
  - opción -D
    - comando `ikecert`, 306
    - comando `ikecert certlocal`, 275
  - opción -F, comando `ikecert certlocal`, 275
  - opción -f, daemon `in.iked`, 270
  - opción -L, comando `ipsecon`, 235
  - opción -l
    - comando `ikecert certdb`, 277
    - comando `ipsecon`, 235
  - opción -m, comando `ikecert certlocal`, 275
  - opción -q, daemon `in.routed`, 147
  - opción -S
    - comando `ikecert certlocal`, 275
    - daemon `in.routed`, 148
  - opción -s, comando `ping`, 102
  - opción -T
    - comando `ikecert certlocal`, 275
  - opción -t
    - comando `ikecert`, 306
    - comando `ikecert certlocal`, 275
  - opción -kc
    - comando `ikecert certlocal`, 280, 305
  - opción -ks
    - comando `ikecert certlocal`, 275, 305
- P**
- palabra clave `cert_root`
    - archivo de configuración de IKE, 282, 287
  - palabra clave `cert_trust`
    - archivo de configuración de IKE, 278, 286
    - comando `ikecert`, 305
  - palabra clave `ignore_crls`, archivo de configuración de IKE, 283
  - palabra clave `ldap-list`, archivo de configuración de IKE, 290
  - palabra clave `pkcs11_path`
    - descripción, 305
    - utilizar, 285
  - palabra clave proxy, archivo de configuración de IKE, 290
  - palabra clave `tunnel`
    - política IPsec, 222, 237, 240
  - palabra clave `use_http`, archivo de configuración IKE, 289
  - paquetes
    - comprobar flujo, 107
    - descartados o perdidos, 102
    - observación en la capa IP, 110–113
    - protección
      - con IPsec, 214
      - paquetes entrantes, 214
      - paquetes salientes, 214
    - proteger
      - con IKE, 260
      - con IPsec, 218–221
      - verificar protección, 248–249
      - visualizar contenido, 107
  - paquetes descartados o perdidos, 102
  - paquetes perdidos o descartados, 102
  - paquetes registrados, guardar en un archivo, 347–348
  - perfil de derechos de gestión de red IPsec, 246
  - perfil de derechos de seguridad de red, 245–246
  - perfiles de derechos
    - gestión de red, 246
    - gestión de red IPsec, 246
  - perfiles de derechos de gestión de red, 246
  - petición de comentarios (RFC), IPQoS, 413
  - PFS, *Ver* confidencialidad directa perfecta (PFS)
  - placa Sun Crypto Accelerator 6000, uso con IKE, 298–299
  - planificación de red
    - decisiones de diseño, 25
    - esquema de direcciones IP, 27
    - registro de red, 29
  - política de seguridad
    - archivo `ike/config` (IKE), 227
    - archivo `ipseconinit.conf` (IPsec), 252–254
    - IPsec, 221
  - política IPsec, ejemplos de sintaxis de túnel, 236–237
  - política QoS, 414
    - crear filtros, 436
    - plantilla para organizar la política, 431

- políticas, IPsec, 221
- prefijo de sitio, IPv6
  - advertir, en el enrutador, 81
  - obtención, 37
- prefijos
  - anuncio de enrutador, 165, 168, 171
- presencia de color, 419
- programa /usr/sbin/in.rdisc, descripción, 148
- programa in.rdisc, descripción, 148
- Protección del tráfico con IPsec (mapa de tareas), 230
- proteger
  - paquetes entre dos sistemas, 230–233
  - servidor web con IPsec, 233–235
  - sistemas portátiles con IPsec, 291–297
  - tráfico IPsec, 211
  - VPN con túnel IPsec en modo túnel, 239–242
- protocolo ARP (Address Resolution Protocol),
  - comparación con protocolo ND (Neighbor Discovery), 168–170
- protocolo BOOTP, y DHCP, 175
- protocolo de gestión de claves y asociación de seguridad de Internet (ISAKMP) asociaciones de seguridad,
  - descripción, 261
- protocolo de información de enrutamiento (RIP),
  - descripción, 147
- protocolo DHCP
  - descripción general, 175
  - secuencia de eventos, 177
  - ventajas en la implementación de Oracle Solaris, 176
- protocolo ICMP
  - invocar, con ping, 101
  - mensajes, para protocolo ND, 164
  - visualizar estadísticas, 95
- protocolo ICMP Router Discovery (RDISC), 148
- protocolo IP
  - comprobación de conectividad de host, 102
  - comprobar conectividad de host, 101
  - visualizar estadísticas, 95
- protocolo ND (Neighbor Discovery)
  - características principales, 163–170
  - comparación con ARP, 168–170
  - configuración automática de direcciones, 164
  - descubrimiento de enrutador, 165
  - protocolo ND (Neighbor Discovery) (*Continuación*)
    - descubrimiento de prefijo, 165
    - detección de direcciones duplicadas, 167
    - solicitud de vecino, 166
- protocolo RARP, comprobar direcciones Ethernet, 140
- protocolo SCTP
  - agregar servicios activados para SCTP, 71–74
  - IPsec y, 230
  - limitaciones con IPsec, 225
  - visualizar estadísticas, 95
  - visualizar estado, 97
- protocolo TCP, visualizar estadísticas, 95
- protocolo UDP, visualizar estadísticas, 95
- protocolos de enrutamiento
  - daemons de enrutamiento asociados, 148–149
  - descripción, 147, 148
- RDISC
  - descripción, 148
- RIP
  - descripción, 147
- protocolos de seguridad
  - carga de seguridad encapsuladora (ESP), 219–220
  - consideraciones de seguridad, 219
  - descripción general, 212
  - encabezado de autenticación (AH), 218
  - mecanismos de protección IPsec, 218
- protocolos TCP/IP, servicios estándar, 70
- próximo salto, 169
- puerta de enlace, en una topología de red, 59
- punto de código DS (DSCP), 419, 422
  - configuración de reconocimiento de color, 494
  - configurar, en un enrutador diffserv, 473, 495
  - definir, en el archivo de configuración IPQoS, 457
  - parámetro dscp\_map, 497
  - PHB y DSCP, 422
  - planificar, en la política QoS, 441
  - punto de código de reenvío AF, 423, 496
  - punto de código de reenvío EF, 496
  - punto de código de reenvío EF, 423

**Q**

- QoS, política
  - implementar en archivo de configuración IPQoS, 447
  - mapa de tareas de planificación, 432

**R**

- ranuras, del hardware, 307
- RBAC, IPsec y, 229
- RDISC, descripción, 148
- reconocimiento de colores, 493
- redes IPv4, archivos de configuración, 143
- redes privadas virtuales (VPN)
  - configuración con el comando `routeadm`, 239, 240
  - construidas con IPsec, 224
  - ejemplo de IPv4, 239–242
  - proteger con IPsec, 239–242
- redes TCP/IP
  - configuración
    - servicio SMF `name-service/switch`, 145
  - configurar
    - servicios TCP/IP estándar, 70
  - proteger con ESP, 219
  - resolución de problemas, 109
    - comando `netstat`, 95
    - comando `ping`, 101, 102
    - comprobaciones de software, 139
    - métodos generales, 139
    - pérdida de paquetes, 102
    - programas de diagnóstico de terceros, 139
    - visualizar contenido de paquetes, 107
- redirección
  - IPv6, 164, 169
- reemplazar, claves previamente compartidas (IKE), 270–271
- reenviar tráfico, planificar, en la política QoS, 435
- reenvío acelerado (EF), 423, 496
  - definir, en el archivo de configuración IPQoS, 458
- reenvío asegurado (AF), 423, 496
  - para una instrucción `action` de marcador, 457
  - tabla de puntos de código AF, 496
- reenvío de IP
  - en VPN, 224
  - reenvío de IP (*Continuación*)
    - en VPN IPv4, 239
  - reenvío de tráfico, efecto de comportamientos PHB en el reenvío de tráfico, 495
  - reenvío del tráfico
    - flujo del tráfico a través de redes Diffserv, 423
    - reenvío de datagramas, 497
    - reenvío de paquetes IP, con DSCP, 422
  - registro, redes, 29
  - registro de archivo `syslog.conf` para IPQoS, 477
  - registros AAAA, 90, 172
  - regulación del ancho de banda, 415
  - regular el ancho de banda, planificar, en la política QoS, 435
  - resolución
    - redes TCP/IP
      - supervisión de transferencia de paquetes en la capa IP, 110–113
  - resolución de problemas
    - carga útil de IKE, 284
    - comprobar vínculos de PPP
      - flujo de paquetes, 107
    - redes TCP/IP
      - comando `ping`, 102
      - comando `traceroute`, 105–107
      - comprobaciones de software, 139
      - comprobar paquetes entre cliente y servidor, 109
      - métodos generales, 139
      - observar transmisiones de interfaces, 97–98
      - obtener estadísticas por protocolo, 95–96
      - obtener estado del protocolo de transporte, 96–97
      - pérdida de paquetes, 102
      - programas de diagnóstico de terceros, 139
      - seguimiento de actividad de `in.ndpd`, 105
      - seguimiento de `in.routed`, 104
      - sondear hosts remotos con comando `ping`, 101
      - supervisar estado de red con comando `netstat`, 95
      - supervisar transferencia de paquetes con el comando `snoop`, 107
      - visualizar estado de rutas conocidas, 100–101
  - resolver
    - problemas IPv6, 140–142



roles, crear rol de seguridad de red, 245–246

## S

### seguridad

- IKE, 302

- IPsec, 211

seguridad de red, configurar, 209

selección de direcciones predeterminadas, 156–157

- definición, 113–115

- tabla de directrices de selección de direcciones

  - IPv6, 114–115

selectores, 418

- IPQoS 5-tuple, 417

- planificar, en la política QoS, 436

- selectores, lista de, 490

servicio de nombres de archivos locales, archivo

- /etc/inet/hosts, 231

servicio ike

- descripción, 218, 252

- uso, 232

servicio ipsecalgs, descripción, 251

servicio manual-key

- descripción, 218, 251

- uso, 245

servicio policy

- descripción, 251

- uso, 232

- utilizar, 241

servicio SMF /network/dhcp-server,

- descripción, 208

servicio SMF /network/dns/client, usado por

- DHCP, 208

servicio SMF /system/name-service/switch, usado

- por DHCP, 208

servicio SMF name-service/switch, 145

servicio SMF nis/tdomain, configuración de modo de

- archivos locales, 54

servicios

- IPsec

  - ipsecalgs, 227

servicios de nombres

- bases de datos de red y, 147

servicios de nombres (*Continuación*)

- especificación de orden de búsqueda de base de datos, 145

- selección de un servicio, 31

servicios diferenciados, 411

- distribuciones de red, 428

- modelo de servicios diferenciados, 417

- proporcionar diferentes clases de servicio, 416

servicios SMF, usados por DHCP, 208

servicios SMF /network/dhcp/relay, descripción, 208

servicios SMF /network/dhcp/server,

- descripción, 208

servidor, DHCPv6, 188

servidor de aplicaciones, configurar para IPQoS, 463

servidores, IPv6

- habilitar IPv6, 88–89

- planificación de tareas, 36

servidores de configuración de red, configuración, 55

servidores web

- configurar para IPQoS, 450, 451, 460, 462

- proteger con IPsec, 233–235

sistema autónomo (SA), *Ver* topología de red

sistema de nombres de dominio (DNS)

- archivo de zona, 89

- archivo de zona inversa, 89

- extensiones para IPv6, 172

- selección como servicio de nombres, 31

sistema nombres de dominio (DNS), preparar, para

- admitir IPv6, 40

sistemas, proteger comunicación, 230–233

sistemas de host múltiple, definición, 47

sockets

- seguridad IPsec, 253

- visualizar estado de sockets con netstat, 98

solicitud de enrutador

- IPv6, 164, 165

solicitud de vecino, IPv6, 164

solicitudes de certificados

- de autoridad de certificación, 280

- en hardware, 285

- utilizar, 306

solicitudes de comentarios (RFC)

- IKE, 213

- IPsec, 213



solicitudes de opciones, 191

subredes, 32

- agregar a una red IPv4, 68–70
- IPv4
  - configuración de máscara de red, 54
- IPv6
  - sugerencias de numeración, 38
  - topología 6to4 y, 121

**T**

opción -T

- comando `ikecert`, 285, 306

-t, opción, `daemon inetd`, 70

tabla de enrutamiento, 59

tabla de red DHCP, descripción, 207

tabla `dhcptab`, descripción, 207

tablas de enrutamiento

- configuración manual, 61
- creación de `daemon` de `in.routed`, 147
- modo de ahorro de espacio, 148
- seguimiento de todas las rutas, 106–107
- visualización, 139

tablas de estado, ver, 342

topología de red, sistema autónomo, 45

topologías de red para IPQoS, 428

traducción de direcciones de red (NAT), *Ver* NAT

Trusted Extensions, IPsec y, 230

túneles, 117–138

- comandos `dladm`
  - `create-iptun`, 127–131
  - `delete-iptun`, 138
  - `modify-iptun`, 135–136
  - `show-iptun`, 136–137
  - subcomandos para configurar túneles, 126
- configuración con comandos `dladm`, 126–138
- configuración de IPv4 en túneles IPv4, 130
- configuración de IPv6 en túneles IPv4, 130
- configuración de IPv6 en túneles IPv6, 131
- configuración de túneles 6to4, 132
- configurar IPv6
  - en enrutador de reenvío 6to4, 133
- creación y configuración de túneles, 127–131

túneles (*Continuación*)

- dirección de destino del túnel
  - Ver* túneles, *dst*
- dirección de origen del túnel
  - Ver* túneles, *src*
- direcciones locales y remotas, 135
- encaplimit, 128
- encapsulación de paquetes, 118
- hoplimit, 128
- implementación, 124–125
- interfaces IP necesarias, 125
- IPsec, 224
- IPv4, 118–119
- IPv6, 118–119
- mecanismos de creación de túneles IPv6, 118
- modificación de la configuración de un
  - túnel, 135–136
- modo transporte, 221
- modo túnel, 222
- modos en IPsec, 221–223
- planificar, para IPv6, 41
- proteger paquetes, 224
- requisitos para la creación, 124–125
- supresión de túneles IP, 138
- tipos, 118
  - 6to4, 118
  - IPv4, 118
  - IPv4 en IPv4, 118
  - IPv4 en IPv6, 118
  - IPv6, 118
  - IPv6 en IPv4, 118
  - IPv6 en IPv6, 118
- topología, a enrutador de relé 6to4, 123
- túneles 6to4, 119
  - flujo de paquetes, 121, 123
  - topología, 120
- visualización de información de túnel, 136–137
- VPN
  - Ver* redes privadas virtuales (VPN)

túneles 6to4

- Ver también* túneles, tipos
- enrutador de reenvío 6to4, 133
- flujo de paquetes, 121, 123
- topología de ejemplo, 120

túneles IP, *Ver* túneles  
 túneles IPv4, *Ver* túneles, tipos  
 túneles IPv6, *Ver* túneles, tipos

## U

unidad de transmisión máxima (MTU), 169  
 utilidad de gestión de claves (SMF)  
     servicios IPsec  
         descripción manual-key, 218  
 utilidad de gestión de servicios (SMF)  
     servicio IKE  
         descripción, 301–302  
         habilitación, 232, 294, 302  
         propiedades configurables, 301  
         refrescamiento, 245  
         reinicio, 232  
         servicio ike, 218, 263  
 servicios IPsec, 251–252  
     lista de, 226–227  
     servicio ipsecalgs, 254  
     servicio manual-key, 255  
     servicio policy, 227  
     uso de manual-key, 245  
     uso para gestionar IKE, 247–248  
     uso para gestionar IPsec, 247–248  
 utilidades de claves  
     comando ipseckey, 218  
     protocolo IKE, 259  
     servicio ike, 218  
     servicio manual-key, 218  
 utilidades de línea de comandos de DHCP,  
     privilegios, 183

## V

opción -V, comando snoop, 257  
 vaciar, *Ver* eliminar  
 valor de prioridad de usuario, 419  
 varias interfaces de red, sistemas cliente DHCP, 199  
 verificación  
     archivo ipsecinit.conf  
         sintaxis, 241

verificación (*Continuación*)  
     archivo ipseckey  
         sintaxis, 245  
 verificar  
     archivo ipsecinit.conf  
         sintaxis, 232  
     protección de paquetes, 248–249  
 vínculos de datos, configuración de una interfaz IP  
     desde un vínculo, 48  
 vínculos de PPP  
     resolución de problemas  
         flujo de paquetes, 107  
 visualización, configuración IPsec, 252–254  
 visualizar  
     política IPsec, 235  
 visualizar estadísticas de protocolo, 95  
 VPN, *Ver* redes privadas virtuales (VPN)

## Z

zonas  
     gestión de claves y, 229  
     IPsec y, 226, 229