Guide d'administration système : services IP

Référence : 820–2982–18
Août 2011

ORACLE

111013@25097

Table des matières

Préface

Le *System Administration Guide, IP Services* fait partie de l'un des neuf volumes traitant en grande partie de l'administration de système Oracle Solaris. Ce manuel suppose que vous avez déjà installé Oracle Solaris 10. Vous devez être prêt à configurer votre réseau ou tout logiciel de gestion de réseau requis. Oracle Solaris 10 fait partie de la famille de produits Oracle Solaris, comprenant notamment Java Desktop System. Oracle Solaris est compatible avec la version 4 du système d'exploitation System V d'AT&T.

Remarque – Cette version d'Oracle Solaris prend en charge les systèmes utilisant les architectures de processeur SPARC et x86. Les systèmes pris en charge sont répertoriés dans les listes de la page *Oracle Solaris OS: Hardware Compatibility Lists*. Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

Dans ce document, les termes relatifs à x86 ont la signification suivante :

- x86 désigne la famille des produits compatibles x86 64 bits et 32 bits.
- x64 concerne spécifiquement les UC compatibles x86 64 bits.
- x86 32 bits désigne des informations 32 bits spécifiques relatives aux systèmes x86.

Pour connaître les systèmes pris en charge, reportez-vous aux listes de la page *Oracle Solaris OS: Hardware Compatibility Lists*.

Utilisateurs de ce manuel

Ce document s'adresse aux administrateurs de systèmes réseau exécutant Oracle Solaris. Pour utiliser ce manuel, vous devez avoir au moins deux ans d'expérience en administration de systèmes UNIX. Une formation en administration de systèmes UNIX peut se révéler utile.

Organisation des guides d'administration système

La liste des différents sujets traités par les guides d'administration système est la suivante.

Titre du manuel	Sujets
Guide d'administration système : administration de base	Comptes et groupes d'utilisateur, prise en charge de serveur et de client, arrêt et initialisation d'un système et gestion des services
Guide d'administration système : Administration avancée	Terminaux et modems, ressources système (quotas d'utilisation de disque, comptabilisation et crontabs), processus système et dépannage du logiciel Oracle Solaris
System Administration Guide: Devices and File Systems	Médias amovibles, disques et périphériques, systèmes de fichiers, et sauvegarde et restauration des données
Guide d'administration système : services IP	Administration de réseau TCP/IP, administration d'adresses IPv4 et IPv6, DHCP, IPsec, IKE, filtre IP, IP mobile, multiacheminement sur réseau IP (IPMP) et IPQoS
Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)	Services d'annuaire et d'attribution de noms DNS, NIS et LDAP, et transition de NIS à LDAP et de NIS+ à LDAP
System Administration Guide: Naming and Directory Services (NIS+)	Services d'annuaire et d'attribution de noms NIS+
Guide d'administration système : Services réseau	Serveurs cache Web, services à facteur temps, systèmes de fichiers de réseau (NFS et Autofs), mail, SLP et PPP
System Administration Guide: Printing	Tâches et sections concernant l'impression, l'utilisation des services, les outils, protocoles et technologies permettant de configurer et de gérer les imprimantes et services d'impression
System Administration Guide: Security Services	Audit, gestion des périphériques, sécurité des fichiers, BART, services Kerberos, PAM, structure cryptographique Oracle Solaris, privilèges, RBAC, SASL et shell sécurisé Oracle Solaris
Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris	Gestion des ressources pour les projets et les tâches, comptabilisation étendue, contrôles de ressources, ordonnanceur FSS, contrôle de la mémoire physique à l'aide du démon d'allocation restrictive des ressources (rcapd) et pools de ressources ; virtualisation au moyen de la technologie de partitionnement du logiciel Solaris Zones et des zones marquées `lx`
Guide d'administration Oracle Solaris ZFS	Création et gestion de pools de stockage et de systèmes de fichiers ZFS, instantanés, clones, sauvegardes à l'aide de listes de contrôle d'accès (ACL) pour protéger les fichiers ZFS, utilisation de Solaris ZFS sur un système Solaris avec des zones installées, volumes émulés et dépannage et récupération de données

Titre du manuel	Sujets
Procédures de l'administrateur Oracle Solaris Trusted Extensions	Administration système spécifique aux fonctionnalités d'extension sécurisée d'Oracle Solaris
Guide de configuration d'Oracle Solaris Trusted Extensions	À partir de la version Solaris 10 5/08, ce guide décrit la planification, l'activation et la configuration initiale de la fonction d'extension sécurisée d'Oracle Solaris.

Documentation connexe

Ce manuel fait référence aux ouvrages suivants.

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

Références connexes aux sites Web de logiciels tiers

Des URL de sites tiers, qui renvoient à des informations complémentaires connexes, sont référencés dans ce document.

Remarque – Sun ne saurait être tenu responsable de la disponibilité des sites Web tiers mentionnés dans ce manuel. Sun décline toute responsabilité quant au contenu, à la publicité, aux produits ou tout autre matériel disponibles dans ou par l'intermédiaire de ces sites ou ressources. Sun ne pourra en aucun cas être tenu responsable, directement ou indirectement, de tous dommages ou pertes, réels ou invoqués, causés par ou liés à l'utilisation des contenus, biens ou services disponibles dans ou par l'intermédiaire de ces sites ou ressources.

IP Filter dans Oracle Solaris est dérivé du logiciel Open Source IPFilter. Les conditions de licence, attribution et déclarations de copyright sont accessibles via le chemin par défaut `/usr/lib/ipf/IPFILTER.LICENCE`. Si vous avez installé Oracle Solaris dans un autre emplacement que celui par défaut, modifiez le chemin afin d'accéder au fichier se trouvant à l'emplacement de l'installation.

Accès au support technique Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, rendez-vous sur le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou sur le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Conventions typographiques

Le tableau ci-dessous décrit les conventions typographiques utilisées dans ce manuel.

TABLEAU P–1 Conventions typographiques

Type de caractères	Signification	Exemple
`AaBbCc123`	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez votre fichier `.login`. Utilisez `ls -a` pour afficher la liste de tous les fichiers. `nom_machine% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	`nom_machine%` **`su`** `Mot de passe :`
aabbcc123	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est `rm` *nom_fichier*.
AaBbCc123	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie des éléments stockés localement. *N'enregistrez pas* le fichier. **Remarque :** en ligne, certains éléments mis en valeur s'affichent en gras.

Invites de shell dans les exemples de commandes

Le tableau suivant présente l'invite système UNIX par défaut et l'invite superutilisateur pour les shells faisant partie du SE Oracle Solaris. L'invite système par défaut qui s'affiche dans les exemples de commandes dépend de la version Oracle Solaris.

TABLEAU P–2 Invites de shell

Shell	Invite
Shell Bash, shell Korn et shell Bourne	`$`
Shell Bash, shell Korn et shell Bourne pour superutilisateur	`#`
C shell	`nom_machine%`
C shell pour superutilisateur	`nom_machine#`

PARTIE I

Introduction à l'administration système : services IP

Cette section contient des informations présentant la suite du protocole TCP/IP et son implémentation dans Oracle Solaris.

◆ ◆ ◆ CHAPITRE 1

1 Suite de protocoles réseau TCP/IP Oracle Solaris (présentation)

Ce chapitre décrit l'implémentation de la suite de protocoles réseau TCP/IP sur Oracle Solaris. Ces informations sont destinées aux administrateurs système et réseau ne connaissant pas les concepts TCP/IP de base. Les autres parties de ce manuel s'adressent aux lecteurs ayant connaissance de ces concepts.

Le présent chapitre contient les informations suivantes :

Nouveautés dans cette version

À partir de Solaris 10 5/08, la fonction Mobile IP est supprimée. Le composant Mobile IP est disponible dans le SE Solaris 10, version 8/07 et les versions précédentes.

Introduction à la suite de protocoles TCP/IP

Cette section présente en détail les protocoles inclus dans TCP/IP. Les informations sont de nature conceptuelle, mais il est conseillé de connaître les noms des protocoles, ainsi que les opérations effectuées par chacun d'eux.

L'acronyme TCP/IP est généralement utilisé pour désigner la suite de protocoles réseau composant la *suite de protocoles Internet*. Le terme Internet est souvent utilisé pour désigner à la fois la suite de protocoles et le WAN (Wide Area Network, réseau étendu) mondial. Dans ce manuel, TCP/IP fait référence à la suite de protocoles Internet. Le terme Internet fait référence au WAN mondial et aux entités qui gouvernent Internet.

Pour connecter votre réseau TCP/IP à d'autres réseaux, vous devez obtenir une adresse IP unique pour votre réseau. Au moment de la rédaction de ce manuel, cette adresse est disponible auprès d'un fournisseur de services Internet (ISP, Internet Service Provider).

Si les hôtes du réseau doivent participer au DNS (Domain Name System, système de noms de domaine) Internet, vous devez obtenir et enregistrer un nom de domaine unique. L'InterNIC coordonne l'enregistrement des noms de domaine via un groupe de registres mondiaux. Pour plus d'informations sur le DNS, reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Couches de protocoles et modèle OSI

En général, les suites de protocoles réseau sont structurées sous forme d'une série de couches, parfois appelée *pile de protocoles*. Chaque couche correspond à un objectif spécifique. Chaque couche existe à la fois sur le système émetteur et sur le système récepteur. Une couche spécifique sur un système envoie ou reçoit un objet identique à celui que le *processus homologue* d'un autre système envoie ou reçoit. Ces opérations s'exécutent indépendamment des opérations effectuées dans les couches supérieures ou inférieures. Par définition, chaque couche du système agit indépendamment des autres couches du système. Chaque couche agit parallèlement à la couche identique sur les autres systèmes.

Modèle de référence OSI

La plupart des suites de protocoles réseau sont structurées en couches. L'organisation internationale de normalisation (ISO, International Organization for Standardization) a conçu le modèle de référence OSI (Open Systems Interconnection, interconnexion de systèmes ouverts) qui utilise des couches structurées. Le modèle OSI décrit une structure constituée de sept couches représentant les activités du réseau. Un ou plusieurs protocoles sont associés à chaque couche. Les couches représentent les opérations de transfert de données communes à tous les types de transfert de données sur des réseaux coopératifs.

Le modèle OSI répertorie les couches de protocoles de haut (couche 7) en bas (couche 1). Le tableau ci-dessous présente le modèle.

TABLEAU 1–1 Modèle de référence OSI

No. de couche	Nom de couche	Description
7	Application	Applications et services de communication standard à la disposition de tous les utilisateurs.
6	Présentation	Vérifie que les informations sont bien reçues par le système récepteur dans un format compréhensible pour celui-ci.
5	Session	Gère les connexions et interruptions entre les systèmes coopératifs.
4	Transport	Gère le transfert des données. Vérifie également que les données reçues sont identiques aux données transmises.
3	Réseau	Gère l'adressage et la distribution des données sur les différents réseaux.

TABLEAU 1–1 Modèle de référence OSI *(Suite)*

No. de couche	Nom de couche	Description
2	Liaison de données	Prend en charge le transfert des données via le média réseau.
1	Physique	Définit les caractéristiques du matériel réseau.

Le modèle OSI définit les opérations conceptuelles non spécifiques à une suite de protocoles réseau particulière. Par exemple, la suite de protocoles réseau OSI implémente les sept couches du modèle OSI. TCP/IP utilise certaines couches du modèle OSI. TCP/IP combine également d'autres couches. D'autres protocoles réseau, tels que SNA, ajoutent une huitième couche.

Modèle d'architecture de protocoles TCP/IP

Le modèle OSI décrit les processus de communication réseau idéaux à l'aide d'une famille de protocoles. TCP/IP ne correspond pas exactement à ce modèle. TCP/IP combine plusieurs couches OSI en une couche unique et n'utilise pas certaines couches. Le tableau suivant indique les couches de l'implémentation de la suite de protocoles réseau TCP/IP sur Oracle Solaris. Les couches sont répertoriées de la couche la plus haute (application) à la couche la plus base (réseau physique).

TABLEAU 1–2 Pile de protocoles TCP/IP

OSI Réf. No. de couche	Couche OSI équivalente	Couche TCP/IP	Exemples de protocoles TCP/IP
5,6,7	Application, session, présentation	Application	NFS, NIS, DNS, LDAP, `telnet`, `ftp`, `rlogin`, `rsh`, `rcp`, RIP, RDISC, SNMP, etc.
4	Transport	Transport	TCP, UDP, SCTP
3	Réseau	Internet	IPv4, IPv6, ARP, ICMP
2	Liaison de données	Liaison de données	PPP, IEEE 802.2
1	Physique	Réseau physique	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI, etc.

Le tableau répertorie les couches de protocoles TCP/IP et les couches équivalentes dans le modèle OSI. Il indique également des exemples de protocoles disponibles à chaque niveau de la pile de protocoles TCP/IP. Chaque système impliqué dans une transaction de communication exécute une implémentation unique de la pile de protocoles.

Couche réseau physique

La *couche réseau physique* spécifie les caractéristiques du matériel à utiliser pour le réseau. Par exemple, une couche réseau physique spécifie les caractéristiques physiques du média de communications. La couche physique de TCP/IP décrit les standards matériels tels que IEEE 802.3, la spécification du média réseau Ethernet et RS-232, spécification dédiée aux connecteurs à broche standard.

Couche de liaison de données

La *couche de liaison de données* identifie le type de protocole réseau du paquet, dans cette instance TCP/IP. En outre, cette couche de liaison de données assure le contrôle des erreurs et l'"encadrement". Par exemple, les encadrements Ethernet IEEE 802.2 et PPP (Point-to-Point Protocol, protocole point à point) constituent des protocoles de couche de liaison de données.

Couche Internet

La couche Internet, également appelée *couche réseau* ou *couche IP*, accepte et distribue les paquets pour le réseau. Cette couche inclut le puissant protocole Internet (IP, Internet Protocol), le protocole ARP (Address Resolution Protocol, protocole de résolution d'adresse) et le protocole ICMP (Internet Control Message Protocol, protocole de message de contrôle Internet).

Protocole IP

Le protocole IP et les protocoles de routage associés sont sûrement les protocoles les plus importants de la suite TCP/IP. IP prend en charge les opérations suivantes :

- **Adressage IP** : les conventions d'adressage IP appartiennent au protocole IP. L'adressage IPv4 est décrit à la section “Conception d'un schéma d'adressage IPv4” à la page 58 et l'adressage IPv6 est décrit à la section “Présentation de l'adressage IPv6” à la page 76.
- **Communications d'hôte à hôte** : IP détermine le chemin qu'un paquet doit utiliser en fonction de l'adresse IP du système récepteur.
- **Formatage de paquet** : IP rassemble les paquets en unités appelées *datagrammes*. Les datagrammes sont décrits en détail à la section “Couche Internet : préparation des paquets pour la distribution” à la page 47.
- **Fragmentation** : si un paquet est trop volumineux pour être transmis via le média réseau, le protocole IP sur le système émetteur scinde le paquet en fragments plus petits. Ensuite, le protocole IP du système récepteur réunit les fragments pour reconstituer le paquet d'origine.

Oracle Solaris prend en charge les formats d'adressage IPv4 et IPv6 décrits dans ce manuel. Pour éviter toute confusion lors de l'adressage du protocole IP, l'une des conventions ci-dessous est appliquée :

- Lorsque le terme IP est employé dans une description, la description s'applique à IPv4 et à IPv6.
- Lorsque le terme IPv4 est employé dans une description, la description s'applique exclusivement à IPv4.
- Lorsque le terme IPv6 est employé dans une description, la description s'applique exclusivement à IPv6.

Protocole ARP

Conceptuellement, le protocole ARP (Address Resolution Protocol, protocole de résolution d'adresse) existe entre la couche de liaison de données et la couche Internet. ARP permet à IP de diriger les datagrammes vers le système récepteur adéquat en mappant les adresses Ethernet (48 bits) vers des adresses IP connues (32 bits).

Protocole ICMP

Le protocole ICMP (Internet Control Message Protocol, protocole de message de contrôle Internet) détecte et signale les conditions d'erreur réseau. ICMP génère des rapports sur :

- **Paquets abandonnés** : paquets arrivant trop rapidement pour être traités ;
- **un échec de connectivité** : le système de destination est inaccessible ;
- **la redirection** : redirection d'un système émetteur vers un autre routeur.

Pour plus d'informations sur les commandes Oracle Solaris utilisant le composant ICMP pour la détection d'erreurs, reportez-vous au Chapitre 8, “Gestion d'un réseau TCP/IP (tâches)”.

Couche transport

La *couche transport* TCP/IP assure l'arrivée des paquets dans l'ordre et sans erreur, en échangeant les accusés de réception de données et en retransmettant les paquets perdus. Cette communication est dite de type *de bout en bout*. Les protocoles de la couche transport à ce niveau sont TCP (Transmission Control Protocol, protocole de contrôle de la transmission), UDP (User Datagram Protocol, protocole de datagramme utilisateur) et SCTP (Stream Control Transmission Protocol, protocole de transmission de contrôle de flux). TCP et SCTP assurent des services de bout en bout fiables. UDP assure des services de datagramme peu fiables.

Protocole TCP

TCP permet aux applications de communiquer les unes avec les autres comme si elles étaient physiquement connectées. TCP semble transmettre les données caractère par caractère, non sous forme de paquets individuels. Cette transmission s'effectue comme suit :

- point de départ, qui initialise la connexion ;
- transmission dans l'ordre des octets ;
- point d'arrivée, qui interrompt la connexion.

TCP joint un en-tête aux données transmises. Cet en-tête contient de nombreux paramètres qui facilitent la connexion des processus du système émetteur aux processus homologues du système récepteur.

TCP confirme l'arrivée du paquet à destination en établissant une connexion de bout en bout entre les hôtes émetteur et récepteur. TCP est donc considéré comme un protocole "fiable et orienté connexion".

Protocol SCTP

SCTP est un protocole de couche transport fiable et orienté connexion. Il fournit aux applications les mêmes services que TCP. De plus, SCTP peut prendre en charge les connexions entre les systèmes possédant plusieurs adresses, ou *multiréseau*. La connexion SCTP entre les systèmes émetteur et récepteur est appelée *association*. Dans l'association, les données sont classées en blocs. Comme SCTP prend en charge les systèmes multiréseau, certaines applications, notamment des applications employées dans le secteur des télécommunications, doivent s'exécuter sur SCTP, non TCP.

Protocole UDP

UDP assure la distribution de datagramme. UDP ne vérifie pas les connexions entre les hôtes émetteur et récepteur. Comme UDP élimine les processus d'établissement et de vérification des connexions, les applications qui envoient des petites quantités de données utilisent UDP.

Couche d'application

La *couche d'application* définit les services Internet standard et les applications réseau à la disposition des utilisateurs. Ces services fonctionnent conjointement avec la couche transport pour assurer l'envoi et la réception de données. il existe de nombreux protocoles de couche d'application. Des exemples de protocoles de couche d'application sont répertoriés ci-dessous :

- services TCP/IP standard, tels que les commandes `ftp`, `tftp` et `telnet` ;
- commandes UNIX "r", telles que `rlogin` et `rsh` ;
- services de noms, tels que NIS et le DNS (Domain Name System, système de noms de domaine) ;
- services d'annuaire (LDAP, Lightweight Directory Access Protocol, protocole d'accès annuaire léger) ;
- services de fichier, tels que le service NFS ;
- SNMP (Simple Network Management Protocol, protocole de gestion de réseau simple), pour la gestion de réseau ;
- protocoles de routage RDISC (Router Discovery Server protocol, protocole serveur de détecteur de routeur) et RIP (Routing Information Protocol, protocole d'informations de routage).

Services TCP/IP standard

- **FTP et FTP anonyme** : FTP (File Transfer Protocol, protocole de transfert de fichier) transfère les fichiers vers un réseau distant et en provenance de celui-ci. Le protocole inclut la commande `ftp` et le démon `in.ftpd`. FTP permet à l'utilisateur de spécifier le nom de l'hôte distant et les options de commande de transfert de fichier sur la ligne de commande de l'hôte local. Ensuite, sur l'hôte distant, le démon `in.ftpd` gère les requêtes envoyées par l'hôte local. Contrairement à `rcp`, `ftp` fonctionne même si l'ordinateur distant n'exécute pas un système d'exploitation UNIX. Un utilisateur doit se connecter au système distant afin d'établir une connexion `ftp`, sauf si la configuration du système distant autorise le FTP anonyme.

  Vous pouvez obtenir une grande quantité de documents à partir des *serveurs FTP anonymes* connectés à Internet. Les universités et d'autres institutions configurent ces serveurs de manière à mettre des logiciels, des articles scientifiques et d'autres informations à la disposition du public. Lorsque vous vous connectez à ce type de serveur, vous utilisez le nom de connexion `anonymous`, d'où l'appellation "serveur FTP anonyme".

  Ce manuel n'a pas pour objectif de décrire l'utilisation du FTP anonyme et la configuration de serveurs FTP anonymes. Toutefois, de nombreux manuels, tels que *Le monde Internet : guide et ressources*, décrivent le FTP anonyme en détail. Le *Guide d'administration système : Services réseau* fournit les instructions d'utilisation de FTP. La page de manuel `ftp(1)` décrit toutes les options de commande `ftp` appelées via l'interpréteur de commandes. La page de manuel `ftpd(1M)` décrit les services assurés par le démon `in.ftpd`.

- **Telnet** : le protocole Telnet permet la communication des terminaux et processus de terminaux sur un réseau exécutant TCP/IP. Ce protocole est implémenté en tant que programme `telnet` sur les systèmes locaux et le démon `in.telnetd` sur les machines distantes. Telnet fournit une interface utilisateur via laquelle deux hôtes peuvent communiquer caractère par caractère ou ligne par ligne. Telnet inclut des commandes intégralement documentées dans la page de manuel `telnet(1)`.

- **TFTP** : le protocole `tftp` (Trivial File Transfer Protocol, protocole simplifié de transfert de fichiers) assure des fonctions similaires à `ftp`, sans établir la connexion interactive de `ftp`. Par conséquent, les utilisateurs ne peuvent pas répertorier le contenu d'un répertoire ni modifier les répertoires. L'utilisateur doit connaître le nom complet du fichier à copier. Les commandes `tftp` sont décrites dans la page de manuel `tftp(1)`.

Commandes UNIX "r"

Les commandes UNIX "r" permettent d'exécuter des commandes sur une machine locale s'exécutant sur l'hôte distant, notamment :

- `rcp` ;
- `rlogin` ;
- `rsh`.

Les pages de manuel `rcp(1)`, `rlogin(1)` et `rsh(1)` fournissent les instructions d'utilisation de ces commandes.

Services de noms

Oracle Solaris fournit les services de noms suivants :

- **DNS** : le DNS (Domain Name System, système de noms de domaine) est le service de noms fournit par Internet pour les réseaux TCP/IP. DNS fournit les noms d'hôtes au service d'adresses IP. DNS est également utilisé comme base de données pour la gestion des messages. Vous trouverez une description complète de ce service dans le *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*. Reportez-vous également à la page de manuel `resolver`(3RESOLV).
- `Fichiers` **/etc** : le système de noms UNIX basé sur l'hôte d'origine a été développé pour les machines UNIX autonomes, puis adapté pour l'utilisation en réseau. De nombreux ordinateurs et systèmes d'exploitation UNIX anciens utilisent encore ce système, mais il n'est pas adapté aux réseaux complexes de grande amplitude.
- **NIS** : NIS (Network Information Service, service d'information réseau) a été développé indépendamment de DNS et son objectif n'est pas tout à fait le même. DNS a pour but de simplifier les communications grâce à l'utilisation de noms de machine au lieu d'adresses IP numériques ; NIS a pour but de faciliter l'administration réseau en centralisant le contrôle de nombreuses informations réseau. NIS conserve les informations sur les adresses et noms de machines, les utilisateurs, le réseau et les services réseau. Les informations d'espace de noms NIS sont conservées dans les cartes NIS. Pour plus d'informations sur l'architecture NIS et l'administration NIS, reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Service d'annuaire

Oracle Solaris prend en charge le protocole LDAP (Lightweight Directory Access Protocol, protocole d'accès annuaire léger) en conjonction avec le serveur d'annuaire Sun Open Net Environment (Sun ONE), ainsi que d'autres serveurs d'annuaire LDAP. La distinction entre un service de noms et un service d'annuaire réside dans l'étendue des fonctionnalités. Un service d'annuaire assure toutes les fonctionnalités d'un service de noms, ainsi que des fonctionnalités supplémentaires. Reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Services de fichier

Le protocole de couche d'application NFS fournit des services de fichier pour Oracle Solaris. Vous trouverez les informations complètes sur le service NFS dans le *Guide d'administration système : Services réseau*.

Administration de réseaux

Le protocole SNMP (Simple Network Management Protocol, protocole de gestion réseau simple) permet d'afficher la configuration du réseau et le statut des machines-clés. SNMP permet également d'obtenir des statistiques réseau complexes à partir d'un logiciel basé sur une interface graphique. De nombreuses sociétés offrent des packages de gestion réseau qui implémentent SNMP.

Protocoles de routage

Les protocoles de routage RIP (Routing Information Protocol, protocole d'informations de routage) et RDISC (Router Discovery Server Protocol, protocole de serveur de détection de routeur) sont disponibles pour les réseaux TCP/IP. Pour obtenir la liste complète des protocoles de routage pour Oracle Solaris 10, reportez-vous au Tableau 5–1 et au Tableau 5–2.

Gestion des communications de données par le protocole TCP/IP

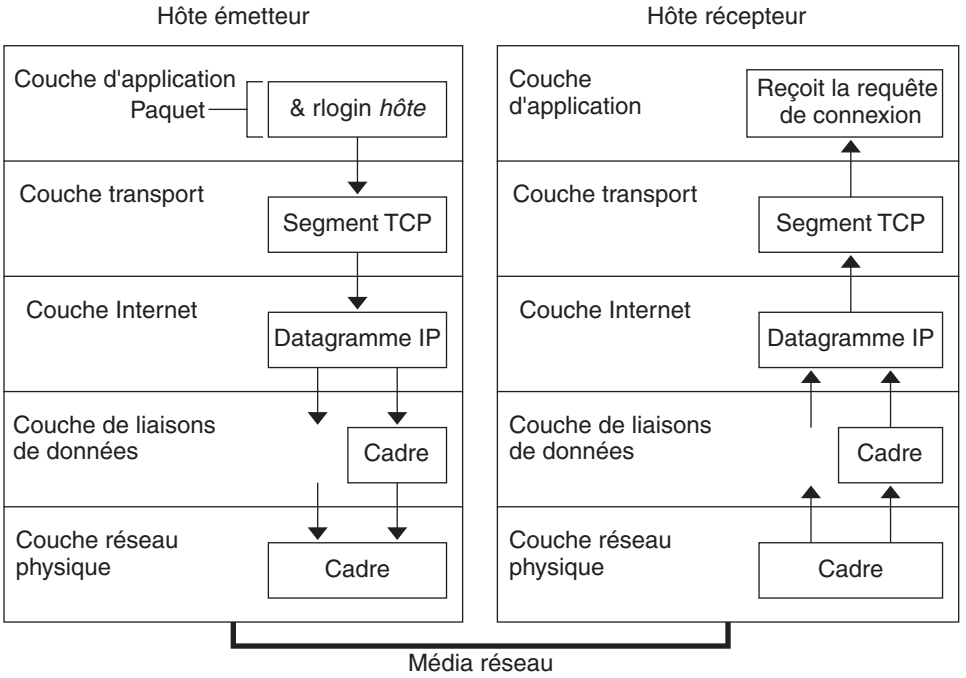
Lorsqu'un utilisateur exécute une commande utilisant un protocole de couche d'application TCP/IP, une série d'événements se lance. La commande ou le message de l'utilisateur passe dans la pile de protocoles TCP/IP sur le système local. Ensuite, la commande ou le message passe via le média réseau aux protocoles sur le système distant. Les protocoles de chaque couche de l'hôte émetteur ajoutent des informations aux données d'origine.

Les protocoles de chaque couche de l'hôte émetteur interagissent également avec leurs homologues sur l'hôte récepteur. La Figure 1–1 illustre cette interaction.

Encapsulation de données et pile de protocoles TCP/IP

Le paquet est l'unité d'information de base transférée via le réseau. Le paquet de base consiste en un en-tête avec les adresses des systèmes émetteur et récepteur, ainsi qu'un corps, ou *champ de données*, avec les données à transférer. Lorsque le paquet parcourt la pile de protocoles TCP/IP, les protocoles de chaque couche ajoutent ou suppriment des champs de l'en-tête de base. Lorsqu'un protocole sur le système émetteur ajoute des données à l'en-tête du paquet, le processus s'appelle *encapsulation de données*. De plus, chaque couche possède un terme différent pour le paquet modifié, comme indiqué dans la figure suivante.

FIGURE 1–1 Parcours d'un paquet dans une pile TCP/IP



Cette section résume le cycle de vie d'un paquet. Le cycle de vie commence à l'exécution d'une commande ou à l'envoi d'un message. Le cycle de vie se termine lorsque l'application adéquate sur le système récepteur reçoit le paquet.

Couche d'application : origine d'une communication

L'historique d'un paquet commence lorsqu'un utilisateur ou un système envoie un message ou exécute une commande devant accéder à un système distant. Les protocoles d'application formatent le paquet afin que le protocole de couche de transport adéquat, TCP ou UDP, puisse gérer le paquet.

Supposons que l'utilisateur exécute la commande `rlogin` afin de se connecter au système distant, comme indiqué sur la Figure 1–1. La commande `rlogin` utilise le protocole de couche transport TCP. TCP attend la réception de données sous forme d'un flux d'octets contenant les informations dans la commande. Par conséquent, `rlogin` envoie ces données sous la forme d'un flux TCP.

Couche transport : début de l'encapsulation des données

Lorsque les données atteignent la couche transport, les protocoles de la couche commencent le processus d'encapsulation des données. La couche transport encapsule les données d'application dans les unités de données du protocole de transport.

Le protocole de couche transport crée un flux de données virtuel entre l'application émettrice et l'application réceptrice, différenciées par le numéro de port de transport. Le numéro de port identifie un *port*, emplacement mémoire dédié à la réception et à l'envoi de données. En outre, la couche de protocole transport peut assurer d'autres services, tels que la distribution fiable de données ordonnées. Le résultat final dépend de la méthode de gestion des informations appliquée par TCP, SCTP ou UDP.

Segmentation TCP

TCP est considéré comme un protocole "orienté connexion", car il assure la distribution des données à l'hôte récepteur sans erreur. La Figure 1–1 indique comment le protocole TCP reçoit le flux de données à partir de la commande `rlogin`. Ensuite, TCP scinde les données reçues de la couche d'application en segments et joint un en-tête à chaque segment.

Les en-têtes de segment contiennent les ports émetteurs et récepteurs, des informations de classement des segments et un champ de données correspondant à la *somme de contrôle*. Les protocoles TCP des deux hôtes utilisent les données de somme de contrôle pour déterminer si le transfert s'est correctement effectué.

Établissement d'une connexion TCP

TCP utilise les segments pour déterminer si le système récepteur est prêt à recevoir les données. Lorsque le protocole TCP de l'hôte émetteur souhaite établir les connexions, il envoie un segment appelé *SYN* au protocole TCP de l'hôte récepteur. Le TCP récepteur renvoie un segment appelé *ACK* afin d'accuser la réception du segment. Le TCP émetteur envoie un autre segment ACK, puis initialise l'envoi des données. Cet échange d'informations de contrôle est appelé *négociation en trois étapes*.

Paquets UDP

UDP est un protocole "sans connexion". Contrairement à TCP, UDP ne vérifie pas que les données sont bien arrivées à l'hôte récepteur. Au lieu de cela, UDP formate le message reçu de la couche d'application en *paquets UDP*. Le protocole joint un en-tête à chaque paquet. L'en-tête contient les ports émetteur et récepteur, un champ spécifiant la longueur du paquet et une somme de contrôle.

Le processus UDP émetteur tente d'envoyer le paquet au processus UDP homologue sur l'hôte récepteur. La couche d'application détermine si le processus UDP récepteur accuse réception du paquet. UDP ne requiert aucun accusé de réception. UDP n'applique pas la négociation en trois étapes.

Couche Internet : préparation des paquets pour la distribution

Les protocoles de transport TCP, UDP et SCTP transmettent les segments et paquets à la couche Internet située au niveau inférieur. Là, le protocole IP gère les segments et paquets. Pour les préparer à la distribution, IP les formate en unités appelées *datagrammes IP*. IP détermine ensuite les adresses IP des datagrammes, afin d'assurer la distribution à l'hôte récepteur.

Datagrammes IP

IP joint un *en-tête IP* à l'en-tête du paquet ou segment, en plus des informations ajoutées par TCP ou UDP. Les informations de l'en-tête IP incluent les adresses IP des hôtes émetteur et récepteur, la longueur du datagramme et le numéro d'ordre du datagramme. Ces informations sont fournies si le datagramme dépasse la taille en octets autorisée pour les paquets réseau et doit être fragmenté.

Couche de liaison de données : encadrement

Les protocoles de la couche de liaison de données, tels que DPPP, formatent le datagramme IP en un *cadre*. Ces protocoles joignent un troisième en-tête et un pied de page pour "encadrer" le datagramme. L'en-tête du cadre contient un champ de *contrôle de redondance cyclique* (CRC, Cyclic Redundancy Check) qui détecte les erreurs éventuelles lorsque le cadre parcourt le média réseau. Ensuite, la couche de liaison de données transmet le cadre à la couche physique.

Couche réseau physique : envoi et réception des cadres

La couche réseau physique de l'hôte émetteur reçoit les cadres et convertit les adresses IP en adresses matérielles adéquates sur le média réseau. Ensuite, la couche réseau physique envoie le cadre via le média réseau.

Gestion du paquet sur l'hôte récepteur

Lorsque le paquet arrive sur l'hôte récepteur, il parcourt la pile de protocoles TCP/IP dans l'ordre inverse à l'ordre dans lequel il a été envoyé. La Figure 1–1 illustre ce chemin. En outre, sur l'hôte récepteur, chaque protocole retire les informations d'en-tête jointes au paquet par son homologue sur l'hôte émetteur. Le processus suivant s'effectue :

1. La couche réseau physique reçoit le paquet sous forme de cadre. La couche réseau physique calcule le CRC du paquet, puis envoie le cadre à la couche de liaisons de données.
2. La couche de liaison de données vérifie que le CRC du cadre est correct et retire l'en-tête du cadre et le CRC. Enfin, le protocole de liaison de données envoie le cadre à la couche Internet.
3. La couche Internet lit les informations de l'en-tête afin d'identifier la transmission. Ensuite, la couche Internet détermine si le paquet est un fragment. Si la transmission est fragmentée, IP rassemble les fragments pour reconstituer le datagramme d'origine. IP retire ensuite l'en-tête IP et transmet le datagramme aux protocoles de la couche transport.
4. La couche transport (TCP, SCTP et UDP) lit l'en-tête pour déterminer le protocole de couche d'application qui doit recevoir les données. Ensuite, TCP, SCTP ou UDP retire l'en-tête associé. TCP, SCTP ou UDP envoie le message ou flux à l'application réceptrice.
5. La couche d'application reçoit le message. La couche d'application effectue ensuite l'opération requise par l'hôte émetteur.

Suivi interne TCP/IP

TCP/IP consigne les communications TCP lorsqu'un paquet RST interrompt une connexion, afin de permettre le suivi interne des opérations. Lorsqu'un paquet RST est transmis ou reçu, les informations sur 10 paquets maximum, qui viennent d'être transmis, sont consignées avec les informations de connexion.

Informations supplémentaires sur TCP/IP et Internet

De nombreuses informations sur TCP/IP et Internet sont à votre disposition. Pour obtenir des informations spécifiques non abordées dans ce document, consultez les sources indiquées ci-dessous.

Manuels informatiques sur TCP/IP

De nombreux ouvrages traitant de TCP/IP et d'Internet sont distribués dans le commerce et disponibles en bibliothèque et dans les librairies informatiques. Les deux ouvrages ci-dessous sont de grands classiques de TCP/IP :

- Craig Hunt. *TCP/IP administration de réseau* : cet ouvrage contient des informations théoriques et pratiques pour la gestion de réseau TCP/IP hétérogène.
- W. Richard Stevens. *TCP/IP illustré, Volume I* : dans cet ouvrage, les protocoles TCP/IP sont décrits en détail. Ce manuel est idéal pour les administrateurs réseau requérant des compétences TCP/IP techniques et pour les programmeurs réseau.

Sites Web liés à TCP/IP et aux réseaux

De multiples sites Web et groupes d'utilisateurs dédiés aux protocoles TCP/IP et à leur gestion sont disponibles sur Internet. De nombreux constructeurs, y compris Oracle Corporation, offrent des ressources Web qui fournissent des informations TCP/IP d'ordre général. Les ressources Web suivantes fournissent des informations sur TCP/IP et des informations générales relatives à l'administration d'un système. Le tableau suivant répertorie les principaux sites Web et descriptions des informations de réseau fournies par les sites.

Site Web	Description
Site Web du groupe IETF (Internet Engineering Task Force) (`http://www.ietf.org/home.html`)	L'IETF est responsable de l'architecture et du contrôle d'Internet. Le site Web de l'IETF contient des informations relatives aux diverses activités de l'organisation. Le site inclut également des liens vers les publications majeures de l'IETF.

Site Web	Description
Oracle Corporation's BigAdmin Portal (`http://www.oracle.com/technetwork/systems/index.html`)	BigAdmin fournit des informations dédiées à l'administration des ordinateurs Sun. Le site contient des FAQ, des ressources, des discussions, des liens vers la documentation correspondante et d'autres informations pertinentes concernant l'administration d'Oracle Solaris 10, notamment les réseaux.

RFC et brouillons Internet

Les groupes de travail de l'IETF publient des documents normatifs appelés RFC (*Request for Comments*, demande de commentaires). Les normes qui restent en cours de développement sont publiées en tant que brouillons Internet (*Internet Drafts*). Avant d'être placé à la disposition du public, toute RFC doit être approuvée par l'IAB (Internet Architecture Board, comité d'architecture Internet). En général, les RFC et brouillons Internet sont destinés aux développeurs et aux personnes possédant des connaissances techniques approfondies. Toutefois, certaines RFC liées au protocole TCP/IP fournissent des informations qui peuvent s'avérer utiles pour les administrateurs système. Ces RFC sont citées à divers emplacements de ce manuel.

En général, les documents FYI (For Your Information, pour information) constituent un sous-ensemble des RFC. Les FYI contiennent des informations non liées aux normes Internet. Les FYI contiennent des informations Internet plus générales. Par exemple, la bibliographie des documents FYI répertorie des manuels et articles décrivant TCP/IP. Les documents FYI constituent un recueil exhaustif des outils logiciels liés à Internet. Enfin, les documents FYI incluent un glossaire d'Internet et des termes généraux liés aux réseaux.

Ce guide et d'autres ouvrages dans la collection Administrateur Système Oracle Solaris contiennent des références aux RFC pouvant être appliquées.

PARTIE II

Administration TCP/IP

Cette partie aborde les tâches et les informations conceptuelles relatives à la configuration, à l'administration et au dépannage de réseaux TCP/IP.

◆ ◆ ◆ CHAPITRE 2

Planification de votre réseau TCP/IP (tâches)

Ce chapitre décrit les problèmes à résoudre pour créer un réseau de façon méthodique et économique. Une fois ces problèmes résolus, vous pouvez concevoir un plan de réseau lors de la configuration et de l'administration du réseau.

Le présent chapitre contient les informations suivantes :

Les tâches de configuration d'un réseau sont décrites au Chapitre 5, "Configuration des services réseau TCP/IP et de l'adressage IPv4 (tâches)".

Planification réseau (liste des tâches)

Le tableau suivant répertorie les différentes tâches permettant de configurer le réseau. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Référence
1. Planification du matériel requis et de la topologie réseau	Déterminez les types d'équipements nécessaires ainsi que la disposition de ces équipements sur le site.	■ Pour les questions de topologie réseau d'ordre général, reportez-vous à la section "Détermination du matériel réseau" à la page 55. ■ Pour la planification de topologie IPv6, reportez-vous à la section "Préparation de la topologie réseau pour une prise en charge d'IPv6" à la page 91. ■ Pour obtenir des informations sur un type d'équipement spécifique, reportez-vous à la documentation du constructeur de l'équipement.
2. Obtention d'une adresse IP enregistrée pour le réseau	Le réseau doit posséder une adresse IP unique si les communications doivent s'effectuer hors du réseau local, via Internet par exemple.	Reportez-vous à la section "Obtention du numéro IP du réseau" à la page 58.
3. Élaboration d'un schéma d'adressage IP pour les systèmes, en fonction du préfixe de réseau IPv4 ou du préfixe de site IPv6	Déterminez la méthode de déploiement des adresses sur le site.	Reportez-vous à la section "Conception d'un schéma d'adressage IPv4" à la page 58 ou à la section "Préparation d'un plan d'adressage IPv6" à la page 95.
4. Création d'une liste contenant les adresses IP et noms d'hôtes de toutes les machines du réseau	Utilisez cette liste pour créer les bases de données réseau.	Reportez-vous à la section "Bases de données réseau" à la page 64
5. Détermination du service de noms à utiliser sur le réseau	Choisissez le service de noms NIS, LDAP, DNS ou les bases de données réseau dans le répertoire `/etc` local.	Reportez-vous à la section "Sélection d'un service de noms et d'un service d'annuaire" à la page 64
6. Établissement des sous-divisions administratives, le cas échéant (selon le réseau)	Décidez si le site requiert une division du réseau en sous-divisions administratives.	Reportez-vous à la section "Sous-divisions administratives" à la page 66
7. Détermination de l'emplacement auquel positionner les routeurs dans le réseau	Si le réseau est étendu et, par conséquent, requiert des routeurs, créez une topologie réseau prenant en charge ces derniers.	Reportez-vous à la section "Planification des routeurs du réseau" à la page 66

Tâche	Description	Référence
8. Élaboration d'une stratégie pour les sous-réseaux, le cas échéant	Vous aurez peut-être besoin de créer des sous-réseaux pour administrer l'espace d'adressage IP ou pour mettre des adresses IP supplémentaires à la disposition des utilisateurs.	Pour la planification de sous-réseau IPv4, reportez-vous à la section "Qu'est-ce que la création de sous-réseaux ?" à la page 244 Pour la planification de sous-réseau IPv6, reportez-vous à la section "Création d'un schéma de numérotation pour les sous-réseaux" à la page 96

Détermination du matériel réseau

Lors de la conception du réseau, vous devez choisir le type de réseau le plus adapté aux besoins de votre organisation. Les décisions à prendre dans le cadre de la planification impliquent le matériel réseau. Vous devez déterminer :

- la topologie réseau, la disposition et les connexions du matériel réseau ;
- le nombre de systèmes hôte que le réseau peut prendre en charge ;
- les types d'hôtes pris en charge par le réseau ;
- les types de serveurs requis ;
- le type de média réseau à utiliser : Ethernet, Token Ring, FDDI, etc. ;
- si des ponts ou routeurs doivent étendre ce média ou connecter le réseau local à des réseaux externes ;
- si des systèmes requièrent des interfaces acquises séparément, outre leurs interfaces intégrées.

En fonction de ces facteurs, vous pouvez définir la taille du réseau local.

Remarque – Ce manuel n'a pas pour objectif de décrire la planification du matériel réseau. Pour obtenir de l'assistance, reportez-vous aux manuels accompagnant le matériel.

Choix du format d'adressage IP du réseau

La configuration du réseau dépend du nombre de systèmes à prendre en charge. Votre organisation peut avoir besoin d'un petit réseau de plusieurs douzaines de systèmes autonomes résidant dans un même bâtiment et au même étage. Vous pouvez aussi configurer un réseau comprenant plus de 1 000 systèmes situés dans différents bâtiments. Cette configuration requiert une division supplémentaire du réseau en sous-divisions appelées *sous-réseaux*.

Lors de la planification du schéma d'adressage du réseau, tenez compte des facteurs suivants :

- le type d'adresse IP à employer : IPv4 ou IPv6
- le nombre de systèmes potentiels sur le réseau ;
- le nombre de systèmes multiréseau ou routeurs, qui requièrent une adresse IP pour chaque interface ;
- si des adresses privées doivent être utilisées sur le réseau ;
- si les pools d'adresses IPv4 doivent être gérés par un serveur DHCP.

En raison de la croissance mondiale d'Internet depuis 1990, les adresses IP disponibles s'épuisent. Pour y remédier, l'IETF (Internet Engineering Task Force, groupe d'étude d'ingénierie Internet) a développé un certain nombre de méthodes alternatives d'adressage IP.

Si plusieurs adresses IP ont été attribuées à votre organisation pour le réseau ou si des sous-réseaux sont utilisés, désignez une autorité centrale au sein de votre organisation comme responsable de l'attribution des adresses réseau IP. Cette autorité doit assurer le contrôle d'un pool d'adresses IP réseau attribuées et allouer des adresses aux hôtes, réseaux et sous-réseaux, le cas échéant. Pour éviter tout problème, assurez-vous qu'il n'existe aucun numéro de réseau aléatoire ou dupliqué dans l'organisation. Les types d'adresses IP suivants sont actuellement utilisés :

Adresses IPv4

Ces adresses 32 bits correspondent au format d'adressage IP initialement conçu pour TCP/IP. À l'origine, les réseaux IP se décomposent en trois classes, A, B et C. Le *numéro de réseau* attribué à un réseau reflète cette identification de classe, tandis que les 8 bits ou plus supplémentaires représentent un hôte. Les adresses IPv4 basées sur les classes requièrent la configuration d'un masque de réseau pour le numéro de réseau. En outre, ces adresses étaient souvent divisées en sous-réseaux afin d'augmenter le nombre d'adresses disponibles pour les systèmes du réseau local.

Aujourd'hui, les adresses IP sont appelées *adresses IPv4*. Il est désormais impossible d'obtenir des numéros de réseau IPv4 basés sur les classes auprès d'un fournisseur de services Internet, mais de nombreux réseaux les utilisent encore. Pour de plus amples informations sur l'administration d'adresses IPv4, reportez-vous à la section “Conception du schéma d'adressage IPv4” à la page 60.

Adresses IPv4 au format CIDR

L'IETF a développé des adresses CIDR (Classless Inter-Domain Routing, routage inter-domaine sans classe) dans le but de résoudre à court ou moyen terme le problème d'épuisement des adresses IPv4. Par ailleurs, le format CIDR a été conçu pour remédier au

manque de capacité des tables de routage Internet. Une adresse IPv4 avec notation CIDR présente une longueur de 32 bits et le même format décimal avec points. Cependant, CIDR ajoute une désignation de préfixe juste après l'octet le plus à droite afin de définir la portion de réseau de l'adresse IPv4. Pour de plus amples informations, reportez-vous à la section "Conception du schéma d'adressage IPv4 CIDR" à la page 61.

Adresses DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol, protocole de configuration dynamique d'hôte) permet à un système de recevoir à l'initialisation les informations de configuration d'un serveur DHCP, notamment une adresse IP. Les serveurs DHCP tiennent à jour des pools d'adresses IP à partir desquels attribuer des adresses aux clients DHCP. Cela permet à un site DHCP d'utiliser un pool d'adresses IP plus petit que celui qui serait nécessaire si tous les clients possédaient une adresse IP permanente. Vous pouvez configurer le service DHCP afin de gérer les adresses IP de votre site ou une partie des adresses. Pour plus d'informations, reportez-vous au Chapitre 12, "À propos de DHCP (présentation)".

Adresses IPv6

L'IETF a déployé des adresses IPv6 128–bits afin de résoudre à long terme le problème d'épuisement des adresses IPv4 disponibles. Les adresses IPv6 assurent un espace d'adressage plus étendu que IPv4. Grâce au protocole TCP/IP double pile, Oracle Solaris prend en charge les adressages IPv4 et IPv6 sur un même hôte. De même que les adresses IPv4 au format CIDR, les adresses IPv6 ne possèdent aucune notion de classe de réseau ni de masque de réseau. Comme dans CIDR, les adresses IPv6 utilisent des préfixes pour désigner la partie de l'adresse définissant le réseau du site. Pour une introduction à IPv6, reportez-vous à la section "Présentation de l'adressage IPv6" à la page 76.

Adresses privées et préfixes de documentation

L'IANA a réservé un bloc d'adresses IPv4 et un préfixe de site IPv6 à utiliser sur les réseaux privés. Vous pouvez déployer ces adresses sur des systèmes au sein d'un réseau d'entreprise, mais les paquets possédant des adresses privées ne peuvent pas être transmis via Internet. Pour de plus amples informations sur les adresses privées, reportez-vous à la section "Utilisation d'adresses IPv4 privées" à la page 62.

Remarque – Des adresses IPv4 privées sont également réservées à la documentation. Les exemples de ce manuel utilisent des adresses IPv4 privées et le préfixe de documentation IPv6 réservé.

Obtention du numéro IP du réseau

Un réseau IPv4 se définit à l'aide d'un numéro de réseau IPv4 et d'un *masque de réseau*. Un réseau IPv6 est défini par son *préfixe de site* et s'il dispose d'un sous-réseau, par son *préfixe de sous-réseau*.

Les utilisateurs locaux auront probablement besoin de communiquer hors du réseau local, sauf si vous souhaitez conserver un réseau privé. Par conséquent, vous devez obtenir un numéro IP enregistré pour le réseau auprès de l'organisation adéquate, afin de permettre au réseau de communiquer avec l'extérieur. Cette adresse devient le numéro de réseau de votre schéma d'adressage IPv4 ou le préfixe de site de votre schéma d'adressage IPv6.

Les fournisseurs d'accès Internet (FAI) procurent des adresses IP pour les réseaux à un coût dépendant du niveau de service assuré. Comparez les offres de divers FAI afin de déterminer celui qui fournit le service le plus adéquat pour votre réseau. Les FAI offrent généralement des adresses allouées dynamiquement ou des adresses IP statiques aux entreprises. Certains FAI proposent à la fois des adresses IPv4 et IPv6.

Si le site est un FAI, vous pouvez obtenir les blocs d'adresses IP pour vos clients auprès de l'IR (Internet Registry, registre Internet) correspondant à votre environnement linguistique. L'IANA (Internet Assigned Numbers Authority, autorité de numéros assignés sur Internet) est actuellement responsable de la délégation des adresses IP enregistrées aux IR dans le monde entier. Chaque IR possède des modèles et des informations d'enregistrement dédiés à l'environnement linguistique assuré par l'IR. Pour plus d'informations sur l'IANA et les IR, reportez-vous à la page des services d'adresse IP de l'IANA (`http://www.iana.org/ipaddress/ip-addresses.htm`).

Remarque – N'attribuez pas d'adresses IP au réseau de façon arbitraire, même s'il n'est connecté à aucun réseau TCP/IP externe. Au contraire, utilisez les adresses privées comme décrit à la section “Utilisation d'adresses IPv4 privées” à la page 62.

Conception d'un schéma d'adressage IPv4

Remarque – Pour plus d'informations sur la planification d'adresses IPv6, reportez-vous à la section “Préparation d'un plan d'adressage IPv6” à la page 95.

Cette section présente l'adressage IPv4 pour vous aider à concevoir un plan d'adressage IPv4. Pour de plus amples informations sur les adresses IPv6, reportez-vous à la section “Présentation de l'adressage IPv6” à la page 76. Pour plus d'informations sur les adresses DHCP, reportez-vous au Chapitre 12, “À propos de DHCP (présentation)”.

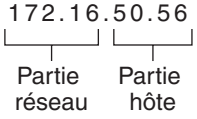
Chaque réseau IPv4 doit posséder les éléments suivants :

- un numéro de réseau unique conçu par un FAI, un IR ou, pour les réseaux plus anciens, enregistré par l'IANA. si vous souhaitez employer des adresses privées, les numéros de réseau créés doivent être uniques au sein de l'organisation ;
- des adresses IPv4 uniques pour les interfaces de chaque système du réseau ;
- un masque de réseau.

Une adresse IPv4 est un nombre de 32 bits identifiant de manière unique une interface réseau sur un système, comme expliqué à la section "Application d'adresses IP aux interfaces réseau" à la page 63. Une adresse IPv4 s'écrit sous forme de nombres décimaux, divisés en quatre champs de 8 bits séparés par des points. Chaque champ de 8 bits représente un octet de l'adresse IPv4. Cette forme de représentation des octets d'une adresse IPv4 est appelée *format décimal avec points*.

La figure ci-dessous présente les composants d'une adresse IPv4, `172.16.50.56`.

FIGURE 2–1 Format d'adresse IPv4



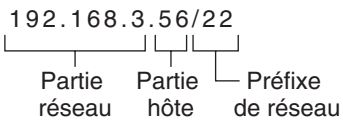
`172.16` Numéro de réseau IPv4 enregistré. En notation IPv4 basée sur les classes, ce numéro définit également la classe de réseau IP (la classe B dans cet exemple) qui aurait été enregistrée par l'IANA.

`50.56` Partie hôte de l'adresse IPv4. La partie hôte identifie de manière unique l'interface d'un système résidant sur le réseau. La partie réseau de l'adresse est la même pour toutes les interfaces du réseau local, mais la partie hôte doit être différente.

Si vous souhaitez diviser un réseau IPv4 basé sur les classes en sous-réseaux, vous devez définir un masque de sous-réseau (*masque de réseau*), comme indiqué à la section "Base de données `netmasks`" à la page 244.

L'exemple suivant présente l'adresse de format CIDR `192.168.3.56/22`.

FIGURE 2–2 Adresse IPv4 au format CIDR



`192.168.3` Partie réseau, qui correspond au numéro de réseau IPv4 fourni par le FAI ou l'IR.

`56` Partie hôte attribuée à une interface d'un système.

`/22` Préfixe de réseau, qui définit le nombre de bits de l'adresse constituant le numéro de réseau. Le préfixe de réseau indique également le masque de sous-réseau de l'adresse IP. Les préfixes de réseau sont également attribués par le FAI ou l'IR.

Un réseau Oracle Solaris peut combiner des adresses IPv4 standard, des adresses IPv4 au format CIDR, des adresses DHCP, des adresses IPv6 et des adresses IPv4 privées.

Conception du schéma d'adressage IPv4

Cette section décrit les classes selon lesquelles l'adresse IPv4 standard est organisée. L'IANA ne distribue plus de numéros de réseau, mais de nombreux réseaux utilisent encore ces numéros. Sur certains sites, l'espace d'adressage doit être administré à l'aide de numéros de réseau définis par rapport aux classes. Vous trouverez une description détaillée des classes de réseau IPv4 à la section "Classes de réseau" à la page 258.

Le tableau suivant indique la décomposition d'une adresse IPv4 standard en espaces d'adressage hôte et réseau. Pour chaque classe, la plage de valeurs décimales du premier octet du numéro de réseau est indiquée dans la colonne Plage d'octets. La colonne Numéro de réseau indique le nombre d'octets de l'adresse IPv4 dédiés à la partie réseau de l'adresse. Chaque octet est représenté par *xxx*. La colonne Adresse hôte indique le nombre d'octets dédiés à la partie hôte de l'adresse. Par exemple, pour une adresse réseau de classe A, le premier octet est dédié au réseau, tandis que les trois derniers octets définissent l'hôte. Dans un réseau de classe C, c'est le contraire.

TABLEAU 2–1 Décomposition des adresses IPv4 selon la classe

Classe	Plage d'octets	Numéro de réseau	Adresse hôte
A	0–127	*xxx*	*xxx.xxx. xxx*
B	128–191	*xxx.xxx*	*xxx.xxx*
C	192–223	*xxx.xxx. xxx*	*xxx*

Les numéros du premier octet de l'adresse IPv4 définissent la classe du réseau (soit A, B ou C). La plage des trois autres octets est 0–255. Les numéros 0 et 255 sont réservés. Vous pouvez attribuer les numéros 1 à 254 à chaque octet, selon la classe de réseau attribuée à votre réseau par l'IANA.

Le tableau ci-dessous indique les octets de l'adresse IPv4 qui vous est attribuée. Ce tableau indique également, pour chaque octet, la plage de numéros attribuables aux hôtes.

TABLEAU 2–2 Plage de classes IPv4 disponibles

Classe de réseau	Plage du premier octet	Plage du deuxième octet	Plage du troisième octet	Plage du quatrième octet
A	0–127	1–254	1–254	1–254
B	128–191	Préattribué par l'IANA	1–254	1–254
C	192–223	Préattribué par l'IANA	Préattribué par l'IANA	1–254

Numéro de sous-réseau IPv4

Les réseaux locaux comprenant un grand nombre d'hôtes sont parfois répartis en sous-réseaux. Si vous décomposez le numéro de réseau IPv4 en sous-réseaux, vous devez attribuer un identificateur réseau à chaque sous-réseau. Le cas échéant, utilisez une partie des bits de la partie hôte de l'adresse IPv4 en tant qu'identificateur réseau afin d'optimiser l'espace d'adressage IPv4. Lorsqu'une partie spécifiée de l'adresse est utilisée en tant qu'identificateur réseau, elle devient le numéro de sous-réseau. Pour créer un numéro de sous-réseau, vous devez utiliser un masque de réseau, ou masque de bits, qui sélectionne les parties réseau et sous-réseau d'une adresse IPv4. Pour plus d'informations, reportez-vous à la section “Création du masque de réseau des adresses IPv4” à la page 245.

Conception du schéma d'adressage IPv4 CIDR

Les classes de réseau qui constituaient IPv4 à l'origine ne sont plus utilisées sur Internet. Aujourd'hui, l'IANA distribue des adresses de format CIDR sans classe à ses registres du monde entier. Toute adresse IPv4 obtenue auprès d'un FAI se présente au format CIDR, comme illustré à la Figure 2–2.

Le préfixe de réseau de l'adresse CIDR indique le nombre d'adresses IPv4 disponibles pour les hôtes du réseau. Ces adresses hôte sont attribuées aux interfaces d'un hôte. Si un hôte possède plusieurs interfaces physiques, vous devez attribuer une adresse hôte à chaque interface physique employée.

Le préfixe de réseau d'une adresse CIDR définit également la longueur du masque de sous-réseau. La plupart des commandes Oracle Solaris reconnaissent le préfixe CIDR d'un masque de sous-réseau dans un réseau. Toutefois, vous devez définir le masque de sous-réseau à l'aide de la représentation décimale avec points pour le programme d'installation Oracle Solaris et le fichier `/etc/netmask`. Dans ces deux cas, appliquez la représentation décimale avec points du préfixe de réseau CIDR, comme indiqué dans le tableau ci-dessous.

TABLEAU 2–3 Préfixes CIDR et leur équivalent décimal

Préfixe de réseau CIDR	Adresses IP disponibles	Équivalent en numérotation décimale avec points
/19	8 192	255.255.224.0
/20	4 096	255.255.240.0
/21	2 048	255.255.248.0
/22	1 024	255.255.252.0
/23	512	255.255.254.0
/24	256	255.255.255.0
/25	128	255.255.255.128
/26	64	255.255.255.192
/27	32	255.255.255.224

Pour de plus amples informations sur les adresses CIDR, reportez-vous aux sources suivantes :

- Vous trouverez des informations techniques sur CIDR dans le document RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy (`http://www.ietf.org/rfc/rfc1519.txt?number=1519`) (en anglais).
- Des informations plus générales sur CIDR sont disponibles auprès de Pacific Bell Internet dans le document Classless Inter-Domain Routing (CIDR) Overview (`http://www.wirelesstek.com/cidr.htm`) (en anglais).
- Vous trouverez également une présentation sur CIDR dans l'article de Wikipedia intitulé Classless inter-domain routing" (`http://en.wikipedia.org/wiki/Classless_inter-domain_routing`).

Utilisation d'adresses IPv4 privées

L'IANA a réservé trois blocs d'adresses IPv4 pour permettre aux sociétés de les utiliser sur leurs réseaux privés. Ces adresses sont définies dans le document RFC 1918, Address Allocation for Private Internets (`http://www.ietf.org/rfc/rfc1918.txt?number=1918`) (en anglais). Vous pouvez utiliser ces *adresses privées*, également appelées adresses 1918, pour les systèmes résidant sur des réseaux locaux au sein d'un intranet d'entreprise. Toutefois, les adresses privées ne son pas valides sur Internet. Ne les utilisez pas sur des systèmes devant communiquer hors du réseau local.

Le tableau suivant répertorie les plages d'adresses IPv4 privées et des masques de réseau respectifs.

Plage d'adresses IPv4	Masque de réseau
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

Application d'adresses IP aux interfaces réseau

Pour se connecter au réseau, un système doit posséder au moins une *interface réseau physique*. Chaque interface réseau doit posséder une adresse IP unique. Lors de l'installation Oracle Solaris, vous devez spécifier l'adresse IP de la première interface détectée par le programme d'installation. En général, le nom de cette interface est *nom-périphérique*0, par exemple `eri0` ou `hme0`. Cette interface est considérée comme l'*interface réseau principale*.

Si vous ajoutez une autre interface réseau à l'hôte, celle-ci doit également posséder une adresse IP unique. Une fois la deuxième interface réseau ajoutée, l'hôte devient *multiréseau*. Par contre, lorsque vous ajoutez une deuxième interface réseau à un hôte et activez la transmission IP, cet hôte devient un routeur. Pour plus d'explications, reportez-vous à la section “Configuration d'un routeur IPv4” à la page 124.

Chaque interface réseau possède un nom de périphérique, un pilote de périphérique et un fichier de périphérique associé dans le répertoire `/devices`. L'interface réseau peut posséder un nom de périphérique, par exemple `eri` ou `smc0`, qui correspondent aux noms de périphérique de deux interfaces Ethernet usuelles.

Pour obtenir des informations et la description des tâches liées aux interfaces, reportez-vous au Chapitre 6, “Administration d'interfaces réseau (tâches)”.

Remarque – Dans ce manuel, il va de soi que les systèmes possèdent des interfaces réseau Ethernet. Si vous souhaitez utiliser un autre média réseau, reportez-vous aux manuels fournis avec l'interface réseau pour obtenir les informations de configuration.

Attribution de noms aux entités du réseau

Lorsque vous avez reçu l'adresse IP réseau qui vous est attribuée, et lorsque vous avez indiqué les adresses IP à vos systèmes, la tâche suivante consiste à attribuer les noms aux hôtes. Ensuite, vous devez déterminer comment gérer les services de noms sur le réseau. Ces noms sont initialement utilisés pour configurer le réseau et, par la suite, pour étendre le réseau à l'aide de routeurs, de ponts ou de PPP.

Les protocoles TCP/IP détectent un système sur le réseau à l'aide de son adresse IP. Toutefois, choisissez un nom reconnaissable afin d'identifier facilement le système. Par conséquent, les protocoles TCP/IP (et Oracle Solaris) nécessitent à la fois l'adresse IP et le nom d'hôte pour identifier de manière unique le système.

Dans le cadre de TCP/IP, un réseau correspond à un ensemble d'entités nommées. Un hôte correspond à une entité possédant un nom. Un routeur correspond à une entité possédant un nom. Le réseau correspond à une entité possédant un nom. Vous pouvez également attribuer un nom à un groupe ou service dans lequel le réseau est installé, ainsi qu'à une division, une région ou une société. Théoriquement, la hiérarchie de noms utilisée pour identifier un réseau est illimitée. Le nom de domaine identifie un *domaine*.

Administration des noms d'hôtes

Sur de nombreux sites, les utilisateurs sont autorisés à choisir les noms d'hôtes de leur machine. Tout serveur requiert également au moins un nom d'hôte associé à l'adresse IP de son interface réseau principale.

L'administrateur système doit s'assurer que chaque nom d'hôte du domaine est unique. En d'autres termes, vous ne pouvez pas attribuer le même nom, Fred par exemple, à deux machines du réseau. Par contre, la machine appelée Fred peut posséder plusieurs adresses IP.

Lors de la planification du réseau, dressez la liste des adresses IP et des noms d'hôtes associés afin d'en faciliter l'accès lors des processus de configuration. Cette liste permet de vérifier que chaque nom d'hôte est unique.

Sélection d'un service de noms et d'un service d'annuaire

Oracle Solaris permet d'utiliser trois types de services de noms : fichiers locaux, NIS et DNS. Les services de noms mettent à jour d'importantes informations sur les machines du réseau, par exemple les noms d'hôtes, les adresses IP, les adresses Ethernet, etc. Oracle Solaris permet également d'utiliser le service d'annuaire LDAP avec ou à la place d'un service de noms. Pour une présentation des services de noms d'Oracle Solaris, reportez-vous à la Partie I, “À propos des services d’annuaire et de nommage” du *Guide d’administration système : Services d’annuaire et de nommage (DNS, NIS et LDAP)*.

Bases de données réseau

Lors de l'installation du système d'exploitation, vous indiquez le nom d'hôte et l'adresse IP du serveur, des clients ou du système autonome. Le programme d'installation d'Oracle Solaris ajoute ces informations aux `hôtes`. Dans Solaris 10 11/06 et les versions Solaris 10 antérieures, ces informations sont ajoutées à la base de données réseau `ipnodes`. Cette base de données fait

partie d'un ensemble de bases de données réseau contenant les informations nécessaires aux opérations TCP/IP sur le réseau. Le service de noms sélectionné pour le réseau lit ces bases de données.

La configuration des bases de données réseau est d'une importance capitale. Par conséquent, vous devez choisir le service de noms à utiliser au cours du processus de planification réseau. En outre, l'utilisation des services de noms affecte également l'organisation du réseau en un domaine administratif. La section "Bases de données réseau et fichier `nsswitch.conf`" à la page 248 contient des informations détaillées sur les bases de données réseau.

Utilisation de NIS ou DNS en tant que service de noms

Les services de noms NIS et DNS mettent à jour des bases de données réseau sur plusieurs serveurs du réseau. Ces services de noms et la configuration des bases de données sont décrits dans le *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*. En outre, ce manuel explique en détail les concepts d'espace de noms et de domaine administratif.

Utilisation de fichiers locaux en tant que service de noms

Si vous n'implémentez ni NIS, ni LDAP, ni DNS, le réseau assure le service de noms à l'aide de *fichiers locaux*. Le terme "fichiers locaux" fait référence à la série de fichiers du répertoire `/etc` utilisé par les bases de données réseau. Sauf indication contraire, les procédures de ce manuel partent du principe que vous utilisez des fichiers locaux comme service de noms.

Remarque – Si vous décidez d'utiliser des fichiers locaux en tant que service de noms pour le réseau, vous pouvez configurer plus tard un autre service de noms.

Noms de domaine

De nombreux réseaux organisent leurs hôtes et routeurs selon une hiérarchie de domaines administratifs. Si vous utilisez le service de noms NIS ou DNS, vous devez sélectionner pour l'organisation un nom de domaine unique au monde. Pour vérifier que le nom de domaine est unique, enregistrez-le auprès de l'InterNIC. Si vous souhaitez utiliser DNS, vous devez également enregistrer votre nom de domaine auprès de l'InterNIC.

La structure des noms de domaine est hiérarchique. En général, tout nouveau domaine se place sous un domaine existant associé. Par exemple, le nom de domaine d'une filiale peut se placer sous le nom de domaine de la maison mère. Si le nom de domaine n'a pas d'autre relation, une organisation peut placer son nom de domaine directement sous l'un des domaines supérieurs existants.

Vous trouverez ci-dessous quelques exemples de domaines supérieurs :

- `.com` : entreprises commerciales (d'envergure internationale) ;

- `.edu` : institutions d'enseignement (d'envergure internationale) ;
- `.gov` : organismes publics américains ;
- `.fr` : France.

Vous devez sélectionner un nom unique pour identifier votre organisation.

Sous-divisions administratives

La création de sous-divisions administratives dépend de la taille du réseau et du contrôle requis. À mesure que les nombres d'hôtes et de serveurs augmentent, la gestion du réseau devient de plus en plus complexe. Dans une telle situation, il peut s'avérer indispensable de configurer des divisions administratives supplémentaires. Par exemple, ajoutez des réseaux d'une classe particulière ou séparez les réseaux existants en sous-réseaux. La configuration de sous-divisions administratives pour le réseau dépend des facteurs ci-dessous :

- **Étendue du réseau**

  Une division administrative peut gérer à elle seule un réseau de plusieurs centaines d'hôtes se trouvant physiquement au même endroit et requérant des services administratifs identiques. Toutefois, il peut s'avérer judicieux d'établir plusieurs sous-divisions administratives. Les sous-divisions sont particulièrement utiles dans le cas d'un petit réseau réparti en sous-réseaux, si le réseau s'étend sur une large zone géographique.

- **Besoins des utilisateurs**

  Par exemple, un réseau peut résider entièrement dans un bâtiment et prendre en charge des machines relativement peut nombreuses. Ces machines sont réparties en plusieurs sous-réseaux. Chaque sous-réseau prend en charge des groupes d'utilisateurs ayant des besoins différents. Dans cet exemple, il serait judicieux de créer une sous-division administrative par sous-réseau.

Planification des routeurs du réseau

Il existe deux types d'entités TCP/IP sur un réseau : les hôtes et les routeurs. Tout réseau doit contenir des hôtes, mais les routeurs ne sont pas toujours requis. La topologie physique du réseau détermine si des routeurs sont requis. Cette section présente les concepts de routage et de topologie réseau. Ces concepts sont importants pour l'ajout d'un réseau à l'environnement réseau existant.

Remarque – Pour obtenir les détails de la configuration des routeurs sur les réseaux IPv4, ainsi que la description des tâches associées, reportez-vous à la section "Transfert et routage de paquets sur des réseaux IPv4" à la page 117. Pour obtenir les détails de la configuration des routeurs sur les réseaux IPv6, ainsi que la description des tâches associées, reportez-vous à la section "Configuration d'un routeur IPv6" à la page 179.

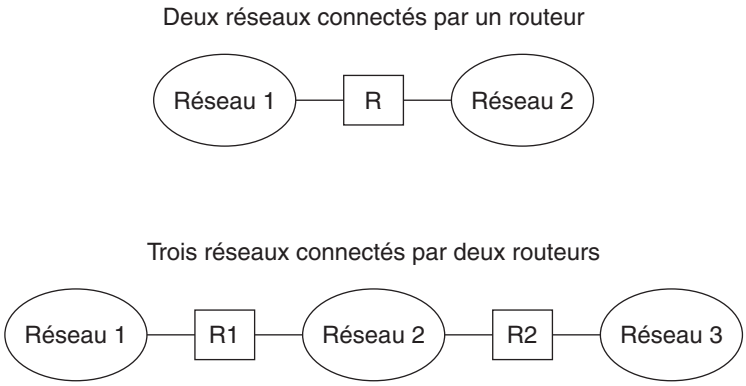
Présentation de la topologie réseau

La topologie réseau décrit l'organisation des réseaux. Les routeurs constituent des entités connectant les réseaux les uns aux autres. Toute machine possédant plusieurs interfaces réseau et implémentant la transmission IP constitue un routeur. Toutefois, pour fonctionner en tant que routeur, le système doit être configuré, comme décrit à la section "Configuration d'un routeur IPv4" à la page 124.

Les routeurs connectent plusieurs réseaux pour former des interréseaux plus étendus. Les routeurs doivent être configurés de manière à transmettre des paquets entre deux réseaux adjacents. Les routeurs doivent également être à même de transmettre les paquets vers les réseaux résidant au-delà des réseaux adjacents.

La figure ci-dessous indique les composants de base d'une topologie réseau. La première illustration présente une configuration simple de deux réseaux connectés par un routeur. La deuxième illustration présente la configuration de trois réseaux interconnectés par deux routeurs. Dans le premier exemple, le routeur R joint le réseau 1 et le réseau 2 pour former un interréseau plus étendu. Dans le deuxième exemple, le routeur R1 connecte les réseaux 1 et 2. Le routeur R2 connecte les réseaux 2 et 3. Les connexions forment un réseau comprenant les réseaux 1, 2 et 3.

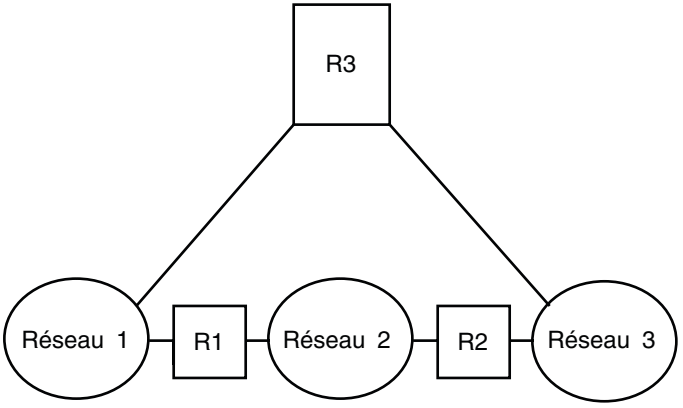
FIGURE 2–3 Topologie réseau de base



Outre la formation d'interréseaux par la jonction de réseaux, les routeurs assurent la transmission de paquets entre les réseaux en fonction des adresses du réseau de destination. À mesure que les interréseaux se complexifient, chaque routeur doit prendre de plus en plus de décisions relativement à la destination des paquets.

La figure ci-dessous présente un cas plus complexe. Le routeur R3 connecte directement les réseaux 1 et 3. La redondance améliore la fiabilité. Si le réseau 2 tombe en panne, le routeur R3 fournit encore une route entre les réseaux 1 et 3. Vous pouvez interconnecter plusieurs réseaux. Toutefois, les réseaux doivent employer les mêmes protocoles réseau.

FIGURE 2–4 Topologie réseau assurant un chemin supplémentaire entre des réseaux



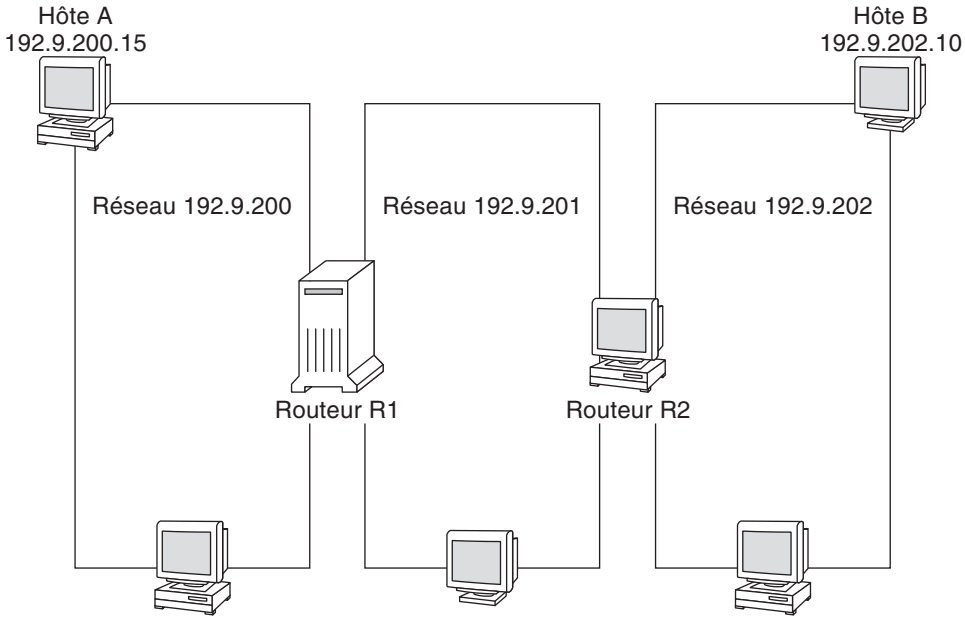
Transfert des paquets par les routeurs

L'adresse IP du destinataire, indiquée dans l'en-tête du paquet, détermine la méthode de routage du paquet. Si le numéro de réseau de l'adresse correspond au réseau local, le paquet se dirige directement vers l'hôte possédant cette adresse IP. Si le numéro de réseau ne correspond pas au réseau local, le paquet se dirige directement vers le routeur du réseau local.

Les routeurs conservent les informations de routage dans des *tables de routage*. Ces tables contiennent les adresses IP des hôtes et routeurs résidant sur les réseaux auxquels le routeur est connecté. Elles incluent également des pointeurs vers ces réseaux. À la réception d'un paquet, le routeur recherche dans sa table de routage l'adresse de destination indiquée dans l'en-tête du paquet. Si l'adresse de destination ne se trouve pas dans la table, le routeur transfère le paquet à un autre routeur répertorié dans sa table de routage. Pour plus d'informations sur les routeurs, reportez-vous à la section “Configuration d'un routeur IPv4” à la page 124.

La figure ci-dessous présente une topologie réseau constituée de trois réseaux connectés par deux routeurs.

FIGURE 2–5 Topologie réseau correspondant à trois réseaux interconnectés



Le routeur R1 connecte les réseaux `192.9.200` et `192.9.201`. Le routeur R2 connecte les réseaux `192.9.201` et `192.9.202`. SI l'hôte A du réseau `192.9.200` envoie un message à l'hôte B du réseau `192.9.202`, les événements suivants se produisent :

1. L'hôte A envoie un paquet au réseau `192.9.200`. L'en-tête du paquet contient l'adresse IPv4 de l'hôte destinataire, soit l'hôte B, `192.9.202.10`.
2. Aucune machine du réseau `192.9.200` ne possède l'adresse IPv4 `192.9.202.10`. Par conséquent, le routeur R1 accepte le paquet.
3. Le routeur R1 examine ses tables de routage. Aucune machine du réseau `192.9.201` ne possède l'adresse `192.9.202.10`. Toutefois, le routeur R2 est répertorié dans les tables de routage.
4. R1 sélectionne ensuite R2 comme routeur du "saut suivant". R1 envoie le paquet à R2.
5. Comme il connecte le réseau `192.9.201` au réseau `192.9.202`, R2 possède des informations de routage pour l'hôte B. Il transfère ensuite le paquet vers le réseau `192.9.202`, où l'hôte B l'accepte.

◆ ◆ ◆ CHAPITRE 3

Présentation d'IPv6

Ce chapitre présente un aperçu de l'implémentation du protocole Internet version 6 (IPv6) d'Oracle Solaris. Cette implémentation inclut le démon et les utilitaires associés prenant en charge l'espace d'adressage IPv6.

L'environnement réseau d'Oracle Solaris peut contenir des adresses IPv6 et IPv4. Les systèmes configurés avec des adresses IPv6 conservent leurs adresses IPv4, si celles-ci existent déjà. Les opérations utilisant les adresses IPv6 n'ont pas d'incidence sur les opérations IPv4 et inversement.

Les rubriques traitées sont les suivantes :

Pour obtenir des informations détaillées sur IPv6, consultez les chapitres suivants.

- Planification de réseau IPv6 – Chapitre 4, "Planification d'un réseau IPv6 (tâches)"
- Tâches relatives à IPv6 – Chapitre 7, "Configuration d'un réseau IPv6 (tâches)" et Chapitre 8, "Gestion d'un réseau TCP/IP (tâches)".
- Informations détaillées sur IPv6 – Chapitre 11, "Présentation détaillée de IPv6 (référence)"

Fonctions principales d'IPv6

L'espace d'adressage offert par IPv6 est plus grand que celui qui est fournit par IPv4. IPv6 permet également d'améliorer les capacités Internet, et ce dans de nombreux domaines, tel que décrit dans cette section.

Adressage étendu

La taille de l'adresse IP passe de 32 bits pour IPv4 à 128 bits pour IPv6, ce qui permet une prise en charge d'un plus grand nombre de niveaux de hiérarchie d'adressage. En outre, IPv6 fournit beaucoup plus de systèmes IPv6 adressables. Pour de plus amples informations, reportez-vous à la section "Présentation de l'adressage IPv6" à la page 76.

Configuration automatique d'adresses et détection de voisins

Le protocole IPv6 de détection de voisins (*ND, Neighbor Discovery*) facilite la configuration automatique des adresses IPv6. La *configuration automatique* correspond à la capacité d'un hôte IPv6 à générer automatiquement sa propre adresse IPv6, ce qui simplifie l'administration d'adresses. Pour de plus amples informations, reportez-vous à la section "Configuration automatique d'adresse IPv6" à la page 84.

Le protocole de détection de voisins correspond à une combinaison de ces protocoles IPv4 : ARP (Address Resolution Protocol, protocole de résolution d'adresse), ICMP (Internet Control Message Protocol, protocole de message de contrôle Internet), RDISC (Router Discovery, détection de routeur) et ICMP Redirect. Les routeurs IPv6 utilisent la détection de voisins afin de publier le préfixe de site IPv6. Les hôtes IPv6 utilisent la détection de voisins à des fins diverses, incluant la demande de préfixe à un routeur IPv6. Pour de plus amples informations, reportez-vous à la section "Présentation du protocole de détection de voisins IPv6" à la page 83.

Simplification du format d'en-tête

Avec le format d'en-tête IPv6, certains champs d'en-tête IPv4 ne sont plus utilisés tandis que d'autres deviennent facultatifs. Cette modification permet de maintenir les coûts de bande passante de l'en-tête IPv6 aussi bas que possible, malgré l'augmentation de la taille d'adresse. Bien que les adresses IPv6 soient quatre fois plus longues que les adresses IPv4, l'en-tête IPv6 n'est que deux fois plus grande l'en-tête IPv4.

Prise en charge améliorée des options d'en-tête d'IP

Des modifications de la méthode d'encodage des options d'en-tête d'IP permettent un transfert plus efficace. En outre, les limites relatives à la longueur des options IPv6 sont moins strictes. Ces modifications permettent une plus grande flexibilité pour l'introduction future de nouvelles options.

Prise en charge d'applications pour l'adressage IPv6

De nombreux services réseau Oracle Solaris critiques reconnaissent et prennent en charge les adresses IPv6, par exemple :

- les services de noms comme DNS, LDAP et NIS. Pour obtenir des informations sur la prise en charge de ces services dans IPv6, reportez-vous à la section *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.
- les applications d'authentification et de confidentialité, telles que IPsec (IP Security Architecture, architecture de sécurité IP) et IKE (Internet Key Exchange, échange de clé Internet). Pour plus d'informations, reportez-vous à la Partie IV.
- les services différenciés, par exemple ceux qui sont fournis par IPQoS (IP Quality of Service, qualité de service IP). Pour plus d'informations, reportez-vous à la Partie VII.
- la détection de basculement, fournie par IPMP (IP Network Multipathing, multiacheminement sur réseau IP). Pour plus d'informations, reportez-vous à Partie VI.

Ressources IPv6 supplémentaires

Outre cette partie, vous pouvez obtenir des informations sur IPv6 auprès des sources répertoriées dans les sections suivantes.

RFC et brouillons Internet

De nombreux RFC (Request for Comments, demande de commentaires) relatifs à IPv6 sont disponibles. Le tableau suivant répertorie les principaux articles sur IPv6 et leur emplacement sur le site Web de l'IETF (Internet Engineering Task Force, groupe d'étude d'ingénierie Internet) à ce jour.

TABLEAU 3–1 RFC et brouillons Internet relatifs à IPv6

RFC ou brouillon Internet	Objet	Emplacement
RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*	Description des caractéristiques et fonctions du protocole de détection de voisins IPv6.	http://www.ietf.org/rfc/rfc2461.txt$number=2461 (`http://www.ietf.org/rfc/rfc2461.txt?number-2461`)

TABLEAU 3–1 RFC et brouillons Internet relatifs à IPv6 *(Suite)*

RFC ou brouillon Internet	Objet	Emplacement
RFC 3306, *Unicast-Prefix-Based IPv6 Multicast Addresses*	Description du format et des types d'adresses IPv6 multidiffusion.	ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt (`ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt`)
RFC 3484: *Default Address Selection for Internet Protocol version 6 (IPv6)*	Description des algorithmes utilisés pour la sélection d'adresses IPv6 par défaut.	http://www.ietf.org/rfc/rfc3484?number=3484 (`http://www.ietf.org/rfc/rfc3484.txt?number=3484`)
RFC 3513, *Internet Protocol version 6 (IPv6) Addressing Architecture*	Informations détaillées sur les types d'adresses IPv6 et de nombreux exemples.	http://www.ietf.org/rfc/rfc3513.txt?number=3513 (`http://www.ietf.org/rfc/rfc3513.txt?number=3513`)
RFC 3587, *IPv6 Global Unicast Address Format*	Définition du format standard des adresses IPv6 unicast.	http://www.ietf.org/rfc/rfc3587.txt?number=3587 (`http://www.ietf.org/rfc/rfc3587.txt?number=3587`)

Sites Web

Vous trouverez des informations sur IPv6 sur les sites Web suivants.

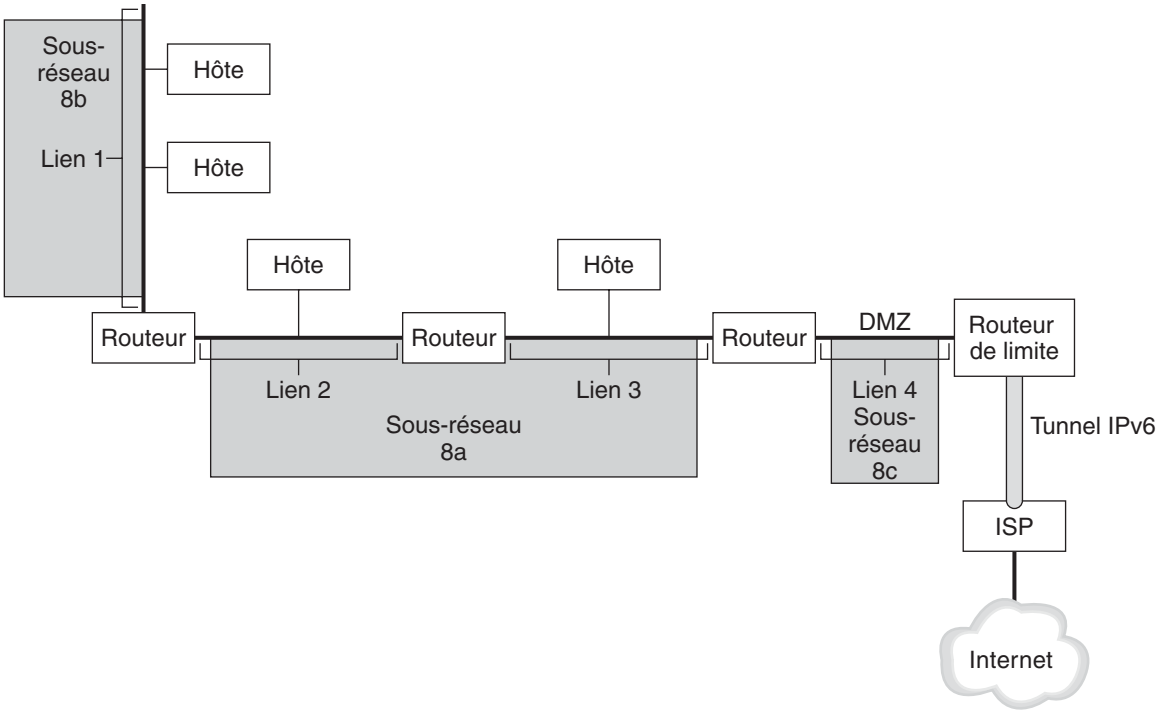
TABLEAU 3–2 Sites Web relatifs à IPv6

Site Web	Description	Emplacement
Forum IPv6	Des liens vers des présentations, événements, formations et implémentations relatifs à IPv6 et à dimension mondiale sont disponibles sur le site Web de cette société.	http://www.ipv6forum.com
Internet Educational Task Force IPv6 Working Group	Des liens vers la totalité des RFC et brouillons Internet IPv6 pertinents sont disponibles sur la page d'accueil de ce groupe de travail IETF.	http://www.ietf.org/html.charters/ipv6-charter.html

Présentation du réseau IPv6

Cette section présente les termes fondamentaux de la topologie réseau IPv6. La figure ci-dessous indique les composants de base d'un réseau IPv6.

FIGURE 3–1 Composants de base d'un réseau IPv6



L'illustration représente un réseau IPv6 et sa connexion à un FAI. Le réseau interne se compose des liens 1, 2, 3 et 4. Chaque lien est renseigné par des hôtes et terminé par un routeur. Le routeur de bordure se trouve à l'une des extrémités du lien 4, qui correspond à la DMZ du réseau. Le routeur de bordure exécute un tunnel IPv6 vers un FAI, lequel fournit la connectivité Internet au réseau. Le lien 2 et le lien 3 sont gérés en tant que sous-réseau 8a. Le sous-réseau 8b ne contient des systèmes que sur le lien 1. Le sous-réseau 8c et DMZ sont contigus sur le lien 4.

Comme indiqué sur la Figure 3–1, un réseau IPv6 se compose des mêmes éléments qu'un réseau IPv4. Cependant, la terminologie IPv6 diffère légèrement de celle d'IPv4. Voici une liste des termes courants de composants de réseau tels qu'ils sont utilisés dans un contexte IPv6.

Nœud — Tout système disposant d'une adresse IPv6 et d'une interface configurée pour une prise en charge d'IPv6. Ce terme générique s'applique aux hôtes et aux routeurs.

Routeur IPv6 — Nœud transférant les paquets IPv6. Au moins une des deux interfaces du routeur doit être configurée afin d'assurer la prise en charge d'IPv6. Un routeur IPv6 peut également publier sur le réseau interne le préfixe de site IPv6 enregistré pour l'entreprise.

Hôte IPv6	Nœud avec adresse IPv6. Un hôte IPv6 peut disposer de plusieurs interfaces configurées pour une prise en charge d'IPv6. Tout comme dans IPv4, les hôtes IPv6 n'assurent pas le transfert de paquets.
Lien	Média réseau unique et contigu limité à l'une de ses extrémités par un routeur.
Voisin	Nœud IPv6 situé sur le même lien que le nœud local.
Sous-réseau IPv6	Segment administratif d'un réseau IPv6. Les composants d'un sous-réseau IPv6 peuvent correspondre directement avec tous les nœuds d'un lien, comme dans IPv4. Les nœuds d'un lien peuvent être administrés dans des sous-réseaux séparés si nécessaire. En outre, IPv6 prend en charge les sous-réseaux à liens multiples, dans lesquels les nœuds situés sur plusieurs liens peuvent être les composants d'un sous-réseau unique. Les liens 2 et 3 de la Figure 3–1 sont des composants du sous-réseau à liens multiples 8a.
Tunnel IPv6	Tunnel fournissant un chemin virtuel point à point entre un nœud IPv6 et l'extrémité d'un autre nœud IPv6. IPv6 prend en charge les tunnels configurables manuellement et les tunnels 6to4 automatiques.
Routeur de bordure	Routeur situé à la limite d'un réseau qui fournit l'une des extrémités du tunnel IPv6 à une extrémité située à l'extérieur du réseau local. Ce routeur doit disposer au moins d'une interface IPv6 avec le réseau interne. Pour le réseau externe, le routeur peut disposer d'une interface IPv6 ou IPv4.

Présentation de l'adressage IPv6

Les adresses IPv6 sont assignées à des interfaces, plutôt qu'à des nœuds, dans la mesure où un nœud peut disposer de plusieurs interfaces. De plus, vous pouvez assigner plusieurs adresses IPv6 à une interface.

Remarque – Pour obtenir des informations techniques complètes sur le format d'adresse IPv6, consultez le document RFC 2374, IPv6 Global Unicast Address Format (`http://www.ietf.org/rfc/rfc2374.txt?number=2374`)

IPv6 définit trois types d'adresse :

Unicast	Identifie l'interface d'un nœud individuel.

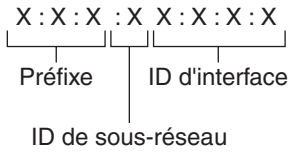
Multidiffusion Identifie un groupe d'interfaces, en règle générale sur des nœuds différents. Les paquets envoyés à l'adresse multidiffusion vont à tous les membres du *groupe multidiffusion*.

Anycast Identifie un groupe d'interfaces, en règle générale sur des nœuds différents. Les paquets envoyés à l'adresse anycast vont au nœud membre du *groupe anycast* le plus proche de l'expéditeur.

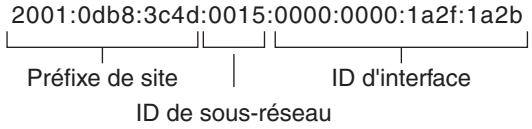
Parties de l'adresse IPv6

Une adresse IPv6 est longue de 128 bits et se compose de huit champs de 16 bits, chacun étant délimité par deux-points (:). Chaque champ doit contenir un nombre hexadécimal, à la différence de la notation en format décimal avec points des adresses IPv4. Dans l'illustration suivante, les x représentent des nombres hexadécimaux.

FIGURE 3–2 Format d'adresse IPv6 de base



Exemple :



Les trois champs situés complètement à gauche (48 bits) contiennent le *préfixe de site*. Le préfixe décrit la *topologie publique* allouée en général à votre site par un FAI ou un registre Internet régional (RIR, Regional Internet Registry).

Le champ suivant correspond à l'*ID de sous-réseau* de 16 bits alloué au site (par vous ou par un autre administrateur). L'ID de sous-réseau décrit la *topologie privée*, appelée également *topologie de site*, car elle est interne au site.

Les quatre champs les plus à droite (64 bits) contiennent l'*ID d'interface*, également appelée *jeton*. L'ID d'interface est soit configurée automatiquement à partir de l'adresse MAC de l'interface, soit configurée manuellement au format EUI-64.

Observez à nouveau l'adresse de l'illustration Figure 3–2 :

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

Cet exemple illustre les 128 bits d'une adresse IPv6. Les premiers 48 bits, `2001:0db8:3c4d`, contiennent le préfixe de site, représentant la topologie publique. Les 16 bits suivants, `0015`, contiennent l'ID de sous-réseau. Ils représentent la topologie privée du site. Les 64 bits situés complètement à droite, `0000:0000:1a2f:1a2b`, contiennent l'ID d'interface.

Abréviation d'adresses IPv6

En général, les adresses IPv6 n'occupent pas la totalité des 128 bits dont elles disposent. Par conséquent, certains champs sont renseignés partiellement ou en totalité par des zéros.

L'architecture d'adressage IPv6 vous permet d'utiliser la notation à deux points (: :) pour représenter les champs de zéros contigus de 16 bits. Vous pouvez par exemple raccourcir l'adresse IPv6 de la Figure 3–2 en remplaçant les deux champs de zéros contigus de l'ID d'interface par deux deux-points. L'adresse devient alors : `2001:0db8:3c4d:0015::1a2f:1a2b`. Les autres champs de zéros peuvent être représentés par un seul 0. Vous pouvez également omettre tout zéro de début d'un champ, en remplaçant par exemple `0db8` par `db8`.

Par conséquent, l'adresse `2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b` peut être raccourcie en `2001:db8:3c4d:15::1a2f:1a2b`.

Vous pouvez utiliser la notation à deux deux-points afin de remplacer les champs contigus composés de zéros de l'adresse IPv6. Par exemple, l'adresse IPv6 `2001:0db8:3c4d:0015:0000:d234::3eee:0000` peut être raccourcie en `2001:db8:3c4d:15:0:d234:3eee::`.

Préfixes d'IPv6

Les champs de l'adresse IPv6 situés complètement à gauche contiennent le préfixe utilisé pour le routage de paquets IPv6. Le format des préfixes IPv6 est le suivant :

préfixe/longueur en bits

La longueur du préfixe est indiquée en notation CIDR. La notation CIDR correspond à un slash (/) à la fin de l'adresse, suivi de la longueur du préfixe en bits. Pour de plus amples informations sur les adresses IP au format CIDR, reportez-vous à la section “Conception du schéma d'adressage IPv4 CIDR” à la page 61.

Le *préfixe de site* d'une adresse IPv6 occupe jusqu'à 48 des bits situés complètement à gauche de celle-ci. Par exemple, le préfixe de site de l'adresse IPv6

`2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48` réside dans les 48 bits situés complètement à gauche, soit `2001:db8:3c4d`. Vous pouvez représenter ce préfixe de la façon suivante, avec zéros compressés :

```
2001:db8:3c4d::/48
```

Remarque – Le préfixe `2001:db8::/32` est un préfixe IPv6 spécial utilisé spécifiquement dans les exemples de documentation.

Vous pouvez spécifier un *préfixe de sous-réseau* définissant la topologie interne du réseau vers un routeur. Le préfixe de sous-réseau de l'exemple d'adresse IPv6 est le suivant.

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

Le préfixe de sous-réseau contient toujours 64 bits. Ceux-ci se décomposent en 48 bits pour le préfixe de site et 16 bits pour l'ID de sous-réseau.

Les préfixes suivants sont réservés à un usage spécial :

`2002::/16` Indique qu'un préfixe de routage 6to4 suit.

`fe80::/10` Indique qu'une adresse lien-local suit.

`ff00::/8` Indique qu'une adresse multidiffusion suit.

Adresses unicast

IPv6 inclut deux assignations différentes d'adresses unicast :

- adresse unicast globale ;
- adresse lien-local.

Le type d'adresse unicast est déterminé par les bits contigus situés complètement à gauche de l'adresse, qui contiennent le préfixe.

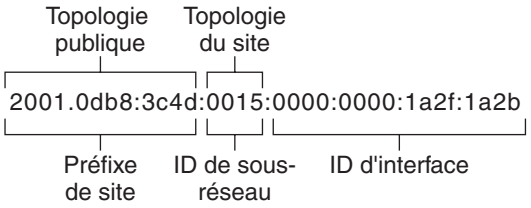
Le format d'adresse unicast est organisé selon la hiérarchie suivante :

- topologie publique ;
- topologie de site (privée) ;
- ID d'interface.

Adresse unicast globale

L'adresse unicast globale est unique au monde sur Internet. L'adresse IPv6 d'exemple figurant à la section "Préfixes d'IPv6" à la page 78 constitue une adresse unicast globale. L'illustration suivante représente l'étendue de l'adresse unicast globale, en comparaison avec les parties de l'adresse IPv6.

FIGURE 3–3 Parties de l'adresse unicast globale



Topologie publique

Le préfixe de site définit la *topologie publique* de votre réseau auprès d'un routeur. Vous pouvez obtenir le préfixe de site pour votre entreprise auprès d'un FAI ou d'un RIR (Regional Internet Registry, registre Internet régional).

Topologie de site et sous-réseaux IPv6

Dans IPv6, l'*ID de sous-réseau* définit un sous-réseau administratif du réseau ; sa longueur est de 16 bits maximum. L'assignation d'un ID de sous-réseau fait partie de la configuration de réseau IPv6. Le *préfixe de sous-réseau* définit la topologie du site vers un routeur en spécifiant le lien spécifique auquel a été assigné le sous-réseau.

Conceptuellement, les sous-réseaux IPv6 sont similaires aux sous-réseaux IPv4, dans la mesure où chaque sous-réseau est en général associé à un lien matériel unique. Cependant, les ID de sous-réseau IPv6 s'expriment en notation hexadécimale plutôt qu'en notation décimale avec points.

ID d'interface.

L'*ID d'interface* identifie l'interface d'un nœud donné. Un ID d'interface doit être unique au sein du sous-réseau. Les hôtes IPv6 peuvent utiliser le protocole de détection de voisins afin de générer automatiquement leurs propres ID d'interface. La détection de voisins génère automatiquement l'ID d'interface, en fonction de l'adresse MAC ou EUI-64 de l'interface de l'hôte. Vous pouvez également attribuer manuellement les ID d'interface ; cela est recommandé pour les routeurs IPv6 et les serveurs compatibles IPv6. Pour obtenir des instructions de

création manuelle d'adresses EUI-3513, reportez-vous au document RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture.

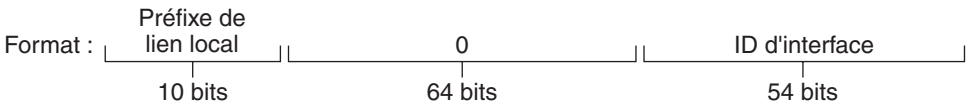
Adresses unicast transitionnelles globales

Le protocole IPv6 inclut, à des fins de transition, la capacité d'intégrer une adresse IPv4 dans une adresse IPv6. Ce type d'adresse IPv4 facilite la mise en tunnel de paquets IPv6 au travers de réseaux IPv4 existants. L'adresse 6to4 constitue un exemple d'adresse unicast transitionnelle globale. Pour de plus amples informations sur l'adressage 6to4, reportez-vous à la section "Tunnels automatiques 6to4" à la page 294.

Adresse unicast lien-local

L'adresse unicast lien-local s'utilise exclusivement sur le lien de réseau local. Les adresses lien-local ne sont ni valides ni reconnues en dehors de l'entreprise. L'exemple suivant représente le format de l'adresse lien-local.

EXEMPLE 3–1 Parties de l'adresse unicast lien-local



Exemple : fe80::123e:456d

Le format d'un *préfixe lien-local* est le suivant :

`fe80::`*ID-interface*`/10`

L'exemple suivant constitue une adresse lien-local :

```
fe80::23a1:b152
```

`fe80`	Représentation hexadécimale du préfixe binaire 10 bits 1111111010. Ce préfixe identifie le type d'adresse IPv6 comme étant un lien local.
ID-interface	Adresse hexadécimale de l'interface, dérivée en général de l'adresse MAC 48 bits.

Lorsque vous activez le protocole IPv6 lors de l'installation d'Oracle Solaris, l'interface avec le numéro le plus faible de l'ordinateur local est configurée avec une adresse de lien local. Chaque interface doit disposer d'au moins une adresse lien-local afin d'identifier le nœud auprès d'autres nœuds sur le lien local. Par conséquent, vous devez configurer manuellement les

adresses lien-local pour les interfaces supplémentaires d'un nœud. Une fois la configuration terminée, le nœud utilise ses adresses lien-local pour la configuration automatique d'adresses et la détection de voisins.

Adresses multicast

IPv6 prend en charge l'utilisation d'adresses multicast. L'adresse multicast identifie un *groupe multicast*, qui correspond à un groupe d'interfaces, en règle générale sur des nœuds différents. Une interface peut faire partie d'un nombre indéfini de groupes multicast. Si les premiers 16 bits d'une adresse IPv6 sont `ff00` *n*, il s'agit d'une adresse multicast.

Les adresses multicast sont utilisées pour l'envoi d'informations ou de services à toutes les interfaces définies en tant que membres du groupe multicast. Par exemple, les adresses multicast s'utilisent entre autres afin de communiquer avec tous les nœuds IPv6 du lien local.

Lors de la création de l'adresse unicast IPv6 d'une interface, le noyau ajoute automatiquement l'interface à un certain nombre de groupes multicast. Par exemple, chaque nœud est ajouté par le noyau au groupe multicast Solicited Node, qui est utilisé par le protocole de détection de voisins afin de détecter l'accessibilité. En outre, le noyau ajoute automatiquement un nœud aux groupes multicast All-Nodes ou All Routers.

Pour obtenir des informations détaillées sur les adresses multicast, reportez-vous à la section "Présentation détaillée des adresses IPv6 multicast" à la page 264. Pour obtenir des informations techniques, reportez-vous au document RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses (`ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt`). Le format d'adresse multicast y est décrit. Pour plus d'informations sur l'utilisation appropriée des adresses et des groupes multicast, reportez-vous au document RFC 3307, Allocation Guidelines for IPv6 Multicast Addresses (`ftp://ftp.rfc-editor.org/in-notes/rfc3307.txt`).

Adresses et groupes anycast

Les adresses anycast IPv6 identifient un groupe d'interfaces situées sur différents nœuds IPv6. Chaque groupe d'interfaces correspond à un *groupe anycast*. Lorsqu'un paquet est envoyé à l'adresse anycast, le membre du groupe anycast le plus proche de l'expéditeur reçoit le paquet.

Remarque – L'implémentation du protocole IPv6 dans Oracle Solaris n'est pas compatible avec la création de groupes et d'adresses anycast. Cependant, les nœuds IPv6 Oracle Solaris peuvent envoyer des paquets à des adresses anycast. Pour de plus amples informations, reportez-vous à la section "Informations importantes pour la création de tunnels vers un routeur relais 6to4" à la page 297.

Présentation du protocole de détection de voisins IPv6

IPv6 introduit le protocole de détection de voisins, qui utilise la messagerie pour gérer les interactions entre nœuds voisins. Les *nœuds voisins* sont des nœuds IPv6 situés sur le même lien. Par exemple, un nœud peut connaître l'adresse lien-local d'un voisin grâce à l'émission de messages relatifs à la détection de voisins. La détection de voisins contrôle les activités principales suivantes de lien local IPv6 :

- **Détection de routeur** : aide les hôtes à localiser les routeurs sur le lien local.
- **Configuration automatique d'adresse** : permet à un nœud de configurer automatiquement les adresses IPv6 pour ses interfaces.
- **Détection de préfixe** : permet aux nœuds de détecter les préfixes de sous-réseau connus alloués à un lien. Les nœuds utilisent les préfixes afin de faire la distinction entre les destinations situées sur le lien local et celles qu'il n'est possible d'atteindre que par le biais d'un routeur.
- **Résolution d'adresse** : permet aux nœuds de déterminer l'adresse lien-local d'un voisin, uniquement à l'aide de l'adresse IP de la destination.
- **Détermination du prochain saut** : utilise un algorithme afin de déterminer l'adresse IP d'un destinataire de paquet un saut au-delà du lien local. Le prochain saut peut être un routeur ou le nœud de destination.
- **Détection d'inaccessibilité de voisin** : aide les nœuds à déterminer si un voisin est désormais inaccessible. Il est possible de répéter la résolution d'adresse pour les routeurs et les hôtes.
- **Détection d'adresses dupliquées** : permet à un nœud de déterminer si une adresse qu'il souhaite utiliser n'est pas déjà en cours d'utilisation.
- **Redirection** : permet à un routeur d'informer un hôte de l'existence d'un nœud premier saut plus adéquat pour atteindre une destination particulière.

La détection de voisins utilise les types de messages IMCP suivants afin de communiquer parmi les nœuds sur un lien :

- sollicitation de routeur ;
- publication de routeur ;
- sollicitation de voisin ;
- publication de voisin ;
- réacheminement.

Pour obtenir des informations sur les messages de détection de voisins et sur d'autres sujets relatifs au protocole de détection de voisins, reportez-vous à la section "Protocole ND IPv6" à la page 282. Pour obtenir des informations techniques sur le protocole Neighbor Discovery, reportez-vous au document, RFC 2461, Neighbor Discovery for IP Version 6 (IPv6) (`http://www.ietf.org/rfc/rfc2461.txt?number=2461`).

Configuration automatique d'adresse IPv6

Une des fonctions principales d'IPv6 correspond à la capacité de l'hôte à configurer automatiquement une interface. La détection de voisins permet à l'hôte de localiser un routeur IPv6 sur le lien local et d'émettre une requête de préfixe de site. L'hôte effectue les tâches suivantes dans le cadre du processus de configuration automatique :

- création d'une adresse lien-local pour chaque interface ne nécessitant pas de routeur sur le lien ;
- vérification de l'unicité de l'adresse d'un lien ne nécessitant pas de routeur sur le lien ;
- définition du mode d'obtention des adresses globales, soit à l'aide du mécanisme sans état, soit du mécanisme avec état, soit à l'aide des deux mécanismes (requiert un routeur sur le lien).

Présentation de la configuration automatique sans état

La configuration automatique sans état ne nécessite aucune configuration manuelle des hôtes, une configuration minimale (voire aucune) des routeurs et aucun serveur supplémentaire. Le mécanisme sans état permet à un hôte de générer ses propres adresses. Le mécanisme sans état utilise des informations locales et non locales publiées par les routeurs pour la génération d'adresses.

Vous pouvez implémenter des adresses temporaires pour une interface, lesquelles sont également configurées automatiquement. Vous activez un jeton d'adresse temporaire pour une ou plusieurs interfaces sur un hôte. Cependant, à la différence des adresses IPv6 standard configurées automatiquement, une adresse temporaire se compose du préfixe de site et d'un numéro de 64 bits généré aléatoirement. Ce numéro aléatoire devient la partie d'ID d'interface de l'adresse IPv6. Une adresse lien-local n'est pas générée avec l'adresse temporaire en tant qu'ID d'interface.

Les routeurs publient tous les préfixes assignés sur le lien. Les hôtes IPv6 utilisent la détection de voisins afin d'obtenir un préfixe de sous-réseau d'un routeur local. Les hôtes créent des adresses IPv6 automatiquement en combinant le préfixe de sous-réseau avec l'ID d'interface généré à partir de l'adresse MAC d'une interface. En l'absence de routeur, un hôte génère uniquement des adresses lien-local. Les adresses lien-local s'utilisent exclusivement pour la communication avec les nœuds sur un même lien.

Remarque – N'utilisez pas la configuration automatique sans état pour la création d'adresses IPv6 de serveurs. Les hôtes génèrent automatiquement des ID d'interface basés sur des informations spécifiques au matériel lors de la configuration automatique. L'ID d'interface actuel pourrait devenir incorrecte en cas de remplacement de l'interface par une nouvelle interface.

Présentation des tunnels IPv6

Dans la plupart des entreprises, l'introduction du protocole IPv6 sur un réseau IPv4 doit s'effectuer progressivement. L'environnement de réseau à double pile Oracle Solaris prend en charge à la fois les fonctionnalités IPv4 et IPv6. Comme la plupart des réseaux utilisent le protocole IPv4, il est impossible aux réseaux IPv6 de communiquer sans tunnels.

En général, la création de tunnels IPv6 inclut l'encapsulation du paquet IPv6 sortant dans un paquet IPv4. Le routeur de bordure du réseau IPv6 configure un tunnel point à point sur plusieurs réseaux IPv4 jusqu'au routeur de bordure du réseau IPv6 de destination. Le paquet passe ensuite à travers le tunnel jusqu'au routeur de bordure du réseau cible qui le décapsule. Enfin, le routeur transmet le paquet IPv6 distinct au noeud de destination.

L'implémentation du protocole IPv6 sous Oracle Solaris prend en charge les scénarios de mise en tunnel suivants :

- Configuration manuelle d'un tunnel entre les deux réseaux IPv6 sur le réseau IPv4. Le réseau IPv4 peut correspondre à un réseau Internet ou au réseau local d'une entreprise.
- Configuration manuelle d'un tunnel entre les deux réseaux IPv4 sur un réseau IPv6 (généralement de l'entreprise).
- Configuration automatique et dynamique d'un tunnel 6to4 entre les deux réseaux IPv6 sur le réseau IPv4 d'une entreprise ou sur un réseau Internet.

Pour de plus amples informations sur les tunnels IPv6, reportez-vous à la section "Tunnels IPv6" à la page 290. Pour de plus amples informations sur les tunnels IPv4-to-IPv4 et VPN, reportez-vous à la section "Réseaux privés virtuels et IPsec" à la page 510.

◆ ◆ ◆ CHAPITRE 4

Planification d'un réseau IPv6 (tâches)

Le déploiement d'IPv6 sur un réseau, nouveau ou existant, requiert un grand effort de planification. Ce chapitre décrit les tâches de planification requise avant de configurer IPv6 sur votre site. Dans le cas de réseaux existants, le déploiement d'IPv6 doit s'effectuer progressivement. Les rubriques de ce chapitre vous permettent d'effectuer une introduction progressive d'IPv6 dans un réseau exclusivement IPv4 à l'origine.

Ce chapitre examine les rubriques suivantes :

Le Chapitre 3, "Présentation d'IPv6" présente les concepts d'IPv6. Pour obtenir des informations détaillées, reportez-vous au Chapitre 11, "Présentation détaillée de IPv6 (référence)".

Planification IPv6 (liste des tâches)

Effectuez les tâches de la liste suivante dans l'ordre afin de planifier les tâches nécessaires au déploiement d'IPv6.

Le tableau suivant répertorie les différentes tâches de configuration du réseau IPv6. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

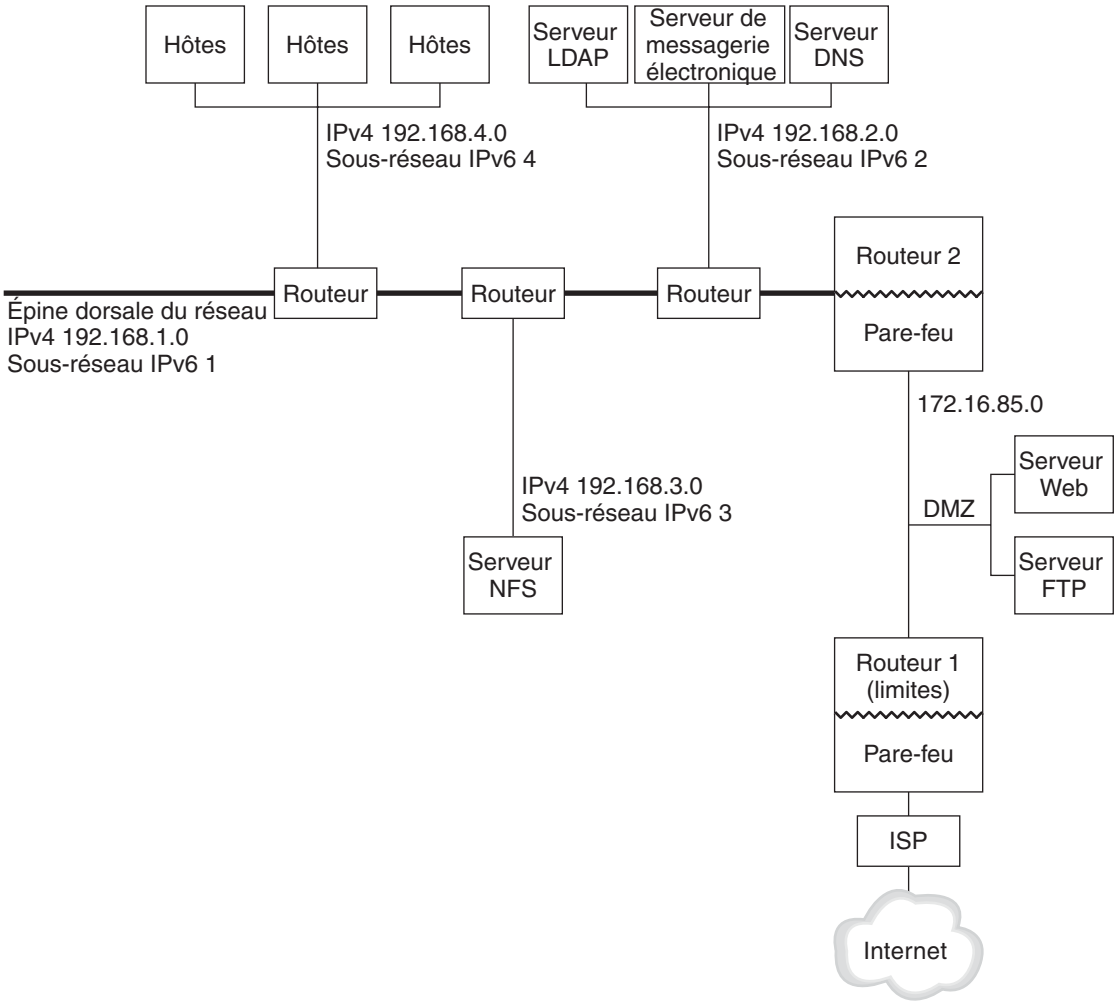
Tâche	Description	Voir
1. Préparation du matériel pour qu'il prenne en charge IPv6.	Vérifiez qu'il est possible de mettre le matériel à niveau vers IPv6.	"Préparation de la topologie réseau pour une prise en charge d'IPv6" à la page 91

Tâche	Description	Voir
2. Obtention d'un FAI prenant en charge IPv6.	Assurez-vous que votre FAI actuel prend en charge le protocole IPv6. Dans le cas contraire, trouvez un FAI prenant en charge IPv6. Vous pouvez faire appel à deux FAI : l'un pour IPv6, l'autre pour les communications IPv4.	
3. Vérification de la compatibilité des applications avec IPv6.	Assurez-vous que les applications peuvent s'exécuter dans un environnement IPv6.	“Procédure de préparation de services réseau pour la prise en charge d'IPv6” à la page 92
4. Obtention d'un préfixe de site.	Obtenez un préfixe de site de 48 octets pour votre site auprès de votre FAI ou du registre Internet régional le plus proche.	“Obtention d'un préfixe de site” à la page 95
5. Créer un plan d'adressage de sous-réseau.	Vous devez planifier la topologie globale du réseau IPv6 ainsi que le schéma d'adressage avant de configurer IPv6 sur les différents nœuds de votre réseau.	“Création d'un schéma de numérotation pour les sous-réseaux” à la page 96
6. Conception d'un plan pour l'utilisation de tunnels.	Déterminez les routeurs qui vont exécuter les tunnels vers d'autres sous-réseaux ou des réseaux externes.	“Planification de tunnels dans la topologie réseau” à la page 94
7. Création d'un plan d'adressage pour les entités du réseau.	Vous devez disposer au préalable d'un plan pour l'adressage des serveurs, des routeurs et des hôtes avant d'effectuer la configuration d'IPv6.	“Création d'un plan d'adressage IPv6 pour les nœuds” à la page 96
8. Développement d'une stratégie de sécurité IPv6.	Vérifiez les filtres IP, l'architecture de sécurité IP (IPsec), la fonction d'échange de clés Internet (IKE, Internet Key Exchange) et les autres fonctionnalités de sécurité d'Oracle Solaris lors de la création de la stratégie de sécurité IPv6.	Partie IV
9. (Facultatif) Paramétrage d'une DMZ.	Pour des raisons de sécurité, vous devez disposer d'un plan d'adressage pour la DMZ et ses entités avant de configurer IPv6.	“Considérations de sécurité relatives à l'implémentation d'IPv6” à la page 94
10. Activation de la prise en charge d'IPv6 par les nœuds.	Configurez IPv6 sur tous les routeurs et les hôtes.	“Configuration de routeur IPv6 (liste des tâches)” à la page 179
11. Activation des services réseau.	Assurez-vous que les serveurs existants prennent en charge IPv6.	“Principales tâches d'administration TCP/IP (liste des tâches)” à la page 208
12. Mise à jour des noms de serveurs pour la prise en charge d'IPv6.	Assurez-vous que les serveurs DNS, NIS et LDAP sont mis à jour avec les nouvelles adresses IPv6.	“Configuration de prise en charge de services d'attribution de noms pour IPv6” à la page 201

Scénario de topologie de réseau IPv6

Les tâches de ce chapitre permettent de planifier des services IPv6 dans un réseau d'entreprise typique. L'illustration suivante correspond au réseau auquel il est fait référence tout au long du chapitre. Le réseau IPv6 proposé peut inclure une partie ou la totalité des liaisons réseau figurant dans l'illustration.

FIGURE 4–1 Scénario de topologie de réseau IPv6



Le scénario de réseau d'entreprise se compose de cinq sous-réseaux disposant d'adresses IPv4. Les liaisons du réseau correspondent directement aux sous-réseaux administratifs. Les quatre

réseaux internes sont affichés avec des adresses IPv4 privées de type RFC 1918, ce qui correspond à une solution courante pour le manque d'adresses IPv4. Le schéma d'adressage de ces réseaux internes est comme suit :

- Le sous-réseau 1 correspond à l'épine dorsale du réseau interne `192.168.1`.
- Le sous-réseau 2 correspond au réseau interne `192.168.2`, avec LDAP, `sendmail` et serveurs DNS.
- Le sous-réseau 3 correspond au réseau interne `192.168.3`, avec les serveurs NFS de l'entreprise.
- Le sous-réseau 4 correspond au réseau interne `192.168.4` qui contient les hôtes des employés de l'entreprise.

Le réseau public externe `172.16.85` fait office de DMZ pour l'entreprise. Ce réseau contient des serveurs Web, des serveurs FTP anonymes et d'autres ressources que l'entreprise propose au monde extérieur. Le routeur 2 exécute un pare-feu et sépare le réseau public `172.16.85` de l'épine dorsale interne. Sur l'autre extrémité de la DMZ, le routeur 1 exécute un pare-feu et fait office de serveur de limites de l'entreprise.

Sur la Figure 4–1, la DMZ publique possède l'adresse privée RFC 1918 `172.16.85`. Dans le monde réel, la DMZ publique doit disposer d'une adresse IPv4 enregistrée. La plupart des sites IPv4 utilisent une combinaison d'adresses publiques et d'adresses privées RFC 1918. Cependant, lors de l'introduction d'IPv6, le concept d'adresses publiques et privées est modifié. Dans la mesure où IPv6 dispose d'un espace d'adresse beaucoup plus important, les adresses publiques IPv6 s'utilisent à la fois sur les réseaux privés et publics.

Préparation du réseau existant à la prise en charge d'IPv6

Remarque – Le protocole double pile Oracle Solaris prend en charge à la fois les opérations IPv4 et IPv6. Vous pouvez effectuer des opérations liées à IPv4 pendant et après le déploiement d'IPv6 sur votre réseau.

IPv6 introduit des fonctionnalités supplémentaires dans un réseau existant. Par conséquent, lors du premier déploiement d'IPv6, vous devez vous assurer de ne pas perturber les opérations fonctionnant avec IPv4. Les sujets abordés dans cette section décrivent une méthode pas à pas d'introduction d'IPv6 dans un réseau existant.

Préparation de la topologie réseau pour une prise en charge d'IPv6

La première étape du déploiement IPv6 consiste à déterminer les entités existantes sur votre réseau prenant en charge IPv6. Dans la plupart des cas, la topologie du réseau (les câbles, les routeurs et les hôtes) n'est pas modifiée par l'implémentation d'IPv6. Cependant, dans certains cas, il est nécessaire de préparer le matériel et les applications existantes pour IPv6 avant d'effectuer la configuration des adresses IPv6 sur les interfaces réseau.

Assurez-vous que le matériel de votre réseau peut être mis à niveau vers IPv6. Par exemple, consultez la documentation du fabricant en matière de compatibilité IPv6 en ce qui concerne les classes de matériel suivantes :

- routeurs ;
- pare-feux ;
- serveurs ;
- commutateurs.

Remarque – Toutes les procédures décrites dans cette partie partent du principe qu'il est possible de mettre le matériel à niveau (en particulier les routeurs) vers IPv6.

Certains modèles de routeurs ne permettent pas une mise à niveau vers IPv6. Pour obtenir des informations supplémentaire et une solution au problème, reportez-vous à la section "Impossible de mettre à niveau un routeur IPv4 vers IPv6" à la page 235.

Préparation de services réseau pour la prise en charge d'IPv6

Les services réseau IPv4 suivants de la version active d'Oracle Solaris sont compatibles avec le protocole IPv6 :

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

Le service de messagerie IMAP est compatible uniquement avec IPv4.

Les nœuds configurés pour IPv6 peuvent exécuter des services IPv4. Lors de l'activation d'IPv6, tous les services n'acceptent pas les connexions IPv6. Les services préparés pour IPv6 acceptent les connexions. Les services qui ne le sont pas continuent de fonctionner avec la partie IPv4 de la pile de protocole.

Certains problèmes peuvent survenir après une mise à niveau des services vers IPv6. Pour de plus amples informations, reportez-vous à la section "Problèmes survenant après la mise à niveau de services vers IPv6" à la page 235.

Préparation de serveurs pour une prise en charge d'IPv6

Les serveurs étant considérés comme des hôtes IPv6, par défaut, leurs adresses IPv6 sont automatiquement configurées par le protocole de détection des voisins. Cependant, de nombreux serveurs possèdent plusieurs cartes d'interface réseau et il peut s'avérer nécessaire de les retirer en vue de leur maintenance ou de leur remplacement. Lorsqu'une carte d'interface réseau est remplacée, la détection de voisins génère automatiquement un nouvel ID d'interface pour cette carte. Ce comportement pourrait s'avérer problématique pour un serveur.

Par conséquent, il est conseillé de configurer manuellement la partie ID d'interface des adresses IPv6 pour chaque interface du serveur. Pour obtenir des instructions, reportez-vous à la section "Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur" à la page 188. Si le remplacement d'une carte d'interface réseau est nécessaire ultérieurement, l'adresse IPv6 configurée est appliquée à la carte de substitution.

▼ Procédure de préparation de services réseau pour la prise en charge d'IPv6

1. **Mettez les services réseau suivants à jour afin qu'ils prennent en charge IPv6 :**
   - serveurs de courrier.
   - serveurs NIS ;
   - NFS

   Remarque – LDAP prend en charge IPv6 sans aucune configuration supplémentaire nécessaire.

2. **Assurez-vous que le matériel de votre pare-feu est compatible avec le protocole IPv6.**

   Reportez-vous à la documentation adéquate pour obtenir des instructions.

3. **Assurez-vous que les autres services de votre réseau ont été préparés pour prendre en charge le protocole IPv6.**

   Pour de plus amples informations, reportez-vous à la documentation technique et marketing du logiciel.

4. **Si votre site déploie les services suivante, assurez-vous d'avoir pris les mesures adéquates pour ces services :**

   - pare-feux ;

     Pensez à renforcer les stratégies en place pour le protocole IPv4 afin qu'elles prennent en charge le protocole IPv6. Pour prendre connaissance de problèmes de sécurité supplémentaires, reportez-vous à la section "Considérations de sécurité relatives à l'implémentation d'IPv6" à la page 94.

   - Messagerie

     Vous pouvez envisager d'ajouter les adresses IPv6 de votre serveur de messagerie aux enregistrements MX pour DNS.

   - DNS

     Pour prendre connaissance des considérations spécifiques à DNS, reportez-vous à la section "Procédure de préparation de DNS pour la prise en charge d'IPv6" à la page 93.

   - IPQoS

     Utilisez les mêmes stratégies Diffserv que celles utilisées pour le protocole IPv4 sur l'hôte. Pour de plus amples informations, reportez-vous à la section "Module de classification" à la page 885.

5. **Contrôlez tout service réseau offert par un nœud avant de convertir ce dernier vers IPv6.**

▼ Procédure de préparation de DNS pour la prise en charge d'IPv6

La version d'Oracle Solaris actuelle prend en charge la résolution de DNS côté client et côté serveur. Procédez comme suit pour préparer les services DNS à IPv6.

Pour obtenir des informations supplémentaires relatives à la prise en charge de DNS pour IPv6, reportez-vous à la section *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

1. **Assurez-vous que le serveur DNS effectuant la résolution récursive de nom est double pile (IPv4 et IPv6) ou uniquement compatible avec IPv4.**

2. **Dans le serveur DNS, renseignez la base de données DNS avec les enregistrements AAAA de base de données IPv6 dans la zone de transfert.**

Remarque – Les serveurs exécutant plusieurs services critiques requièrent une attention particulière. Assurez-vous du bon fonctionnement du réseau. En outre, tous les services critiques doivent avoir été préparés pour IPv6. Ensuite, ajoutez l'adresse IPv6 du serveur à la base de données DNS.

3 **Ajoutez les enregistrements PTR associés aux enregistrements AAAA dans la zone d'inversion.**

4 **Ajoutez des données exclusivement IPv4 ou des données IPv6 et IPv4 à l'enregistrement NS décrivant les zones.**

Planification de tunnels dans la topologie réseau

L'implémentation d'IPv6 prend en charge un certain nombre de configurations de tunnel faisant office de mécanismes de transition lors de la migration de votre réseau vers un mélange d'IPv4 et d'IPv6. Les tunnels permettent aux réseaux IPv6 isolés de communiquer. Dans la mesure où Internet exécute essentiellement IPv4, les paquets IPv6 de votre site doivent circuler dans Internet via des tunnels ayant pour destination des réseaux IPv6.

Vous trouverez ici les scénarios les plus courants d'utilisation de tunnels dans la topologie de réseau IPv6 :

- Le FAI qui vous fournit des services IPv6 vous permet de créer un tunnel à partir du routeur de bordure du site vers le réseau du FAI. La Figure 4–1 représente un de ces tunnels. Dans ce cas, vous devez exécuter un tunnel manuel IPv6 sur IPv4.
- Vous gérez un réseau distribué de grande taille avec connectivité IPv4. Pour connecter les sites distribués utilisant IPv6, vous pouvez exécuter un tunnel automatique 6to4 à partir du routeur de périphérie de chaque sous-réseau.
- Il est parfois impossible de mettre un routeur à niveau vers IPv6 dans l'infrastructure de l'entreprise. Dans ce cas, vous pouvez créer un tunnel manuel à travers le routeur IPv4, avec deux routeurs IPv6 en guise d'extrémités.

La section "Tâches de configuration de tunnels pour la prise en charge d'IPv6 (liste des tâches)" à la page 191 contient les procédures de configuration des tunnels. Pour des informations conceptuelles à propos des tunnels, reportez-vous à la section "Tunnels IPv6" à la page 290.

Considérations de sécurité relatives à l'implémentation d'IPv6

En cas d'introduction d'IPv6 dans un réseau existant, veillez à ne pas compromettre la sécurité du site. Tenez compte des problèmes de sécurité suivants lors de l'implémentation progressive d'IPv6 :

- La même quantité de filtrage est requise pour les paquets IPv6 et IPv4.
- Les paquets IPv6 sont souvent mis en tunnel via un pare-feu. Par conséquent, implémentez l'un des deux scénarios suivants :
  - Paramétrez le pare-feu de sorte qu'il inspecte le contenu du tunnel.
  - Placez un pare-feu IPv6 avec des règles similaires à l'extrémité opposée du tunnel.
- Certains mécanismes de transition utilisent des tunnels IPv6 sur UDP sur IPv4. Ces mécanismes peuvent s'avérer dangereux et court-circuiter le pare-feu.
- Globalement, il est possible d'atteindre les nœuds IPv6 à partir de l'extérieur du réseau de l'entreprise. Si votre stratégie de sécurité interdit tout accès public, vous devez établir des règles de pare-feu plus strictes. Vous pourriez par exemple configurer un pare-feu avec état.

Ce manuel inclut des fonctionnalités de sécurité qu'il est possible d'utiliser dans une implémentation IPv6.

- La fonction d'architecture IPsec (sécurité IP) permet d'obtenir une protection cryptographique des paquets IPv6. Pour plus d'informations, reportez-vous au Chapitre 19, “Architecture IPsec (présentation)”.
- La fonctionnalité IKE (Internet Key Exchange, échange de clé Internet) permet d'utiliser l'authentification de clé publique pour les paquets IPv6. Pour plus d'informations, reportez-vous au Chapitre 22, “Protocole IKE (présentation)”.

Préparation d'un plan d'adressage IPv6

Le développement d'un plan d'adressage constitue une des parties les plus importantes de la transition d'IPv4 à IPv6. Cette tâche nécessite les préparatifs suivants :

- “Obtention d'un préfixe de site” à la page 95
- “Création du schéma de numérotation IPv6” à la page 96

Obtention d'un préfixe de site

Vous devez disposer d'un préfixe de site préalablement à la configuration d'IPv6. Le préfixe de site permet de dériver les adresses IPv6 pour tous les nœuds de votre implémentation IPv6. Pour une présentation des préfixes de site, reportez-vous à la section “Préfixes d'IPv6” à la page 78.

Tout FAI prenant en charge IPv6 devrait être en mesure de fournir un préfixe de site IPv6 de 48 octets. Si votre FAI ne prend en charge que IPv4, vous pouvez faire appel à un autre FAI pour la prise en charge d'IPv6 tout en conservant votre FAI actuel pour la prise en charge d'IPv4. Dans ce cas, il existe plusieurs solutions au problème. Pour de plus amples informations, reportez-vous à la section “Le FAI actuel ne prend pas en charge IPv6” à la page 235.

Si votre entreprise est un FAI, les préfixes de site pour vos clients s'obtiennent auprès du registre Internet adéquat. Pour plus d'informations, reportez-vous au site Internet Assigned Numbers Authority (IANA) (`http://www.iana.org`).

Création du schéma de numérotation IPv6

Si votre réseau IPv6 n'est pas entièrement nouveau, basez le schéma de numérotation IPv6 sur la topologie IPv4 existante.

Création d'un schéma de numérotation pour les sous-réseaux

Commencez par mapper les sous-réseaux IPv4 existants vers les sous-réseaux IPv6 équivalents. Par exemple, utilisez les sous-réseaux illustrés sur la Figure 4–1. Les sous-réseaux 1 à 4 utilisent l'identification d'adresse privée IPv4 RFC 1918 pour les 16 premiers octets de leurs adresses, en plus des chiffres 1 à 4 qui identifient le sous-réseau. Par exemple, supposons que le préfixe IPv6 `2001:db8:3c4d/48` a été assigné au site.

Le tableau suivant illustre le mappage des préfixes IPv4 privés vers les préfixes IPv6.

Préfixe de sous-réseau IPv4	Préfixe de sous-réseau IPv6 équivalent
`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`

Création d'un plan d'adressage IPv6 pour les nœuds

Pour la plupart des hôtes, la configuration automatique d'adresses IPv6 sans état pour leurs interfaces constitue une stratégie adéquate et rapide. Lorsque l'hôte reçoit le préfixe de site en provenance du routeur le plus proche, la détection de voisin génère automatiquement des adresses IPv6 pour chaque interface de l'hôte.

Les serveurs doivent disposer d'adresses IPv6 stables. Si vous ne configurez pas manuellement les adresses IPv6 d'un serveur, une nouvelle adresse IPv6 est configurée automatiquement à chaque fois qu'une carte d'interface réseau est remplacée sur le serveur. Tenez compte des conseils suivants lors de la création d'adresses de serveurs :

- Attribuez aux serveurs des ID d'interface significatifs et stables. Vous pouvez par exemple utiliser un schéma de numérotation séquentiel pour les ID d'interface. Par exemple, l'interface interne du serveur LDAP dans la Figure 4–1 pourrait devenir `2001:db8:3c4d:2::2`.

- Si vous ne renommez pas régulièrement votre réseau IPv4, vous pouvez également utiliser les adresses IPv4 des routeurs et serveurs en tant qu'ID d'interface. Dans la Figure 4–1, on suppose que l'interface du routeur 1 vers la DMZ a pour adresse IPv4 `123.456.789.111`. Vous pouvez convertir l'adresse IPv4 vers le format hexadécimale et utiliser le résultat de la conversion en tant qu'ID d'interface. Le nouvel ID d'interface serait `::7bc8:156F`.

  Cette approche est applicable uniquement si vous êtes propriétaire de l'adresse IPv4 enregistrée, non pas si vous l'avez obtenue auprès d'un FAI. Si vous utilisez une adresse IPv4 qui vous a été fournie par un FAI, vous créez une dépendance qui risque d'entraîner des problèmes en cas de changement de FAI.

En raison du nombre limité d'adresses IPv4, un concepteur de réseau devait auparavant se demander s'il devait utiliser des adresses globales enregistrées ou des adresses privées RFC 1918. Cependant, la notion d'adresses IPv4 privées et publiques ne s'applique pas aux adresses IPv6. Vous pouvez utiliser des adresses globales unicast incluant le préfixe de site, sur toutes les liaisons du réseau, DMZ publique incluse.

◆ ◆ ◆ CHAPITRE 5

Configuration des services réseau TCP/IP et de l'adressage IPv4 (tâches)

L'administration réseau TCP/IP comporte deux étapes. La première correspond à l'assemblage matériel. La seconde consiste à configurer les démons, fichiers et services de mise en œuvre du protocole TCP/IP.

Le présent chapitre décrit la configuration TCP/IP sur un réseau implémentant les services et l'adressage IPv4.

Remarque – De nombreuses tâches abordées dans ce chapitre s'appliquent aussi bien aux réseaux IPv4 uniquement qu'aux réseaux IPv6. En cas de différence des étapes de configuration des deux formats d'adressage, les instructions se rapportent au format IPv4. Des renvois aux tâches IPv6 correspondantes décrites au Chapitre 7, “Configuration d'un réseau IPv6 (tâches)” sont inclus.

Le présent chapitre contient les informations suivantes :

Nouveautés

Les changements apportés dans Solaris 10 8/07 sont les suivants :

- La configuration et la gestion du routage peuvent s'effectuer à l'aide de l'utilitaire SMF (Service Management Facility, utilitaire de gestion de service) et non plus uniquement à l'aide de la commande `routeadm`. Pour plus d'informations, reportez-vous aux procédures et exemples décrits à la section "Transfert et routage de paquets sur des réseaux IPv4" à la page 117 et à la page de manuel `routeadm(1M)`.
- Le fichier `/etc/inet/ipnodes` est devenu obsolète. Comme expliqué dans chaque procédure, utilisez le chemin `/etc/inet/ipnodes` uniquement pour les versions précédentes d'Oracle Solaris 10.

Étapes préalables à la configuration d'un réseau IPv4 (liste des tâches)

Avant de configurer TCP/IP, effectuez les tâches répertoriées dans le tableau suivant. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Voir
1. Conception de la topologie réseau	Choisissez la configuration physique du réseau.	"Présentation de la topologie réseau" à la page 67 et "Topologie du système autonome IPv4" à la page 121
2. Obtention d'un numéro réseau via l'ISP (Internet Service Provider, fournisseur de services Internet) ou RIR (Regional Internet Registry, organisme d'enregistrement Internet local)	Obtenez un numéro réseau enregistré permettant les communications externes des systèmes de votre site.	"Conception du schéma d'adressage IPv4" à la page 60.
3. Programmation du plan d'adressage IPv4 du réseau Incluez l'adressage de sous-réseau, le cas échéant.	Élaborez le plan d'adressage à partir du numéro réseau.	"Conception du schéma d'adressage IPv4" à la page 60.
4. Assemblage du matériel réseau conformément à la topologie réseau Assurez-vous du bon fonctionnement du matériel.	Configurez les systèmes, médias réseau, routeurs, commutateurs, hubs et passerelles exposés dans la conception de la topologie réseau.	Manuels du matériel et "Présentation de la topologie réseau" à la page 67.

Tâche	Description	Voir
5. Assignation des adresses IPv4 et des noms d'hôtes à tous les systèmes du réseau	Assignez les adresses IPv4 pendant ou après l'installation d'Oracle Solaris dans les fichiers correspondants.	"Conception du schéma d'adressage IPv4" à la page 60 et "Modification de l'adresse IPv4 et des autres paramètres de configuration réseau" à la page 112
6. Exécution du logiciel de configuration requis par les routeurs et les interfaces réseau, le cas échéant	Configurez les routeurs et les hôtes multiréseaux.	"Planification des routeurs du réseau" à la page 66 et "Configuration d'un routeur IPv4" à la page 124 pour toute information sur les routeurs.
7. Identification du service de noms ou du service d'annuaire utilisé sur le réseau NIS, LDAP, DNS ou fichiers locaux.	Configurez le service de noms et/ou le service d'annuaire sélectionné.	*Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.
8. Sélection de noms de domaine pour le réseau, le cas échéant	Sélectionnez un nom de domaine pour votre réseau et enregistrez-le auprès de l'InterNIC.	*Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*

Choix des modes de configuration des hôtes

En tant qu'administrateur réseau, vous configurez TCP/IP pour une exécution sur les hôtes et sur les routeurs (le cas échéant). Les informations de configuration utilisées par ces systèmes peuvent se trouver dans des fichiers du système local ou dans des fichiers résidant sur d'autres systèmes du réseau. Les informations de configuration requises sont répertoriées ci-dessous :

- nom d'hôte de chaque système ;
- adresse IP de chaque système ;
- nom de domaine auquel chaque système appartient ;
- Routeur par défaut
- masque de réseau IPv4 utilisé sur le réseau de chaque système.

Un système qui obtient les informations de configuration TCP/IP à partir de fichiers locaux fonctionne en mode *Fichiers locaux*. Un système qui obtient les informations de configuration TCP/IP à partir d'un serveur réseau à distance fonctionne en mode *Client réseau*.

Systèmes devant s'exécuter en mode Fichiers locaux

Pour s'exécuter en mode Fichiers locaux, un système doit posséder des copies locales des fichiers de configuration TCP/IP. Ces fichiers sont décrits à la section "Fichiers de configuration TCP/IP" à la page 237. L'attribution d'un disque dédié, sans faire figure de configuration requise, est toutefois recommandée pour le système.

La plupart des serveurs doivent s'exécuter en mode Fichiers locaux. Cette exigence s'applique aux serveurs suivants :

- serveurs de configuration réseau ;
- serveurs NFS ;
- serveurs de noms fournissant les services NIS, LDAP ou DNS ;
- serveurs de courrier.

Les routeurs doivent également s'exécuter en mode Fichiers locaux.

Les systèmes fonctionnant exclusivement en tant que serveurs d'impression ne sont pas tenus de s'exécuter en mode Fichiers locaux. L'exécution des hôtes en mode Fichiers locaux est fonction de la taille du réseau.

Pour les réseaux de taille réduite, il est facile de gérer le volume de travail consacré à la maintenance de ces fichiers. Dans le cas d'un réseau desservant des centaines d'hôtes, la tâche est plus complexe, même si le réseau est divisé en plusieurs sous-domaines d'administration. Par conséquent, le mode Fichiers locaux se révèle moins efficace dans le cadre de réseaux de grande taille. Toutefois, le mode Fichiers locaux s'appliquent aux routeurs et serveurs, qui doivent pouvoir fonctionner de manière indépendante.

Serveurs de configuration réseau

Les *serveurs de configuration réseau* fournissent les informations de configuration TCP/IP aux hôtes configurés en mode Client réseau. Ces serveurs prennent en charge trois protocoles d'initialisation :

- RARP – le protocole RARP (Reverse Address Resolution Protocol) mappe les adresses Ethernet (48 bits) vers les adresses IPv4 (32 bits). En d'autres termes, il réalise l'opération inverse du protocole ARP. Lorsque vous utilisez RARP sur un serveur de configuration réseau, les hôtes exécutés en mode Client réseau obtiennent leur adresses IP et leurs fichiers de configuration TCP/IP à partir du serveur. Le démon `in.rarpd` active les services RARP. Pour plus d'informations, reportez-vous à la page de manuel `in.rarpd(1M)`.
- TFTP – Le protocole TFTP (Trivial File Transfer Protocol) transfère les fichiers d'un système distant à l'autre. Le démon `in.tftpd` exécute les services TFTP, qui autorisent le transfert de fichiers entre les serveurs de configuration réseau et leurs clients réseau. Pour plus d'informations, reportez-vous à la page de manuel `in.tftpd(1M)`.
- Bootparams – Le protocole Bootparams fournit les paramètres d'initialisation, requis par les clients chargés d'initialiser le réseau. Le démon `rpc.bootparamd` exécute ces services. Pour plus d'informations, reportez-vous à la page de manuel `bootparamd(1M)`.

Les serveurs de configuration réseau peuvent également être configurés en tant que serveurs de fichiers NFS.

Si vous configurez des hôtes en tant que clients réseau, vous devez aussi configurer au moins un système sur le réseau en tant que serveur de configuration réseau. En cas de division du réseau en sous-réseaux, vous devez configurer au moins un serveur de configuration réseau pour chaque sous-réseau doté de clients réseau.

Systèmes clients réseau

Les hôtes recevant leurs informations de configuration d'un serveur de configuration réseau fonctionnent en mode Client réseau. Les systèmes configurés en tant que clients réseau ne requièrent aucune copie locale des fichiers de configuration TCP/IP.

Le *mode Client réseau* simplifie la gestion des réseaux de grande taille. Il réduit le nombre de tâches de configuration à effectuer sur chaque hôte et garantit la conformité de tous les systèmes du réseau aux mêmes normes de configuration.

Le mode Client réseau peut être configuré sur tous les types d'ordinateur. Par exemple, vous pouvez configurer le mode client réseau sur des systèmes autonomes.

Configurations mixtes

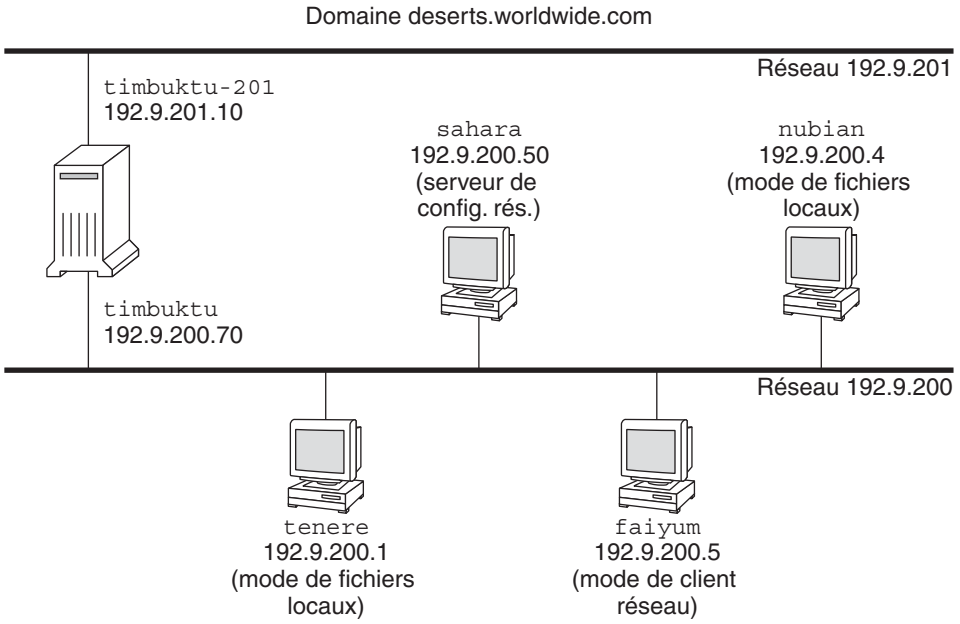
Les configurations ne se limitent pas aux modes Fichiers locaux uniquement ou Clients réseau uniquement. Les routeurs et les clients doivent toujours être configurés en mode local. En revanche, la configuration des hôtes peut combiner les modes Fichiers locaux et Clients réseau.

Scénario de topologie de réseau IPv4

La Figure 5–1 illustre les hôtes d'un réseau fictif présentant le numéro réseau `192.9.200`. Le serveur de configuration du réseau s'intitule `sahara`. Les hôtes `tenere` et `nubian` possèdent des disques qui leur sont propres et s'exécutent en mode Fichiers locaux. L'hôte `faiyum` dispose également d'un disque, mais s'exécute en mode Clients réseau

Enfin, le système `timbuktu` est configuré comme un routeur. Il inclut deux interfaces réseau. La première, intitulée `timbuktu`, appartient au réseau `192.9.200`. La seconde, `timbuktu-201`, appartient au réseau `192.9.201` . Les deux réseaux résident dans le domaine d'organisation `deserts.worldwide.com` Le domaine utilise des fichiers locaux comme service de nom.

FIGURE 5–1 Hôtes dans un scénario de topologie de réseau IPv4



Ajout d'un sous-réseau à un réseau (liste des tâches)

Si vous remplacez un réseau sans sous-réseau par un réseau avec sous-réseau, suivez la procédure ci-dessous.

Remarque – Les informations contenues dans cette section ne s'appliquent qu'aux sous-réseaux IPv4. Pour plus d'informations sur la planification des sous-réseaux IPv6, reportez-vous aux sections "Préparation de la topologie réseau pour une prise en charge d'IPv6" à la page 91 et "Création d'un schéma de numérotation pour les sous-réseaux" à la page 96.

Le tableau suivant répertorie la liste des tâches permettant d'ajouter un sous-réseau au réseau en cours. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Voir
1. Identification des besoins en sous-réseaux de la topologie réseau	Décidez de la nouvelle topologie de sous-réseau, notamment de l'emplacement des routeurs et hôtes sur les sous-réseaux.	"Planification des routeurs du réseau" à la page 66, "Qu'est-ce que la création de sous-réseaux ?" à la page 244 et "Classes de réseau" à la page 258
2. Assignation des adresses IP avec le nouveau numéro de sous-réseau aux systèmes qui doivent devenir membres du sous-réseau.	Configurez les adresses IP utilisant le nouveau numéro de sous-réseau lors de l'installation d'Oracle Solaris ou ultérieurement dans le fichier `/etc/hostname.`*interface*.	"Choix du format d'adressage IP du réseau" à la page 55
3. Configuration du masque du sous-réseau sur tous les systèmes potentiels du sous-réseau	Dans le cadre d'une configuration manuelle des clients réseau, modifiez le fichier `/etc/inet/netmasks`. Dans le cas contraire, indiquez le masque de réseau au programme d'installation Oracle Solaris.	"Base de données `netmasks`" à la page 244 et "Création du masque de réseau des adresses IPv4" à la page 245
4. Modification des bases de données réseau par rapport aux nouvelles adresses IP de tous les systèmes du sous-réseau	Modifiez `/etc/inet/hosts` et, pour Solaris 10 11/06 ou versions antérieures,`/etc/inet/ipnodes`, sur tous les hôtes afin de prendre en compte les nouvelles adresses hôte.	"Base de données `hosts`" à la page 239
5. Réinitialisation de tous les systèmes		

Liste des tâches de la configuration réseau

Le tableau suivant répertorie les tâches supplémentaires à effectuer une fois que vous êtes passé d'une configuration réseau sans sous-réseaux à un réseau utilisant des sous-réseaux. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Voir
Configuration d'un hôte en mode Fichiers locaux	Modification des fichiers `nodename`, `hostname`, `hosts`, `defaultdomain`, `defaultrouter` et `netmasks`	"Configuration d'un hôte en mode Fichiers locaux" à la page 107
Configuration d'un serveur de configuration réseau	Activation du démon `in.tftp` et modification des fichiers `hosts`, `ethers` et `bootparams`	"Configuration d'un serveur de configuration réseau" à la page 109

Tâche	Description	Voir
Configuration d'un hôte en mode Client réseau	Création du fichier `hostname`, modification du fichier `hosts` et suppression des fichiers `nodename` et `defaultdomain`, s'ils existent	"Configuration des hôtes en mode Client réseau" à la page 111
Spécification de la stratégie de routage du client réseau	Choix entre un routage statique ou dynamique sur l'hôte	"Activation du routage statique sur un hôte à interface unique" à la page 136 et "Activation du routage dynamique sur un hôte à interface unique" à la page 138
Modification de la configuration réseau existante	Modification du nom d'hôte, de l'adresse IP et des autres paramètres définis lors de l'installation ou ultérieurement.	"Modification de l'adresse IPv4 et des autres paramètres de configuration réseau" à la page 112

Configuration des systèmes sur le réseau local

L'installation logicielle réseau s'effectue en parallèle avec celle du logiciel du système d'exploitation. C'est lors de cette étape que vous devez stocker certains paramètres de configuration IP dans les fichiers adéquats de sorte à ce qu'ils soient lus lors de l'initialisation.

Le processus de configuration réseau implique la création ou la modification des fichiers de configuration réseau. L'accès aux informations de configuration par le noyau du système est soumis à certains facteurs. Le stockage manuel (mode Fichiers locaux) ou l'acquisition sur le serveur de configuration réseau (mode Client réseau) conditionne la disponibilité.

Les paramètres fournis lors de la configuration réseau sont répertoriés ci-dessous.

- Adresse IP de chaque interface réseau sur tous les systèmes.
- Noms d'hôtes de chaque système sur le réseau. Vous pouvez saisir le nom d'hôte dans un fichier local ou une base de données de service de noms.
- Le nom de domaine NIS, LDAP ou DNS dans lequel le système réside, le cas échéant.
- Les adresses de routeur par défaut. Vous devez fournir cette information lorsqu'un routeur unique est connecté à chaque réseau de la topologie. Vous devez également la fournir lorsque les routeurs n'utilisent pas de protocoles de routage tels que RDISC (Router Discovery Server Protocol) ou RIP (Router Information Protocol). Pour plus d'informations sur les routeurs par défaut, reportez-vous à la section "Transfert et routage de paquets sur des réseaux IPv4" à la page 117. Le Tableau 5–1 présente la liste des protocoles de routage pris en charge par Oracle Solaris.
- Le masque de sous-réseau (requis uniquement pour les réseaux avec sous-réseaux).

Lorsque le programme d'installation d'Oracle Solaris détecte plusieurs interfaces sur le système, vous pouvez éventuellement configurer des interfaces supplémentaires lors de l'installation. Pour obtenir l'ensemble des instructions, reportez-vous au *Guide d'installation d'Oracle Solaris 10 9/10 : installations de base*.

Ce chapitre contient des informations sur la création et la modification des fichiers locaux de configuration. Pour plus d'informations sur l'utilisation de bases de données de service de noms, reportez-vous au document *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

▼ Configuration d'un hôte en mode Fichiers locaux

Procédez comme suit pour configurer TCP/IP sur un hôte exécuté en mode Fichiers locaux.

Pour connaître la procédure de configuration manuelle des interfaces dans Solaris 10 11/06 et les versions ultérieures, reportez-vous à la section "Configuration d'une interface physique après l'installation du système" à la page 150.

1 **Connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Allez dans le répertoire `/etc`.**

3 **Vérifiez le nom d'hôte défini dans le fichier `/etc/nodename`.**

Lorsque vous spécifiez le nom d'hôte d'un système lors de l'installation Oracle Solaris, ce dernier est enregistré dans le fichier `/etc/nodename`. Veillez à ce que l'entrée du nom d'hôte corresponde au nom d'hôte correct pour le système.

4 **Vérifiez qu'un fichier `/etc/hostname.`*interface* existe pour chaque interface réseau sur le système.**

Pour connaître la syntaxe et trouver des informations de base sur le fichier `/etc/hostname.`*interface*, reportez-vous à la section "Principes de base de gestion des interfaces physiques" à la page 147.

Lorsque vous exécutez le programme d'installation d'Oracle Solaris, vous devez au moins configurer une interface lors de l'installation. La première interface configurée automatiquement devient l'*interface réseau principale*. Le programme d'installation crée un fichier `/etc/hostname.`*interface* pour l'interface du réseau principal et toute autre interface éventuellement configurée lors de l'installation.

Si vous configurez des interfaces supplémentaires lors de l'installation, assurez-vous que chacune d'elles dispose d'un fichier `/etc/hostname.` *interface*. Vous ne devez pas configurer plusieurs interfaces lors de l'installation d'Oracle Solaris. Toutefois, si vous souhaitez ajouter d'autres interfaces au système plus tard, vous devez les configurer manuellement.

Pour connaître la procédure de configuration manuelle des interfaces dans Solaris 10 11/06 et les versions ultérieures, reportez-vous à la section "Configuration d'une interface physique après l'installation du système" à la page 150.

5 Pour Solaris 10 11/06 et les versions précédentes, assurez-vous que les entrées du fichier `/etc/inet/ipnodes` sont à jour.

Le programme d'installation Oracle Solaris 10 crée le fichier `/etc/inet/ipnodes`. Celui-ci contient le nom de nœud ainsi que l'adresse IPv4 et IPv6 de chaque interface configurée lors de l'installation, le cas échéant.

Utilisez le format d'entrée suivant dans le fichier `/etc/inet/ipnodes` :

IP-address node-name nicknames...

Les *pseudos* correspondent à des noms supplémentaires désignant une interface.

6 Assurez-vous que les entrées du fichier `/etc/inet/hosts` sont à jour.

Le programme d'installation Oracle Solaris crée des entrées pour l'interface réseau principale, l'adresse loopback et toute interface supplémentaire configurée lors de l'installation, le cas échéant.

a. Assurez-vous que les entrées existantes du fichier `/etc/inet/hosts` sont à jour.

b. (Facultatif) Ajoutez les adresses IP et les noms correspondants des interfaces réseau ajoutées à l'hôte local après l'installation.

c. (Facultatif) Ajoutez l'adresse ou les adresses IP du serveur de fichier (pour le montage NFS du système de fichiers `/usr`).

7 Tapez le nom de domaine complet de l'hôte dans le fichier `/etc/defaultdomain`.

Par exemple, si l'hôte `tenere` fait partie du domaine `deserts.worldwide.com`, vous devez taper `deserts.worldwide.com` dans le fichier `/etc/defaultdomain` . Pour plus d'informations, reportez-vous au "Fichier `/etc/defaultdomain`" à la page 239.

8 Tapez le nom du routeur dans le fichier `/etc/defaultrouter`.

Pour plus d'informations sur ce fichier, reportez-vous à la section "Fichier `/etc/defaultrouter`" à la page 239.

9. **Tapez le nom du routeur par défaut et ses adresses IP dans le fichier `/etc/inet/hosts`.**

   La section "Configuration des hôtes en mode Client réseau" à la page 111 contient des options de routage supplémentaires. Vous pouvez appliquer ces options à une configuration en mode Fichiers locaux.

10. **Ajoutez le masque de votre réseau, le cas échéant :**

    - Si l'hôte obtient son adresse IP du serveur DHCP, il n'est pas nécessaire de spécifier le masque de réseau.
    - Si vous avez défini un serveur NIS sur le même réseau que ce client, vous pouvez ajouter les informations du fichier `netmask` dans la base de données appropriée sur le serveur.
    - Dans les autres conditions, effectuez la procédure suivante :

    a. **Tapez le numéro et le masque de réseau dans le fichier `/etc/inet/netmasks` .**

       Utilisez le format suivant :

       ```
       network-number netmask
       ```

       Par exemple, pour le numéro de réseau de Classe C `192.168.83`, vous devez taper :

       ```
       192.168.83.0    255.255.255.0
       ```

       Pour les adresses CIDR, remplacez le préfixe réseau par la représentation décimale avec points équivalente. Les préfixes de réseau et leurs équivalents décimaux à points sont répertoriés dans le Tableau 2–3. Par exemple, pour exprimer le préfixe réseau CIDR `192.168.3.0/22`, tapez ce qui suit :

       ```
       192.168.3.0 255.255.252.0
       ```

    b. **Modifiez l'ordre de recherche des masques de réseau dans `/etc/nsswitch.conf` pour que la recherche porte en premier sur les fichiers locaux.**

       ```
       netmasks:   files nis
       ```

11. **Réinitialisez le système.**

▼ Configuration d'un serveur de configuration réseau

Vous trouverez des informations sur la configuration des serveurs d'installation et des serveurs d'initialisation dans le guide *Guide d'installation d'Oracle Solaris 10 9/10 : installations de base*.

1. **Endossez le rôle de d'administrateur principal ou connectez-vous en tant que superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Modifiez le répertoire root (`/`) du futur serveur de configuration réseau.**

3. **Activez le démon `in.tftpd` en créant le répertoire `/tftpboot` :**

   ```
   # mkdir /tftpboot
   ```

   Cette commande configure le système en tant que serveur RARP, bootparams et TFTP.

4. **Créez un lien symbolique vers le répertoire.**

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

5. **Activez la ligne `tftp` du fichier `/etc/inetd.conf`.**

   Assurez-vous que l'entrée est la suivante :

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

   Cette ligne empêche `in.tftpd` d'extraire un fichier autre que ceux figurant dans `/tftpboot`.

6. **Modifiez la base de données `hosts`.**

   Ajoutez les noms d'hôtes et les adresses IP de chaque client sur le réseau.

7. **Modifiez la base de données `ethers`.**

   Créez des entrées pour chaque hôte du réseau qui s'exécute en mode Client réseau.

8. **Modifiez la base de données `bootparams`.**

   Voir "Base de données `bootparams`" à la page 253. Utilisez une entrée générique ou créez une entrée pour chaque hôte exécuté en mode Client réseau.

9. **Convertissez l'entrée `/etc/inetd.conf` en un fichier manifeste de service SMF (Service Management Facility) et activez le service obtenu :**

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

10. **Assurez-vous que `in.tftpd` fonctionne correctement.**

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

    La sortie que vous devez recevoir ressemble à ce qui suit :

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

Informations supplémentaires

Gestion du démon `in.tftpd`

Le démon `in.tftpd` est géré par SMF (Service Management Facility). La commande `svcadm` permet d'effectuer les opérations de gestion sur `in.tftpd` (par exemple, l'activation, la désactivation ou le redémarrage). L'initiation et la réinitialisation du service s'effectue par l'intermédiaire de la commande `inetd` . Utilisez la commande `inetadm` pour modifier la configuration et afficher les informations de configuration pour `in.tftpd`. La commande `svcs`

permet d'interroger l'état du service. Pour une présentation de l'utilitaire SMF (Service Management Facility), reportez-vous au Chapitre 18, “Gestion des services (présentation) ” du *Guide d'administration système : administration de base*.

Configuration des clients réseau

Les clients réseau reçoivent leurs informations de configuration des serveurs de configuration réseau. Par conséquent, avant de configurer un hôte en tant que client réseau, assurez-vous de configurer au moins un serveur de configuration pour le réseau.

▼ Configuration des hôtes en mode Client réseau

Pour configurer les hôtes en mode Client réseau, suivez la procédure ci-dessous.

1 **Connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Recherchez le fichier `nodename` dans le répertoire `/etc`.**

S'il existe, supprimez-le.

La suppression de `/etc/nodename` oblige le système à utiliser le programme `hostconfig` pour obtenir le nom d'hôte, le nom de domaine et les adresses du routeur auprès du serveur de configuration réseau. Voir “Configuration des systèmes sur le réseau local” à la page 106.

3 **Créez le fichier `/etc/hostname.` *interface*, si ce n'est pas déjà fait.**

Veillez à ce qu'il soit vide. Un fichier `/etc/hostname.`*interface* vide oblige le système à acquérir l'adresse IPv4 auprès du serveur de configuration réseau.

4 **Assurez-vous que le fichier `/etc/inet/hosts` contient uniquement le nom `localhost` et l'adresse IP de l'interface réseau loopback.**

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

L'adresse IP de l'interface loopback IPv4 est `127.0.0.1`.

Pour plus d'informations, reportez-vous à la section “Adresse loopback” à la page 240. Le fichier ne doit pas contenir l'adresse IP ni le nom d'hôte de l'hôte local (interface réseau principale).

5 **Vérifiez qu'il existe un fichier `/etc/defaultdomain`.**

S'il existe, supprimez-le.

Le programme `hostconfig` définit automatiquement le nom de domaine. Pour remplacer le nom de domaine défini par `hostconfig`, saisissez le nom de domaine de substitution dans le fichier `/etc/defaultdomain`.

6 **Assurez-vous que les chemins de recherche dans le fichier `/etc/nsswitch.conf` du client sont conformes aux exigences de service de noms de votre réseau.**

▼ Modification de l'adresse IPv4 et des autres paramètres de configuration réseau

Cette section décrit la procédure de modification de l'adresse IPv4, du nom d'hôte et des autres paramètres réseau d'un système déjà installé. Cette procédure permet de modifier l'adresse IP d'un serveur ou d'un système autonome en réseau. Elle ne s'applique pas aux appareils ou clients réseau. Cette procédure entraîne la création d'une configuration qui sera conservée après les réinitialisations du système.

Remarque – Les instructions s'appliquent explicitement à la modification de l'adresse IPv4 de l'interface réseau principale. Pour ajouter une autre interface au système, reportez-vous à la section "Configuration d'une interface physique après l'installation du système" à la page 150.

Dans la plupart des cas, les étapes suivantes font appel à la numérotation décimale avec points IPv4 classique afin de spécifier l'adresse IPv4 et le masque de sous-réseau. Vous pouvez aussi indiquer l'adresse IPv4 à l'aide de la numérotation CIDR dans tous les fichiers pertinents. La section "Adresses IPv4 au format CIDR" à la page 56 présente la numérotation CIDR.

1 **Connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Pour Solaris 10 11/06 et versions précédentes uniquement, modifiez l'adresse IP dans le fichier `/etc/inet/ipnodes` ou la base de données `ipnodes` équivalente.**

Pour chaque adresse IP que vous ajoutez au système, utilisez la syntaxe suivante :

IP-address host-name, nicknames
IP-address interface-name, nicknames

La première entrée doit contenir l'adresse IP de l'interface réseau principale ainsi que le nom d'hôte du système. Si vous le souhaitez, vous pouvez ajouter des pseudos au nom d'hôte.

Lorsque vous ajoutez des interfaces physiques supplémentaires à un système, créez des entrées dans `/etc/inet/ipnodes` pour les adresses IP et les noms associés de ces interfaces.

3 Si le nom d'hôte du système doit changer, modifiez l'entrée de nom d'hôte dans le fichier `/etc/nodename`.

4 Modifiez l'adresse IP et, le cas échéant, le nom d'hôte dans le fichier `/etc/inet/hosts` ou la base de données équivalente `hosts`.

5 Modifiez l'adresse IP en utilisant la commande `ipadm`.

La commande `ipadm` ne permet pas de modifier une adresse IP directement. Vous devez d'abord supprimer l'objet d'adressage qui représente l'adresse IP que vous souhaitez modifier. Vous pouvez ensuite affecter une nouvelle adresse à l'aide du même nom d'objet d'adressage.

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

6 Modifiez l'adresse IP dans le fichier `/etc/hostname.` *interface* pour l'interface réseau principale.

Utilisez l'un des éléments suivants en tant qu'entrée de l'interface réseau principale dans le fichier `/etc/hostname`*interface* :

- Adresse IPv4 exprimée dans le format décimal avec points classique

  Utilisez la syntaxe suivante :

  IPv4 address subnet mask

  L'entrée de masque de réseau est facultative. Si elle n'est pas spécifiée, le masque de réseau par défaut est utilisé.

  Voici un exemple concret :

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

- Adresse IPv4, exprimée en numérotation CIDR, si elle est appropriée à la configuration réseau

  IPv4 address/network prefix

  Voici un exemple concret :

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

  Le préfixe CIDR désigne le masque de réseau approprié à l'adresse IPv4. Par exemple, le `/8` ci-dessus indique le masque de réseau `255.0.0.0`.

- Nom d'hôte

  Pour utiliser le nom d'hôte du système dans le fichier `/etc/hostname.`*interface*, assurez-vous que le nom d'hôte et l'adresse IPv4 associée figurent également dans la base de données `hosts`.

7 **En cas de changement du masque de sous-réseau, modifiez les entrées de sous-réseau dans les fichiers suivants :**

- `/etc/netmasks`
- (Facultatif) `/etc/hostname.`*interface*

8 **En cas de changement de l'adresse de sous-réseau, remplacez l'adresse IP du routeur par défaut dans `/etc/defaultrouter` par celle du routeur par défaut du nouveau sous-réseau.**

9 **Redémarrez le système.**

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

Exemple 5–1 Modification de l'adresse IPv4 et des autres paramètres réseau pour qu'ils persistent après réinitialisation

Cet exemple illustre la modification des paramètres réseau suivants d'un système déplacé vers un sous-réseau différent :

- L'adresse IP de l'interface réseau principale `eri0` passe de `10.0.0.14` à `192.168.55.14` .
- Le nom d'hôte passe de `myhost` à `mynewhostname`.
- Le masque de réseau passe de `255.0.0.0` à `255.255.255.0`.
- L'adresse de routeur par défaut devient `192.168.55.200` .

Vérifiez l'état actuel du système :

```
# hostname
myhost
# ifconfig -a

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

Ensuite, modifiez l'adresse IP et le nom d'hôte du système `eri0` dans les fichiers concernés :

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

Dans Oracle Solaris 10 11/06 et les versions d'Oracle Solaris 10 antérieures uniquement, effectuez les opérations suivantes :

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

# vi /etc/inet/hosts
#
# Internet host table
```

```
#
127.0.0.1       localhost
192.168.55.14   mynewhostname        loghost
# vi /etc/hostname.eri0
192.168.55.14   netmask  255.255.255.0
```

Enfin, modifiez le masque de réseau et l'adresse IP du routeur par défaut.

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

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

Après avoir apporté ces modifications, réinitialisez le système.

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

Assurez-vous que la configuration que vous venez de définir est conservée après la réinitialisation.

```
# hostname
mynewhostname
# ifconfig -a

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.55.14 netmask ffffff00 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
```

Exemple 5–2 Modification de l'adresse IP et du nom d'hôte pour la session actuelle

Cet exemple illustre la modification du nom d'hôte, de l'adresse IP de l'interface réseau principale et du masque de sous-réseau pour la session actuelle uniquement. Lorsque vous réinitialisez le système, l'adresse IP et le masque de sous-réseau précédents sont rétablis. L'adresse IP de l'interface réseau principale `eri0` passe de `10.0.0.14` à `192.168.34.100` .

```
# ifconfig -a

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

# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
```

```
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.34.100 netmask ffffff00 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
# hostname
mynewhostname
```

Exemple 5–3 Modification de l'adresse IPv4 pour la session actuelle à l'aide de la numérotation CIDR

Cet exemple illustre la modification du nom d'hôte et de l'adresse IP pour la session actuelle à l'aide de la numérotation CIDR. Lorsque vous réinitialisez le système, l'adresse IP et le masque de sous-réseau précédents sont rétablis. L'adresse IP de l'interface réseau principale `eri0` passe de `10.0.0.14` à `192.168.6.25/27`.

```
# ifconfig -a

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

lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
eri0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.06.25 netmask ffffffe0 broadcast 10.255.255.255
        ether 8:0:20:c1:8b:c3
# hostname
mynewhostname
```

Lorsque vous utilisez la numérotation CIDR pour l'adresse IPv4, il n'est pas nécessaire d'indiquer le masque de réseau. `ifconfig` fait appel à la désignation de préfixe de réseau pour identifier le masque de réseau. Par exemple, pour le réseau `192.168.6.0/27`, `ifconfig` définit le masque `ffffffe0`. Si vous avez utilisé la désignation de préfixe `/24` plus courante, le masque de réseau obtenu est `ffffff00`. L'utilisation de la désignation de préfixe `/24` revient à spécifier le masque de réseau `255.255.255.0` dans `ifconfig` lors de la configuration d'une nouvelle adresse IP.

Voir aussi Pour modifier l'adresse IP d'une interface autre que l'interface réseau principale, reportez-vous au *Guide d'administration système : administration de base* (en anglais) et à la section “Configuration d'une interface physique après l'installation du système” à la page 150.

Transfert et routage de paquets sur des réseaux IPv4

Cette section contient les procédures et exemples illustrant la configuration du transfert et du routage des routeurs et des hôtes sur les réseaux IPv4.

Le *transfert de paquet* correspond à la méthode élémentaire de partage des informations d'un système à l'autre sur un réseau. Les paquets sont transférés entre l'interface source et l'interface cible, en principe sur deux systèmes différents. Lorsque vous exécutez une commande ou que vous envoyez un message vers une interface non locale, le système transfère ces paquets sur le réseau local. L'interface avec l'adresse IP cible spécifiée dans les en-têtes de paquet récupère alors les paquets à partir du réseau local. Lorsque l'adresse cible ne figure pas sur le réseau local, les paquets sont alors transférés vers le réseau adjacent suivant, également appelé *saut*. Par défaut, la transmission des paquets est automatiquement configurée lors de l'installation d'Oracle Solaris.

Le *routage* désigne le processus selon lequel les systèmes identifient la destination d'un paquet. Les protocoles de routage d'un système "détectent" les autres systèmes sur le réseau local. Lorsque le système source et le système cible résident sur le même réseau local, le chemin emprunté par les paquets pour se rendre de l'un à l'autre s'appelle une *route directe*. Si les paquets doivent effectuer au moins un saut au-delà du système source, le chemin reliant le système source et le système cible s'appelle une *route indirecte*. Les protocoles de routage prennent connaissance du chemin vers une interface cible et conserve des données sur les routes connues dans la *table de routage* du système.

Les *routeurs* sont des systèmes spécialement configurés et reliés à plusieurs réseaux locaux par l'intermédiaire de plusieurs interfaces physiques. Par conséquent, un routeur peut transférer des paquets au-delà du réseau local domestique, qu'il utilise ou non un protocole de routage. Pour plus d'informations sur le transfert de paquets par les routeurs, reportez-vous à la section “Planification des routeurs du réseau” à la page 66.

Les *protocoles de routage* gèrent les opérations de routage sur un système. L'échange d'informations avec les hôtes leur permet de conserver des routes connues vers les réseaux distants. Les routeurs et les hôtes peuvent exécuter des protocoles de routage. Les protocoles de routage sur l'hôte communiquent avec les démons de routage sur d'autres routeurs et hôtes. Ces protocoles aident l'hôte à identifier la destination des paquets. Lorsque les interfaces réseau sont activées, le système communique automatiquement avec les démons de routage. Ceux-ci contrôlent les routeurs sur le réseau et signalent les adresses des routeurs aux hôtes sur le réseau local. Certains protocoles de routage conservent également des statistiques permettant de mesurer les performances du routage. Contrairement au transfert de paquets, vous devez configurer de manière explicite le routage sur un système Oracle Solaris.

Cette section décrit les procédures de gestion du transfert de paquet et du routage sur les hôtes et routeurs IPv4. Pour plus d'informations sur le routage sur un réseau IPv6, reportez-vous à la section “Configuration d'un routeur IPv6” à la page 179.

Protocoles de routage pris en charge par Oracle Solaris

Les protocoles de routage sont classés en protocoles IGP (Interior Gateway Protocol, protocole de passerelle intérieure), EGP (Exterior Gateway Protocol, protocole de passerelle extérieure) ou une combinaison des deux. Les *protocoles de passerelle intérieure* échangent des informations de routage entre routeurs de réseaux sous contrôle administratif commun. Dans la topologie de réseau de la Figure 5–3, les routeurs exécutent un IGP dans le cadre de l'échange d'informations de routage. Les *protocoles de passerelle extérieure* activent le routeur reliant le réseau Internet local à un réseau extérieur en vue d'échanger des informations avec un routeur sur un réseau externe. Par exemple, le routeur reliant un réseau d'entreprise à un fournisseur de services Internet (ISP, Internet Service Provider) échange les informations de routage avec son homologue ISP via un EGP. L'EGP BGP (Border Gateway Protocol) permet de transporter des informations de routage entre différents IGP et organisations.

Le tableau suivant contient des informations sur les protocoles de routage Oracle Solaris et les emplacements de la documentation correspondant à chaque protocole.

TABLEAU 5–1 Protocoles de routage Oracle Solaris

Protocole	Démon associé	Description	Voir
RIP (Routing Information Protocol)	`in.routed`	IGP acheminant les paquets IPv4 et gérant une table de routage	"Configuration d'un routeur IPv4" à la page 124
Détection de routeur ICMP (Internet Control Message Protocol)	`in.routed`	Permet aux hôtes de détecter la présence d'un routeur sur le réseau	"Activation du routage statique sur un hôte à interface unique" à la page 136 et "Activation du routage dynamique sur un hôte à interface unique" à la page 138
Protocole RIPng (Routing Information Protocol, next generation, protocole d'informations de routage, nouvelle génération)	`in.ripngd`	IGP acheminant les paquets IPv6 et gérant une table de routage	"Procédure de configuration d'un routeur compatible IPv6" à la page 180
Protocole ND (Neighbor Discovery)	`in.ndpd`	Signale la présence d'un routeur IPv6 et détecte les hôtes IPv6 sur un réseau	"Configuration d'une interface IPv6" à la page 173

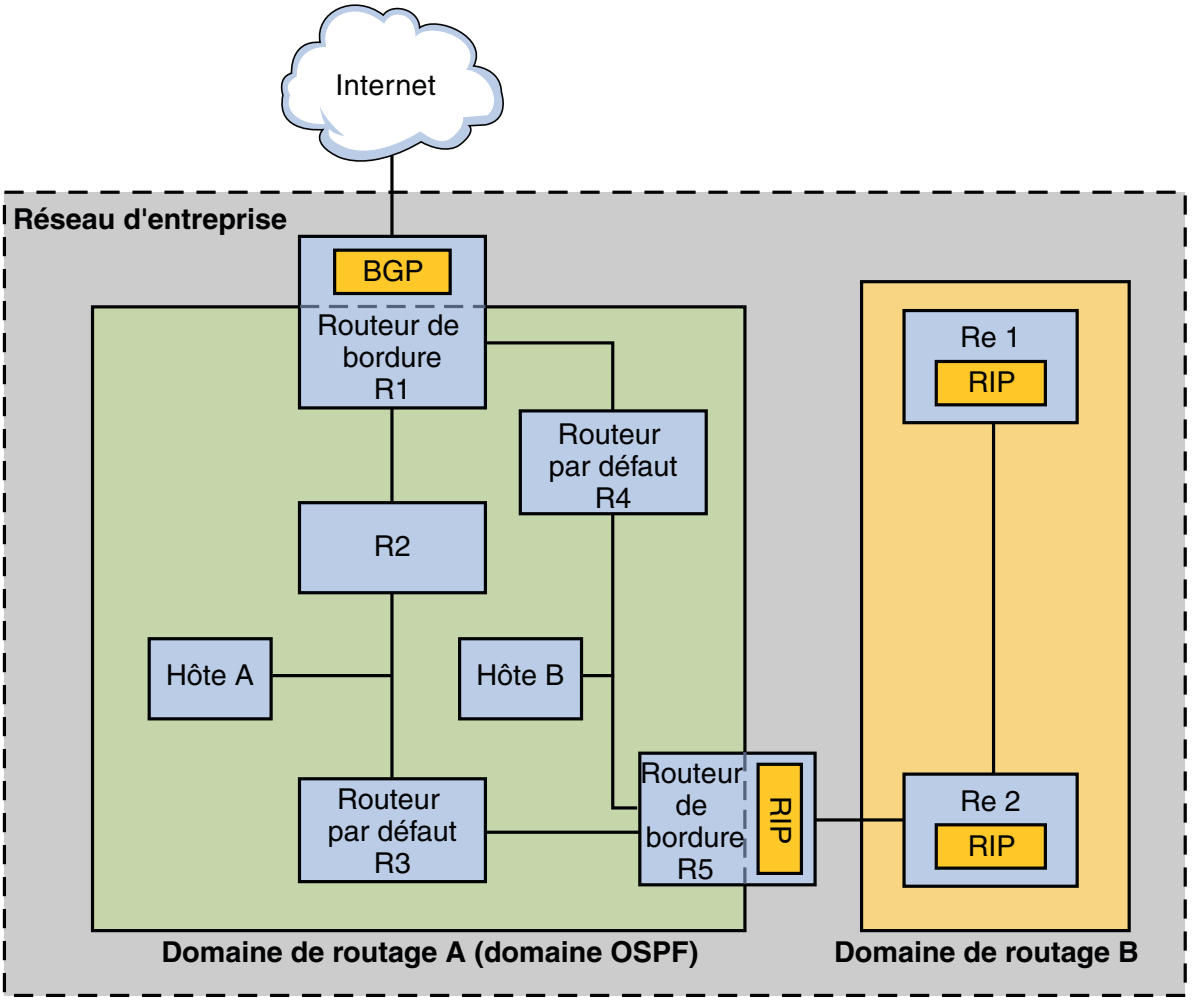
Oracle Solaris prend également en charge la suite de protocole de routage Quagga Open Source. Bien que ne faisant pas partie de la principale distribution Oracle Solaris, ces protocoles sont disponibles à partir du disque de consolidation SFW. Le tableau suivant répertorie les protocoles Quagga.

TABLEAU 5–2 Protocoles Quagga OpenSolaris

Protocole	Démon	Description
Protocole RIP	`ripd`	Protocole IGP à vecteur de distance IPv4 qui achemine les paquets IPv4 et signale sa table de routage aux routeurs adjacents.
RIPng	`ripngd`	Protocole IGP à vecteur de distance IPv6 qui achemine les paquets IPv4 et gère une table de routage.
Protocole OSPF (Open Shortest Path First)	`ospfd`	Protocole IGP d'état des liens IPv4 pour le routage des paquets et la mise en réseau à haute disponibilité.
BGP (Border Gateway Protocol)	`bgpd`	Protocole EGP IPv4 et IPv6 pour le routage d'un domaine administratif à l'autre.

La figure suivante illustre un système autonome ayant recours aux protocoles de routage Quagga.

FIGURE 5–2 Réseau d'entreprise exécutant les protocoles Quagga



La figure illustre un système autonome de réseau d'entreprise divisé en deux domaines de routage, A et B. Le *domaine de routage* A est un interréseau présentant une stratégie de routage cohésive dans un souci de gestion simplifiée ou en raison de l'utilisation d'un protocole de routage unique. Les deux domaines exécutent des protocoles de routage de la suite de protocoles Quagga.

Le domaine de routage A est un domaine OSPF géré sous un ID de domaine OSPF unique. Tous les systèmes à l'intérieur de ce domaine exécutent OSPF en tant qu'IGP. Outre les hôtes et routeurs internes, le domaine A comprend deux routeurs de bordure.

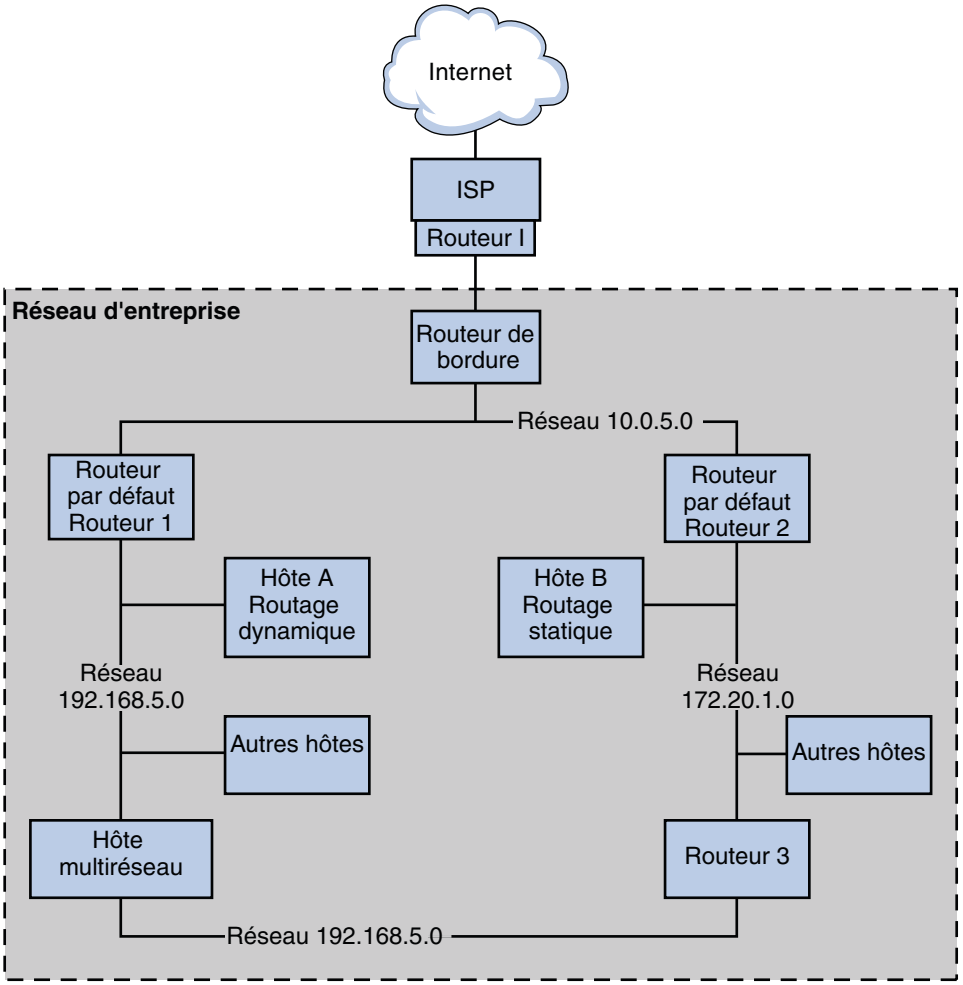
Le routeur de bordure R1 relie le réseau d'entreprise à Internet via un ISP. Pour faciliter les communications entre le réseau d'entreprise et le monde extérieur, R1 exécute BGP sur son interface réseau tournée vers l'extérieur. Le routeur de bordure R5 relie le domaine A au domaine B. Tous les systèmes du domaine B sont gérés avec le protocole de passerelle intérieure RIP. Par conséquent, le routeur de bordure R5 doit exécuter OSPF sur l'interface tournée vers le domaine A et RIP sur l'interface tournée vers le domaine B.

Pour plus d'informations sur les protocoles Quagga, reportez-vous au site Open Solaris Quagga (`http://hub.opensolaris.org/bin/view/Project+quagga/`). Pour connaître les procédures de configuration de ces protocoles, consultez la documentation de quagga (`http://quagga.net/docs/docs-info.php`).

Topologie du système autonome IPv4

Les sites comportant plusieurs routeurs et réseaux gèrent généralement leur topologie réseau comme un domaine de routage unique, également appelé *système autonome AS (Autonomous System)* . La figure suivante illustre une topologie réseau typique, considérée comme un AS de petite taille. Les exemples de cette section font référence à cette topologie.

FIGURE 5–3 Système autonome comportant plusieurs routeurs IPv4



La figure illustre un AS divisé en trois réseaux locaux : `10.0.5.0`, `172.20.1.0` et `192.168.5`. Quatre routeurs se partagent les responsabilités de routage et de transfert des paquets. L'AS inclut les types de systèmes suivants :

- Les *routeurs de bordure* relient un AS à un réseau externe, tel qu'Internet. Les routeurs périphériques réalisent l'interconnexion avec les réseaux externes à l'IGP exécuté sur le AS local. Un routeur de bordure peut exécuter un EGP, BGP (Border Gateway Protocol) par exemple, afin d'échanger des informations avec les routeurs externes, tels que les routeurs de l'ISP. Dans la Figure 5–3, les interfaces du routeur de bordure sont connectées au réseau interne `10.0.5.0` et à un routeur haut débit d'un fournisseur de services.

Pour plus d'informations sur la configuration d'un routeur de bordure et sur BGP (Border Gateway Protocol), consultez la documentation Open Source Quagga (`http://www.quagga.net/docs/docs-info.php#SEC72`).

Si vous envisagez de connecter votre AS à Internet via BGP, vous devez obtenir un ASN (Autonomous System Number, numéro de système autonome) auprès du Registre Internet de votre environnement linguistique. Les registres régionaux, comme l'ARIN (American Registry for Internet Numbers), fournissent des directives pour l'obtention d'un ASN. Par exemple, le document ARIN Number Resource Policy Manual (`http://www.arin.net/policy/nrpm.html#five`) explique comment obtenir un ASN (Autonomous System Number, numéro de système autonome) pour un système autonome aux États-Unis et au Canada. Votre ISP est également en mesure d'obtenir un ASN pour vous.

- Les *routeurs par défaut* gèrent les informations de routage concernant tous les systèmes du réseau local. Généralement, ces routeurs exécutent des IGP, tels que RIP. Dans la Figure 5–3, les interfaces du Routeur 1 sont reliées aux réseaux internes `10.0.5.0` et `192.168.5`. Le routeur 1 sert également de routeur par défaut du réseau `192.168.5`. Le routeur 1 gère les informations de routage pour tous les systèmes du réseau `192.168.5` ainsi que les routes vers d'autres routeurs, tels que le routeur de bordure. Les interfaces du routeur 2 sont reliées aux réseaux internes `10.0.5.0` et `172.20.1`.

  L'Exemple 5–4 illustre la configuration d'un routeur par défaut.

- Les *routeurs de transfert de paquet* transmettent les paquets, mais n'exécutent aucun protocole de routage. Ce type de routeur reçoit les paquets de l'une de ses interfaces connectées à un réseau unique. Ces paquets sont alors transférés via une interface différente du routeur vers un autre réseau local. Sur la Figure 5–3, le routeur de transmission de paquets, Routeur 3, présente des connexions vers les réseaux `172.20.1` et `192.168.5`.
- Les *hôtes multiréseaux* possèdent plusieurs interfaces connectées au même segment de réseau. Par défaut, dans tous les systèmes exécutant Oracle Solaris, un hôte contenant plusieurs réseaux peut transférer des paquets. La Figure 5–3 illustre un hôte multiréseau dont les deux interfaces sont connectées au réseau `192.168.5`. L'Exemple 5–6 décrit la configuration d'un hôte multiréseau.
- Les *hôtes d'interface unique* s'appuient sur les routeurs locaux pour le transfert de paquet et la réception d'informations de configuration critiques. Dans la Figure 5–3, l'hôte A sur le réseau `192.168.5` et l'hôte B sur le réseau `172.20.1` font appel au routage dynamique et au routage statique respectivement. La section "Activation du routage dynamique sur un hôte à interface unique" à la page 138 décrit la configuration d'un hôte exécutant le routage dynamique. La section "Activation du routage statique sur un hôte à interface unique" à la page 136 décrit la configuration d'un hôte exécutant le routage statique.

Configuration d'un routeur IPv4

Cette section décrit la procédure de configuration d'un routeur IPv4 et en donne un exemple. Pour configurer un routeur IPv6, reportez-vous à la section "Procédure de configuration d'un routeur compatible IPv6" à la page 180.

Un routeur représente l'interface entre deux ou plusieurs réseaux. Dès lors, un nom et une adresse IP uniques doivent être assignés à chacune de ses interfaces de réseau physiques. Par conséquent, chaque routeur possède un nom d'hôte et une adresse IP associés à son interface réseau principale ainsi qu'un nom et une adresse IP uniques pour chaque interface réseau supplémentaire.

Vous pouvez également effectuer la procédure suivante pour configurer un système doté d'une seule interface physique (un hôte, par défaut) en tant que routeur. Pour être configuré en tant que routeur, un système d'interface unique doit servir d'extrémité de lien PPP, comme décrit à la section "Planification d'une liaison PPP commutée" du *Guide d'administration système : Services réseau*.

Remarque – Vous pouvez configurer l'ensemble des interfaces d'un routeur lors de l'installation du système Oracle Solaris. Pour obtenir des instructions, reportez-vous au *Guide d'installation d'Oracle Solaris 10 9/10 : installations de base*.

▼ Configuration d'un routeur IPv4

La procédure suivante suppose que vous configurez les interfaces du routeur après l'installation.

Avant de commencer Une fois le routeur physiquement installé sur le réseau, configurez le routeur en mode Fichiers locaux, suivant la procédure décrite à la section "Configuration d'un hôte en mode Fichiers locaux" à la page 107. Cette configuration garantit l'initialisation du routeur en cas de panne du serveur de configuration.

1. **Sur le système à configurer comme routeur, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **À partir de la version Solaris 10 1/06, utilisez la commande `dladm show-link` pour identifier les interfaces physiquement installées sur le routeur.**

   ```
   # dladm show-link
   ```

La sortie suivante de la commande `dladm show-link` indique qu'une carte d'interface réseau `qfe` avec quatre interfaces et deux interfaces `bge` sont disponibles sur le système.

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

3 Vérifiez les interfaces configurées et montées sur le routeur lors de l'installation.

```
# ifconfig -a
```

La sortie suivante de la commande `ifconfig -a` indique que l'interface `qfe0` a été configurée lors de l'installation. Cette interface réside sur le réseau `172.16.0.0`. Les autres interfaces sur de la carte d'interface réseau `qfe`, `qfe1` - `qfe3` et les interfaces `bge` n'ont pas été configurées.

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

4 Configurez et montez une autre interface.

```
# ifconfig interface plumb up
```

Par exemple, pour `qfe1`, vous devez taper :

```
# ifconfig qfe1 plumb up
```

Remarque – Les interfaces explicitement configurées à l'aide de la commande `ifconfig` ne sont pas conservées à la réinitialisation.

---

5 Assignez un masque de réseau et une adresse IPv4 à l'interface.

Attention – Vous pouvez configurer un routeur IPv4 de manière à recevoir son adresse IP via DHCP. Toutefois, cette opération est uniquement conseillée aux administrateurs système DHCP très expérimentés.

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

Par exemple, procédez selon l'une des méthodes suivantes pour assigner l'adresse IP `192.168.84.3` à `qfe1` :

- À l'aide de la numérotation IPv4 classique, tapez les informations suivantes :

  ```
  # ifconfig qfe1 192.168.84.3 netmask + 255.255.255.0
  ```

- À l'aide de la numérotation CIDR, tapez les informations suivantes :

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

Le préfixe `/24` assigne automatiquement le réseau `255.255.255.0` à `qfe1`. Le tableau de la Figure 2–2 répertorie les préfixes CIDR et leurs équivalents décimaux avec points.

6 (Facultatif) Pour garantir la conservation de la configuration d'interface après les réinitialisations, créez un fichier `/etc/hostname.`*interface* pour chaque interface physique supplémentaire.

Vous pouvez par exemple créer les fichiers `/etc/hostname.qfe1` et `/etc/hostname.qfe2` et saisir le nom d'hôte `timbuktu` dans le fichier `/etc/hostname.qfe1` et le nom d'hôte `timbuktu-201` dans le fichier `/etc/hostname.qfe1` . Pour plus d'informations sur la configuration des interfaces uniques, reportez-vous à la section "Configuration d'une interface physique après l'installation du système" à la page 150.

Veillez à réinitialiser la configuration après la création de ce fichier :

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

7 Ajoutez le nom d'hôte et l'adresse IP de chaque interface au fichier `/etc/inet/hosts`.

Exemple :

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

Les interfaces `timbuktu` et `timbuktu-201` résident sur le même système. Notez que l'adresse réseau de `timbuktu-201` est différente de l'interface réseau de `timbuktu`. En effet, le média physique du réseau `192.168.201` est connecté à l'interface réseau `timbuktu-201` tandis que le média du réseau `192.168.200` est connecté à l'interface `timbuktu`.

8 Pour Solaris 10 11/06 et les versions antérieures à Solaris 10 uniquement, ajoutez l'adresse IP et le nom d'hôte de chaque nouvelle interface dans le fichier `/etc/inet/ipnodes` ou la base de données équivalente `ipnodes`.

Exemple :

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

9 Si le routeur est connecté à un réseau de sous-réseaux, ajoutez le numéro du réseau et le masque de réseau dans le fichier `/etc/inet/netmasks`, fichier.

- Pour une adresse IPv4 de numérotation classique, telle que `192.168.83.0` , vous devez taper :

```
192.168.83.0    255.255.255.0
```

- Pour une adresse CIDR, utilisez la version à décimale avec points du préfixe dans l'entrée du fichier `/etc/inet/netmask`. Les préfixes réseau et leurs équivalents décimaux avec points sont répertoriés sur la Figure 2–2. Par exemple, vous devez utiliser l'entrée suivante dans `/etc/netmasks` pour exprimer le préfixe réseau CIDR `192.168.3.0/22` :

  ```
  192.168.3.0 255.255.252.0
  ```

10 Activez le transfert de paquets IPv4 sur le routeur.

Pour cela, exécutez l'une des commandes suivantes :

- Utilisez la commande `routeadm` comme suit :

  ```
  # routeadm -e ipv4-forwarding -u
  ```

- Utilisez la commande SMF (Service Management Facility, utilitaire de gestion de service) suivante :

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

À ce stade, le routeur peut transférer des paquets au-delà du réseau local. Il prend également en charge le *routage statique*, un processus qui permet d'ajouter manuellement des routes à la table de routage. Si vous envisagez de recourir au routage statique, la configuration du routeur est terminée. Toutefois, vous devez gérer les routes dans la table de routage du système. Pour plus d'informations sur l'ajout de routes, reportez-vous à la section "Configuration des routes" à la page 130 et à la page de manuel `route`(1M).

11 (Facultatif) Lancez le protocole de routage.

Le démon de routage `/usr/sbin/in.routed` met automatiquement à jour la table de routage, un processus connu sous le nom de *routage dynamique*. Activez les protocoles de routage IPv4 par défaut de l'une des façons suivantes :

- Utilisez la commande `routeadm` comme suit :

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

- Pour lancer un protocole de routage, tel que RIP, utilisez la commande SMF suivante :

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

  Le FMRI SMF associé au démon `in.routed` est `svc:/network/routing/route`.

Pour plus d'informations sur la commande `routeadm`, reportez-vous à la page de manuel `routeadm`(1M).

Exemple 5–4 Configuration du routeur par défaut d'un réseau

Cet exemple illustre la configuration d'un système existant doté de plusieurs interfaces en routeur par défaut. Le but consiste à faire du Routeur 2 de la Figure 5–3 le routeur par défaut du réseau `172.20.1.0`. Le routeur 2 contient deux connexions réseau câblées, une connexion au

réseau `172.20.1.0` et une connexion au réseau `10.0.5.0`. L'exemple part du principe que le routeur s'exécute en mode Fichiers locaux, comme décrit à la section "Configuration d'un hôte en mode Fichiers locaux" à la page 107.

Prenez le rôle de superutilisateur ou un rôle équivalent, puis déterminez l'état des interfaces du système. À partir de Solaris 10 1/06, vous pouvez utiliser la commande `dladm` comme suit :

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

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

D'après la sortie de la commande `dladm show-link`, trois liens sont disponibles sur le système. Seule l'interface `ce0` a été configurée avec une adresse IP. Pour commencer la configuration du routeur par défaut, vous devez connecter physiquement l'interface `bge0` au réseau `10.0.5.0`. Ensuite, vous devez monter l'interface et la rendre persistante d'une session à l'autre.

```
# ifconfig bge0 plumb up
# ifconfig bge0 10.0.5.10
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 172.20.1.10 netmask ffff0000 broadcast 172.255.255.255
        ether 8:0:20:c1:1b:c6
bge0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.5.10 netmask ff000000 broadcast 10.255.255.255
        ether 8:0:20:e5:95:c4
 # vi /etc/hostname.bge0
10.0.5.10
255.0.0.0
```

Réinitialisez le système à l'aide de la commande de reconfiguration au démarrage :

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

Configurez les bases de données réseau suivantes à l'aide des informations sur l'interface que vous venez de monter et le réseau auquel elle est connectée.

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

Enfin, activez le transfert de paquet, à l'aide de SMF, et le démon de routage `in.routed` .

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

La transmission de paquets IPv4 et le routage dynamique via RIP sont maintenant activés sur le Routeur 2. La configuration du routeur par défaut `172.20.1.0` n'est cependant pas terminée. Procédez comme suit :

- Modifiez les hôtes du réseau `172.10.1.10` pour qu'ils reçoivent leurs informations de routage du nouveau routeur par défaut. Pour plus d'informations, reportez-vous à la section “Activation du routage statique sur un hôte à interface unique” à la page 136.
- Définissez une route statique menant au routeur de bordure dans la table de routage du Routeur 2. Pour plus d'informations, reportez-vous à la section “Tables et types de routage” à la page 129.

Tables et types de routage

Les routeurs et les hôtes gèrent une *table de routage*. Le démon de routage de chaque système actualise la table avec toutes les routes connues. Le noyau du système lit la table de routage avant de transférer des paquets au réseau local. La table de routage dresse la liste des adresses IP des réseaux connus du système, notamment le réseau local par défaut. Elle répertorie également la liste des adresses IP d'un système de passerelle pour chaque réseau connu. Un système de *passerelle* permet de recevoir des paquets sortants et de les envoyer un saut au-delà du réseau local. L'écran suivant représente une table de routage simple d'un système résidant sur un réseau exclusivement IPv4.

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

Dans un système Oracle Solaris, vous pouvez configurer deux types de routage : statique et dynamique. Vous pouvez configurer l'un ou l'autre, ou les deux sur un même système. Dans le cadre de la gestion de sa table de routage, un système dont le routage est *dynamique* s'appuie sur les protocoles de routage, tels que RIP pour les réseaux IPv4 et RIPng pour les réseaux IPv6. Un système où s'applique le *routage statique* uniquement ne fait pas appel à un protocole de routage pour obtenir les informations de routage et mettre à jour sa table de routage. Vous devez gérer les routes connues du système manuellement à l'aide de la commande `route`. Pour plus d'informations, reportez-vous à la page de manuel `route(1M)`.

Lors de la configuration du routage du réseau local ou d'un système autonome, réfléchissez au type de routage à prendre en charge sur des hôtes et des routeurs particuliers.

Le tableau suivant présente les différents types de routage et les scénarios de mise en réseau auquel chaque type de routage convient le mieux.

Type de routage	Utilisation privilégiée
Statique	Réseaux de petite taille, hôtes qui obtiennent leurs routes d'un routeur par défaut et routeurs par défaut qui n'ont besoin de connaître qu'un ou deux routeurs sur les quelques sauts suivants.
Dynamique	Interréseaux volumineux, routeurs sur des réseaux locaux comportant de nombreux hôtes et hôtes sur des systèmes autonomes d'envergure. Le routage dynamique représente le meilleur choix pour les systèmes résidant sur la plupart des réseaux.
Combinaison statique-dynamique	Routeurs effectuant la connexion entre un réseau au routage statique et un réseau au routage dynamique, et routeurs de bordure reliant un système interne autonome aux réseaux externes. La combinaison routage statique et routage dynamique est pratique courante.

Sur la Figure 5–3, l'AS allie le routage statique au routage dynamique.

Configuration des routes

Dans le cadre de la mise en œuvre du routage dynamique d'un réseau IPv4, exécutez la commande `routeadm` ou `svcadm` afin de lancer le démon de routage `in.routed`. La section “Configuration d'un routeur IPv4” à la page 124 décrit la procédure à suivre. Le routage dynamique est la stratégie privilégiée appliquée à la plupart des réseaux et des systèmes autonomes. Toutefois, votre topologie réseau ou un système spécifique sur votre réseau peut exiger un routage statique. Si tel est le cas, vous devez modifier manuellement la table de routage système afin d'y intégrer la route connue vers la passerelle. La procédure suivante décrit l'ajout d'une route statique.

Remarque – Lorsque deux routes présentent la même destination, le système ne procède pas automatiquement à un basculement ou à un équilibrage des charges. Pour bénéficier de ces fonctions, utilisez IPMP, comme l'explique le Chapitre 30, “Présentation d'IPMP”.

▼ Ajout d'une route statique à la table de routage

1 Examinez l'état actuel de la table de routage.

Pour exécuter la forme suivante de la commande `netstat`, utilisez votre compte utilisateur normal :

```
% netstat -rn
```

La sortie doit ressembler à ceci :

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

2 Connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

3 (Facultatif) Supprimez les entrées existantes de la table de routage.

```
# route flush
```

4 Ajoutez une route qui persiste aux réinitialisations du système.

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

`-p`	Crée une route qui doit être conservée après les réinitialisations du système. Si vous souhaitez configurer la route pour la session en cours uniquement, n'utilisez pas l'option `-p`.
`add`	Indique que vous êtes sur le point d'ajouter la route suivante.
`-net` *adresse-réseau*	Indique que la route intègre le réseau avec l'adresse *adresse-réseau*.
`-gateway` *adresse-passerelle*	Indique que le système de passerelle pour la route spécifiée possède l'adresse IP *adresse-passerelle*.

Exemple 5–5 Ajout d'une route statique à la table de routage

L'exemple suivant illustre l'ajout d'une route statique à un système. Le système est Routeur 2, le routeur par défaut du réseau `172.20.1.0` illustré à la Figure 5–3. Dans l'Exemple 5–4, le Routeur 2 est configuré pour un routage dynamique. Pour améliorer son service de routeur par défaut auprès des hôtes du réseau `172.20.1.0`, Router 2 a également besoin d'une route statique vers le routeur de bordure de l'AS, `10.0.5.150` .

Pour afficher la table de routage sur Router 2, effectuez l'opération suivante :

```
# 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
```

D'après la table de routage, Router 2 a connaissance de deux routes. La route par défaut utilise l'interface `172.20.1.10` de Router 2 comme passerelle. La deuxième route, `10.0.5.0`, a été détectée par le démon `in.routed` exécuté sur le Routeur 2. La passerelle de cette route est Routeur 1, avec l'adresse IP `10.0.5.20` .

Pour ajouter une seconde route au réseau `10.0.5.0`, dont la passerelle est le routeur de bordure, procédez comme suit :

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

La table de routage contient désormais une route destinée au routeur de bordure dont l'adresse IP est `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
```

Configuration des hôtes multiréseaux

Dans Oracle Solaris, un système comptant plusieurs interfaces est considéré comme un *hôte multiréseau*. Un hôte multiréseau ne transfère pas de paquets IP. Toutefois, il peut être configuré pour exécuter des protocoles de routage. Les systèmes habituellement configurés en tant qu'hôtes multiréseaux sont les suivants :

- Les serveurs NFS (en particulier ceux qui fonctionnent en tant que vastes centres de données) peuvent être reliés à plusieurs réseaux et permettre ainsi à un grand nombre d'utilisateurs de partager des fichiers. Ils ne doivent pas forcément gérer des tables de routage.
- Tout comme les serveurs NFS, les serveurs de bases de données peuvent posséder plusieurs interfaces réseau en vue de mettre des ressources à la disposition d'un grand nombre d'utilisateurs.
- Les passerelles pare-feu connectent un réseau d'entreprise avec des réseaux publics, tels qu'Internet. Un pare-feu constitue une mesure de sécurité mise en œuvre par les administrateurs. Configuré en tant que pare-feu, l'hôte ne transmet pas de paquets entre les

réseaux qui sont reliés à ses interfaces. Toutefois, l'hôte peut toujours fournir des services TCP/IP standard, tels que `ssh`, aux utilisateurs autorisés.

Remarque – Lorsque les pare-feux sur les interfaces d'un hôte multiréseau sont différents, évitez au maximum toute perturbation accidentelle des paquets de l'hôte. Ce problème se produit particulièrement avec les pare-feux avec état. Une des solutions consiste à configurer des pare-feux sans état. Pour plus d'informations sur les pare-feux, reportez-vous à la section "Firewall Systems" du *System Administration Guide: Security Services* ou à la documentation relative aux pare-feux tiers utilisés sur le réseau.

▼ Création d'un hôte multiréseau

1 Sur le futur hôte multiréseau, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Configurez et montez toutes les interfaces réseau supplémentaires qui n'ont pas été configurées lors de l'installation d'Oracle Solaris.

Reportez-vous à la section "Configuration d'une interface physique après l'installation du système" à la page 150.

3 Assurez-vous que le transfert IP n'est pas activé sur l'hôte multiréseau.

```
# routeadm
```

La commande `routeadm` sans option signale l'état des démons de routage. D'après la sortie de la commande `routeadm` ci-dessous, le transfert IPv4 est activé.

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

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

4 Désactivez le transfert de paquet s'il est activé sur le système.

Exécutez l'une des commandes suivantes :

- Si vous exécutez la commande `routeadm`, tapez ce qui suit :

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

- Si vous utilisez l'utilitaire SMF, tapez ce qui suit :

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

5 (Facultatif) Activez le routage dynamique pour l'hôte multiréseau.

Exécutez l'une des commandes suivantes pour activer le démon `in.routed` :

- Si vous exécutez la commande `routeadm`, tapez ce qui suit :

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

- Si vous utilisez l'utilitaire SMF, tapez ce qui suit :

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

Exemple 5–6 Configuration d'un hôte multiréseau

L'exemple suivant décrit la configuration de l'hôte multiréseau de la Figure 5–3. Dans cet exemple, le nom d'hôte du système est `hostc`. Cet hôte présente deux interfaces connectées au réseau `192.168.5.0` .

Commencez par afficher l'état des interfaces du système.

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

La commande `dladm show-link` signale que `hostc` présente deux interfaces avec un total de cinq liens possibles. Toutefois, seul `hme0` a fait l'objet d'un montage. Pour configurer `hostc` en tant qu'hôte multiréseau, vous devez ajouter le lien `qfe0` ou un autre lien sur la carte d'interface réseau `qfe`. Vous devez d'abord connecter l'interface `qfe0` au réseau `192.168.5.0`. Vous devez ensuite monter l'interface `qfe0` et la rendre persistante après les réinitialisations.

```
# ifconfig qf0 plumb up
# ifconfig qfe0 192.168.5.85
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.5.82 netmask ff0000 broadcast 192.255.255.255
        ether 8:0:20:c1:1b:c6
```

```
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.5.85 netmask ff000000 broadcast 192.255.255.255
        ether 8:0:20:e1:3b:c4
 # vi /etc/hostname.qfe0
192.168.5.85
255.0.0.0
```

Réinitialisez le système à l'aide de la commande de reconfiguration :

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

Ensuite, vous devez ajouter l'interface `qfe0` à la base de données `hosts` :

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

Vous devez alors vérifier l'état du transfert de paquet et du routage sur `host3` :

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

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

La commande `routeadm` signale l'activation du routage dynamique via le démon `in.routed` et du transfert de paquet. Vous devez désactiver le transfert de paquet.

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

Pour désactiver le transfert de paquet, vous pouvez aussi exécuter les commandes `routeadm` comme illustré à la section “Création d'un hôte multiréseau” à la page 133 Une fois le transfert de paquet désactivé, `host3` devient un hôte multiréseau.

Configuration du routage de systèmes à interface unique

Les hôtes à interface unique doivent pouvoir implémenter une forme de routage. S'ils doivent obtenir leurs routes à partir d'un ou de plusieurs routeurs locaux par défaut, configurez-les en vue d'un routage statique. Si ce n'est pas le cas, il est conseillé de recourir au routage dynamique. Les sections suivantes décrivent les procédures d'activation des deux types de routage.

Activation du routage statique sur un hôte à interface unique

Cette procédure active le routage statique sur un hôte à interface unique. Les hôtes utilisant le routage statique n'exécutent aucun protocole de routage dynamique (par exemple, RIP). Pour le routage d'informations, ils utilisent les services d'un routeur par défaut. La figure "Topologie du système autonome IPv4" à la page 121 représente plusieurs routeurs par défaut et leurs hôtes client. Si vous avez fourni le nom d'un routeur par défaut lors de l'installation d'un hôte, ce dernier est configuré de manière à utiliser le routage statique.

Remarque – Vous pouvez également suivre la procédure ci-dessous pour configurer le routage statique sur un hôte multiréseau.

Pour plus d'informations sur le fichier `/etc/defaultrouter`, reportez-vous à la section "Fichier `/etc/defaultrouter`" à la page 239. Pour plus d'informations sur le routage statique et la table de routage, reportez-vous à la section "Tables et types de routage" à la page 129.

1. **Sur l'hôte à interface unique, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Vérifiez la présence du fichier `/etc/defaultrouter` sur l'hôte.**

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

3. **Créez ou modifiez le fichier `/etc/defaultrouter` à l'aide d'un éditeur de texte.**

4. **Ajoutez une entrée pour le routeur par défaut.**

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

   où *IP-routeur* désigne l'adresse IP du routeur par défaut de l'hôte à utiliser.

5. **Assurez-vous que le routage et le transfert de paquets ne sont pas en cours d'exécution sur l'hôte.**

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

```
            IPv6 forwarding   disabled             disabled

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

6 **Ajoutez une entrée pour le routeur par défaut dans le fichier local `/etc/inet/hosts`.**

Pour plus d'informations sur la configuration du fichier `/etc/inet/hosts`, reportez-vous à la section "Modification de l'adresse IPv4 et des autres paramètres de configuration réseau" à la page 112.

Exemple 5–7 Configuration d'un routeur par défaut et du routage statique pour un hôte à interface unique

L'exemple suivant illustre la configuration du routage statique d'`hostb`, hôte à interface unique sur le réseau `172.20.1.0` de la Figure 5–3. L'hôte `hostb` doit utiliser le routeur 2 en tant que routeur par défaut.

Vous devez d'abord vous connecter à `hostb` en tant que superutilisateur ou utilisateur possédant un rôle équivalent. Vérifiez ensuite la présence du fichier `/etc/defaultrouter` sur l'hôte.

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

Si vous n'obtenez aucune réponse de `grep`, vous devez créer le fichier `/etc/defaultrouter`.

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

L'entrée du fichier `/etc/defaultrouter` correspond à l'adresse IP de l'interface sur le routeur 2 reliée au réseau `172.20.1.0`. Vérifiez ensuite si l'hôte autorise actuellement le transfert de paquet et le routage.

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

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

Le transfert de paquet est activé pour cet hôte. Désactivez-le comme suit :

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

Enfin, assurez-vous que le fichier `/etc/inet/hosts` possède une entrée pour le nouveau routeur par défaut.

```
# 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
```

Activation du routage dynamique sur un hôte à interface unique

Le routage dynamique simplifie la gestion du routage sur un hôte. Les hôtes utilisant le routage dynamique exécutent les protocoles de routage fournis par le démon `in.routed` pour IPv4 ou le démon `in.ripngd` pour IPv6. Procédez comme suit pour activer le routage dynamique IPv4 sur un hôte à interface unique. Pour plus d'informations sur le routage dynamique, reportez-vous à la section "Transfert et routage de paquets sur des réseaux IPv4" à la page 117.

1 Sur l'hôte, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Assurez-vous que le fichier `/etc/defaultrouter` existe.

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

3 Si `/etc/defaultrouter` existe, supprimez toutes les entrées qu'il contient.

Un fichier `/etc/defaultrouter` vide oblige l'hôte à utiliser le routage dynamique.

4 Assurez-vous que le transfert de paquets et le routage sont activés sur l'hôte.

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

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

5 Si le transfert de paquet est activé, désactivez-le.

Exécutez l'une des commandes suivantes :

- Si vous exécutez la commande `routeadm`, tapez ce qui suit :

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

- Si vous utilisez l'utilitaire SMF, tapez ce qui suit :

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

6 Activez les protocoles de routage sur l'hôte.

Exécutez l'une des commandes suivantes :

- Si vous exécutez la commande `routeadm`, tapez ce qui suit :

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

- Si vous utilisez l'utilitaire SMF, tapez ce qui suit :

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

Le routage dynamique IPv4 est à présent activé. La table de routage de l'hôte est gérée dynamiquement par le démon `in.routed`.

Exemple 5–8 Exécution du routage dynamique sur un hôte à interface unique

L'exemple suivant illustre la configuration du routage dynamique d'`hosta`, hôte à interface unique sur le réseau `192.168.5.0` de la Figure 5–3. L'hôte `hosta` utilise actuellement le routeur 1 en tant que routeur par défaut. Cependant, `hosta` doit maintenant recourir au routage dynamique.

Vous devez d'abord vous connecter à `hosta` en tant que superutilisateur ou utilisateur possédant un rôle équivalent. Vérifiez ensuite la présence du fichier `/etc/defaultrouter` sur l'hôte.

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

La réponse de `grep` signale l'existence d'un fichier `/etc/defaultrouter` pour `hosta`.

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

Le fichier contient l'entrée `192.168.5.10`, qui est l'adresse IP du Routeur 1. Supprimez cette entrée pour activer le routage statique. Ensuite, vous devez déterminer si le transfert de paquet et le routage sont activés pour l'hôte.

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

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

Le routage et le transfert de paquet sont désactivés pour `hosta` . Pour terminer la configuration du routage dynamique pour `hosta` , activez le routage comme suit :

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

Contrôle et modification des services de couche transport

Les protocoles de couche de transport TCP, SCTP et UDP font partie du package Oracle Solaris standard. Généralement, ces protocoles fonctionnent correctement sans que l'utilisateur ait à intervenir. Toutefois, dans certaines conditions, vous serez peut-être amené à consigner ou modifier des services exécutés via les protocoles de couche transport. Vous devez ensuite modifier les profils de ces services à l'aide de l'utilitaire SMF (Service Management Facility) décrit au Chapitre 18, “Gestion des services (présentation) ” du *Guide d'administration système : administration de base*.

Le démon `inetd` est chargé de lancer les services Internet standard lors de l'initialisation d'un système. Ces services incluent les applications utilisant les protocoles de couche transport TCP, SCTP ou UDP. Vous pouvez modifier les services Internet existants ou ajouter de nouveaux services à l'aide des commandes SMF. Pour plus d'informations sur `inetd`, reportez-vous à la section “Démon de services Internet `inetd`” à la page 248.

Opérations impliquant les protocoles de couche transport :

- Journalisation de toutes les connexions TCP entrantes
- Ajout de services faisant appel à un protocole de couche transport, utilisant SCTP comme exemple
- Configuration des wrappers TCP dans le cadre du contrôle d'accès

Pour plus d'informations sur le démon `inetd`, reportez-vous à la page de manuel `inetd(1M)`.

▼ Journalisation des adresses IP de toutes les connexions TCP entrantes

1 Sur le système local, connectez-vous en tant qu'administrateur réseau ou superutilisateur.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuring RBAC (Task Map)” du *System Administration Guide: Security Services*.

2 Activez le suivi TCP pour tous les services gérés par `inetd`.

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

▼ Ajout de services utilisant le protocole SCTP

Le protocole de transport SCTP fournit des services aux protocoles de couche d'application de façon similaire à TCP. Toutefois, SCTP permet la communication entre deux systèmes multiréseaux ou deux systèmes dont l'un est multiréseau. La connexion SCTP s'appelle une *association*. Dans une association, une application divise les données à transmettre en *plusieurs flux de messages*. Une connexion SCTP peut atteindre les extrémités à l'aide de plusieurs adresses IP, ce qui s'avère particulièrement important dans le cadre d'applications de téléphonie. Les capacités multiréseau de SCTP améliorent la sécurité des sites ayant recours à IP Filter ou IPsec. La page de manuel `sctp(7P)` répertorie les points à prendre en considération au niveau de la sécurité.

Par défaut, le protocole SCTP fait partie d'Oracle Solaris et ne nécessite aucune configuration supplémentaire. Toutefois, vous devrez peut-être configurer explicitement certains services de couche d'application pour utiliser SCTP. `echo` et `discard` sont des exemples d'applications. La procédure suivante illustre l'ajout d'un service d'écho qui utilise un socket de type SCTP bi-univoque.

Remarque – La procédure suivante permet également d'ajouter des services pour les protocoles de couche transport TCP et UDP.

La tâche suivante illustre l'ajout dans le référentiel SMF d'un service `inet` SCTP géré par le démon `inetd`. La tâche décrit ensuite la procédure d'ajout du service à l'aide des commandes SMF (Service Management Facility).

- Pour plus d'informations sur les commandes SMF, reportez-vous aux "Utilitaires d'administration en ligne de commande SMF" du *Guide d'administration système : administration de base*.
- Pour plus d'informations sur la syntaxe, consultez les pages de manuel sur les commandes SMF citées dans la procédure.
- Pour plus d'informations sur SMF, reportez-vous à la page de manuel `smf(5)`.

Avant de commencer Avant d'effectuer la procédure suivante, créez un fichier manifeste pour le service. En exemple, la procédure fait référence à un fichier manifeste du service `echo` intitulé `echo.sctp.xml`.

1 Connectez-vous au système local avec un compte utilisateur disposant de privilèges d'écriture sur les fichiers système.

2 Modifiez le fichier `/etc/services` et ajoutez la définition du nouveau service.

Définissez le service à l'aide de la syntaxe suivante.

service-name |*port/protocol* | *aliases*

3 Ajoutez le nouveau service.

Accédez au répertoire de stockage du manifeste de service et tapez ce qui suit :

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

La page de manuel svccfg(1M) contient la syntaxe complète de `svccfg`.

Admettons que vous voulez ajouter un service `echo` SCTP à l'aide du manifeste `echo.sctp.xml` résidant dans le répertoire `service.dir`. Vous devez taper ce qui suit :

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

4 Assurez-vous que le manifeste de service a été ajouté :

```
# svcs FMRI
```

Pour l'argument *FMRI*, utilisez le FMRI (Fault Managed Resource Identifier, identificateur de ressources gérées erronées) du manifeste de service. Par exemple, pour le service SCTP `echo`, vous devez utiliser la commande suivante :

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

La sortie doit ressembler à ceci :

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

Pour plus d'informations sur la commande `svcs`, reportez-vous à la page de manuel svcs(1).

D'après la sortie, le nouveau manifeste de service est désactivé.

5 Dressez la liste des propriétés du service afin d'identifier les modifications à apporter.

```
# inetadm -l FMRI
```

Pour plus d'informations sur la commande `inetadm`, reportez-vous à la page de manuel inetadm(1M).

Par exemple, pour le service SCTP `echo`, vous devez saisir les informations suivantes :

```
# 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 Activez le nouveau service :

```
# inetadm -e FMRI
```

7 Assurez-vous que le service est activé.

Par exemple, pour le nouveau service echo, vous devez taper :

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

Exemple 5–9 Ajout d'un service utilisant le protocole de transport SCTP

L'exemple suivant indique les commandes à utiliser et les entrées de fichier requises pour que le service d'écho utilise le protocole de couche transport 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
```

▼ Contrôle d'accès aux services TCP à l'aide des wrappers TCP

Le programme `tcpd` met en œuvre les *wrappers TCP*. Les wrappers TCP représentent une mesure de sécurité supplémentaire pour les démons de services, notamment pour `ftpd` . En effet, ils s'interposent entre le démon et les requêtes de service entrantes. Les wrappers TCP consignent les réussites et les échecs des tentatives de connexion. En outre, ils offrent un contrôle d'accès en autorisant ou en refusant la connexion en fonction de l'origine de la requête. Enfin, ils permettent de protéger les démons, notamment SSH, Telnet et FTP. L'application `sendmail` peut également avoir recours aux wrappers TCP (voir la section "Prise en charge des wrappers TCP à partir de la version 8.12 de sendmail" du *Guide d'administration système : Services réseau*.)

1 Sur le système local, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Activez les wrappers TCP.

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

3 Configurez la stratégie de contrôle d'accès des wrappers TCP, telle que décrite à la page de manuel `hosts_access`(3).

Cette page de manuel se trouve sous le répertoire `/usr/sfw/man` du CD-ROM SFW livré avec le CD-ROM Oracle Solaris.

◆ ◆ ◆ CHAPITRE 6

Administration d'interfaces réseau (tâches)

Ce chapitre contient des tâches et des informations relatives aux interfaces réseau :

Nouveautés dans l'administration d'interfaces réseau

Les informations contenues dans ce chapitre décrivent la configuration d'interface à partir de la version Solaris 10 1/06. Vous trouverez une liste complète des nouvelles fonctionnalités d'Oracle Solaris la description des différentes versions de cette application dans le document *Nouveautés apportées à Oracle Solaris 10 8/11*.

Les nouvelles fonctions de Solaris 10 1/06 sont les suivantes :

- La nouvelle commande `dladm` permettant d'afficher le statut de l'interface est présentée à la section "Configuration d'une interface physique après l'installation du système" à la page 150.
- La prise en charge VLAN a été étendue aux interfaces GLDv3, comme expliqué à la section "Administration de réseaux locaux virtuels" à la page 156.
- La prise en charge du groupement de liens est introduite à la section "Présentation des groupements de liens" à la page 162.

Dans Solaris 10 7/07, le fichier `/etc/inet/ipnodes` devient obsolète. Utilisez `/etc/inet/ipnodes` uniquement pour les versions Solaris 10 antérieures, comme expliqué dans chaque procédure.

Administration d'interface (liste des tâches)

Le tableau suivant répertorie les différentes tâches de configuration des interfaces réseau, notamment les configurations spéciales, telles que les configurations de VLAN et de groupements de liens. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Voir
Vérification du statut des interfaces du système	Répertoriez toutes les interfaces du système et vérifiez celles qui sont déjà reliées à un nom de périphérique.	"Affichage du statut d'une interface" à la page 149
Ajout d'une seule interface après l'installation du système	Transformez un système en routeur ou hôte multiréseau en configurant une autre interface.	"Configuration d'une interface physique après l'installation du système" à la page 150
SPARC : vérification de l'unicité de l'adresse MAC d'une interface	Veillez à ce que l'interface soit configurée avec l'adresse MAC par défaut, plutôt qu'avec l'adresse MAC système (SPARC uniquement).	"SPARC : Garantie de l'unicité de l'adresse MAC d'une interface" à la page 154
Planification d'un réseau local virtuel (VLAN)	Réalisez les tâches de planification requises avant la création du VLAN.	"Procédure de planification de la configuration de VLAN" à la page 159
Configuration d'un VLAN	Créez et modifiez les VLAN sur le réseau.	"Procédure de configuration d'un VLAN" à la page 160
Planification des groupements	Concevez le groupement et effectuez les tâches de planification requises avant la configuration de groupements.	"Présentation des groupements de liens" à la page 162
Configuration d'un groupement	Réalisez les diverses tâches en relation avec le groupement de liens.	"Procédure de création d'un groupement de liens" à la page 166
Planification et configuration d'un groupe IPMP	Configurez le basculement et le rétablissement pour les interfaces membres d'un groupe IPMP.	"Procédure de planification pour un groupe IPMP" à la page 779 "Procédure de configuration d'un groupe IPMP avec plusieurs interfaces" à la page 781

Principes de base de gestion des interfaces physiques

Une *interface réseau* connecte un système à un réseau. Un système Oracle Solaris peut contenir deux types d'interfaces : physique et logique. Une *interface physique* comporte un pilote logiciel et un connecteur permettant la connexion du média réseau, tel qu'un câble Ethernet. Pour des raisons de gestion ou de disponibilité, il est possible de regrouper les interfaces physiques. Configurée au sein d'une interface physique, une *interface logique* permet d'ajouter des adresses et de créer des points extrémités de tunnel.

Remarque – Les interfaces réseau logiques sont décrites dans les tâches pour lesquelles elles sont utilisées : tâches IPv6, IPMP, DHCP et autres.

En général, les systèmes informatiques présentent au moins une interface physique *intégrée* par le fabricant sur la carte mère. Certains systèmes peuvent être dotés de plusieurs interfaces intégrées.

Outre les interfaces intégrées, vous pouvez ajouter au système des interfaces acquises séparément. Une interface ayant fait l'objet d'un achat distinct est appelée une *NIC* (Network Interface Card, carte d'interface réseau). Pour installer une NIC, vous devez suivre les instructions du fabricant.

Remarque – Les NIC sont également appelées des *adaptateurs réseau*.

Lors de l'installation du système, le programme d'installation Oracle Solaris détecte les interfaces installées et affiche leur nom. Vous devez configurer au moins une interface de la liste. La première interface configurée lors de l'installation devient l'*interface réseau principale*. L'adresse IP de l'interface réseau principale est associée au nom d'hôte configuré du système, stocké dans le fichier `/etc/nodename`. Toutefois, si vous le souhaitez, vous pouvez configurer des interfaces supplémentaires lors de l'installation ou ultérieurement.

Noms d'interface réseau

Chaque interface physique est identifiée par un nom de périphérique unique. La syntaxe des noms de périphérique est la suivante :

```
<driver-name><instance-number>
```

Les noms de périphérique sur les systèmes Oracle Solaris peuvent comprendre les noms `ce`, `hme`, `bge`, `e1000g` et de nombreux autres noms de périphérique. La variable *numéro_instance* peut présenter une valeur comprise entre zéro et *n*, en fonction du nombre d'interfaces de ce type de pilote installées sur le système.

Par exemple, pour une interface Fast Ethernet 100BASE-TX, fréquemment utilisée en tant qu'interface réseau principale sur les systèmes hôte et serveur, `eri`, `qfe` et `hme` sont des noms de pilote typiques. Si l'interface Fast Ethernet est utilisée tant qu'interface réseau principale, son nom de périphérique est du type `eri0` ou `qfe0`.

Les NIC telles que `eri` et `hme` sont dotées d'une seule interface. Toutefois, de nombreuses marques de NIC présentent plusieurs interfaces. Par exemple, la carte Quad Fast Ethernet (`qfe`) possède quatre interfaces, nommées de `qfe0` à `qfe3` respectivement.

Montage d'une interface

Une interface doit être *montée* avant de transporter le trafic entre le système et le réseau. Le montage consiste à associer une interface à un nom de périphérique. Ensuite, les flux sont configurés de manière à ce que le protocole IP puisse utiliser l'interface. Le montage concerne aussi bien les interfaces physiques que les interfaces logiques. Il intervient dans le cadre de la séquence d'initialisation ou de la syntaxe appropriée de la commande `ifconfig`.

Une interface configurée lors de l'installation est montée automatiquement. Si vous décidez de ne pas configurer les interfaces supplémentaires du système lors de l'installation, celles-ci ne sont pas montées.

Types d'interface Oracle Solaris

À partir de la version Solaris 10 1/06, Oracle Solaris prend en charge les deux types d'interfaces suivants :

- **Interfaces héritées** : il s'agit d'interfaces DLPI et GLDv2. Les interfaces `eri`, `qfe` et `ce` sont toutes trois des interfaces héritées. Lorsque vous vérifiez le statut d'interface à l'aide de la commande `dladm show-link`, ces interfaces sont signalées comme étant "héritées".
- **Interfaces non-VLAN** : il s'agit d'interfaces GLDv3.

Remarque – À présent, GLDv3 est pris en charge sur les types d'interfaces suivants : `bge`, `xge` et `e1000g`.

Gestion d'interfaces réseau individuelles

Une fois l'installation d'Oracle Solaris terminée, vous pouvez être amené à configurer ou à gérer des interfaces pour effectuer les opérations suivantes :

- Mise à niveau du système en hôte multiréseau. Pour plus d'informations, reportez-vous à la section "Configuration des hôtes multiréseaux" à la page 132.

- Conversion d'un hôte en routeur. Pour obtenir les instructions relatives à la configuration de routeurs, reportez-vous à la section “Configuration d'un routeur IPv4” à la page 124.
- Configuration d'interfaces dans le cadre d'un réseau local virtuel. Pour plus d'informations, reportez-vous à la section “Administration de réseaux locaux virtuels” à la page 156.
- Configuration d'interfaces dans le cadre d'un groupement. Pour plus d'informations, reportez-vous à la section “Présentation des groupements de liens” à la page 162.
- Ajout d'une interface à un groupe IPMP. Pour obtenir les instructions relatives à la configuration d'un groupe IPMP, reportez-vous à la section “Configuration de groupes IPMP” à la page 779

Cette section contient des informations relatives à la configuration d'une interface réseau, à partir de la version Solaris 10 1/06. Reportez-vous aux sections suivantes pour plus d'informations sur la configuration d'interfaces au sein d'un groupe :

- Pour configurer une interface dans le cadre d'un réseau local virtuel, reportez-vous à la section “Administration de réseaux locaux virtuels” à la page 156.
- Pour configurer une interface dans le cadre d'un groupement, reportez-vous à la section “Présentation des groupements de liens” à la page 162.
- Pour configurer une interface dans le cadre d'un groupe IPMP, reportez-vous à la section “Configuration de groupes IPMP” à la page 779.

▼ Affichage du statut d'une interface

À partir de la version Solaris 10 1/06, cette procédure permet d'identifier les interfaces disponibles sur un système et d'afficher leur statut. Elle indique également les interfaces actuellement montées. Si vous exécutez une version antérieure à Solaris 10 3/05, reportez-vous à la section “Méthode d'obtention d'informations sur une interface spécifique” à la page 209.

1 Sur le système sur lequel vous devez configurer les interfaces, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Identifiez les interfaces installées sur le système.

```
# dladm show-link
```

Lors de cette étape, vous exécutez la commande `dladm` décrite à la page de manuel `dladm`(1M). Cette commande signale tous les pilotes d'interface qu'elle détecte, que les interfaces soient configurées ou non.

3 Identifiez les interfaces du système actuellement montées.

```
# ifconfig -a
```

La commande `ifconfig` compte de nombreuses fonctions, dont le montage d'interface. Pour plus d'informations, reportez-vous à la page de manuel `ifconfig(1M)`.

Exemple 6–1 Affichage du statut d'une interface à l'aide de la commande `dladm`

L'exemple suivant illustre l'affichage du statut à l'aide de la commande `dladm`.

```
# dladm show-link
ce0             type: legacy    mtu: 1500       device: ce0
ce1             type: legacy    mtu: 1500       device: ce1
bge0            type: non-vlan  mtu: 1500       device: bge0
bge1            type: non-vlan  mtu: 1500       device: bge1
bge2            type: non-vlan  mtu: 1500       device: bge2
```

D'après la sortie de la commande `dladm show-link`, quatre pilotes d'interface sont disponibles pour l'hôte local. Les interfaces `ce` et `bge` peuvent être configurées pour des réseaux locaux virtuels (VLAN). Toutefois, seules les interfaces GLDV3 de type `non-VLAN` peuvent être utilisées pour des groupements de liens.

L'exemple suivant illustre l'affichage du statut à l'aide de la commande `ifconfig - a`.

```
# ifconfig -a
 lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu
8232 index 1
         inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 3
         inet 192.168.84.253 netmask ffffff00 broadcast 192.168.84.255
        ether 0:3:ba:7:84:5e
bge0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,DHCP,IPv4>mtu 1500 index 2
         inet 10.8.57.39 netmask ffffff00 broadcast 10.8.57.255
        ether 0:3:ba:29:fc:cc
```

La sortie de la commande `ifconfig -a` affiche les statistiques des interfaces `ce0` et `bge0` uniquement. Seules les interfaces `ce0` et `bge0` ont été montées et sont en mesure de recevoir le trafic réseau. Elles peuvent être utilisées dans le cadre d'un VLAN. Le montage de `bge0` empêche son utilisation dans le cadre d'un groupement.

▼ Configuration d'une interface physique après l'installation du système

Avant de commencer

- Sélectionnez les adresses IPv4 à utiliser pour les interfaces supplémentaires.
- Assurez-vous de l'installation sur le système de l'interface physique à configurer. Pour plus d'informations sur l'installation de NIC achetées séparément, consultez les instructions correspondantes fournies par le fabricant.

- Si vous venez d'installer l'interface, exécutez une reconfiguration au démarrage avant de passer à l'étape suivante.

1 Sur le système sur lequel vous devez configurer les interfaces, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Identifiez les interfaces installées sur le système.

```
# dladm show-link
```

3 Configurez et montez chaque interface.

```
# ifconfig interface plumb up
```

Par exemple, pour `qfe0`, vous devez taper :

```
# ifconfig qfe0 plumb up
```

Remarque – Les interfaces explicitement configurées à l'aide de la commande `ifconfig` ne sont pas conservées à la réinitialisation.

4 Assignez un masque de réseau et une adresse IPv4 à l'interface.

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

Par exemple, pour `qfe0`, vous devez taper :

```
# ifconfig
qfe0 192.168.84.3 netmask + 255.255.255.0
```

Remarque – Vous pouvez indiquer une adresse IPv4 en notation IPv4 standard ou CIDR.

5 Assurez-vous que les interfaces nouvellement configurées sont montées et configurées ou affichent l'indicateur d'état « `UP` ».

```
# ifconfig
-a
```

Vérifiez la ligne d'état de chaque interface affichée. Veillez à ce que la sortie contienne l'indicateur `UP` sur la ligne d'état, par exemple :

```
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 2
```

6 (Facultatif) Pour conserver la configuration des interfaces après les réinitialisations, suivez les instructions ci-dessous :

a. Créez un fichier `/etc/hostname.`*interface* pour chaque interface à configurer.

Par exemple, pour ajouter l'interface `qfe0`, vous devez créer le fichier suivant :

```
# vi /etc/hostname.qfe0
```

Remarque – Si vous créez d'autres fichiers de nom d'hôte pour la même interface, ces fichiers doivent également suivre le format de nom `hostname.[0-9]*`, par exemple : `hostname.qfe0.a123`. Des noms tels que `hostname.qfe0.bak` ou `hostname.qfe0.old` ne sont pas valides et seront ignorés par les scripts pendant l'initialisation du système.

Une interface ne doit contenir qu'un seul fichier de nom d'hôte correspondant. Si vous créez un autre fichier de nom d'hôte pour une interface avec un nom de fichier valide, tels que `/etc/hostname.qfe` et `/etc/hostname.qfe.a123` , les scripts d'initialisation tenteront de configurer les données en référençant le contenu des deux fichiers de nom d'hôte et cela peut générer des erreurs. Pour éviter ce genre d'erreurs, indiquez un nom de fichier non valide pour le fichier de nom d'hôte à ne pas utiliser dans la configuration.

---

b. Modifiez le fichier `/etc/hostname.`*interface*.

Ajoutez l'adresse IPv4 de l'interface dans le fichier. Vous pouvez pour cela utiliser la notation IPv4 standard ou la notation CIDR. Vous pouvez également ajouter au fichier un masque de réseau et des informations de configuration supplémentaires.

Remarque – Pour ajouter une adresse IPv6 à une interface, reportez-vous à la section "Modification de la configuration d'interface IPv6 pour les hôtes et les serveurs" à la page 184

---

c. Pour les versions Solaris 10 11/06 et les versions précédentes d'Oracle Solaris 10, ajoutez les entrées des nouvelles interfaces dans le fichier `/etc/inet/ipnodes`.

d. Ajoutez les entrées des nouvelles interfaces dans le fichier `/etc/inet/hosts` .

e. Effectuez une reconfiguration au démarrage.

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

f. Assurez-vous que l'interface créée dans le fichier `/etc/hostname.` *interface* a été configurée.

```
# ifconfig -a
```

Reportez-vous à l'Exemple 6–2.

Exemple 6–2 Ajout de configurations d'interface persistantes

L'exemple illustre la configuration des interfaces `qfe0` et `qfe1` sur un hôte. Ces interfaces sont persistantes en cas de réinitialisation.

```
# dladm show-link
eri0    type: legacy    mtu: 1500       device: eri0
qfe0    type: legacy    mtu: 1500       device: qfe0
qfe1    type: legacy    mtu: 1500       device: qfe1
qfe2    type: legacy    mtu: 1500       device: qfe2
qfe3    type: legacy    mtu: 1500       device: qfe3
bge0    type: non-vlan  mtu: 1500       device: bge0
# vi /etc/hostname.qfe0
192.168.84.3 netmask 255.255.255.0
# vi /etc/hostname.qfe1
192.168.84.72 netmask 255.255.255.0
# vi /etc/inet/hosts
# Internet host table
#
127.0.0.1       localhost
10.0.0.14       myhost
192.168.84.3       interface-2
192.168.84.72       interface-3
For Solaris 10 11/06 and earlier releases:# vi /etc/inet/ipnodes
10.0.0.14 myhost
192.168.84.3       interface-2
192.168.84.72       interface-3
```

À ce stade, vous devez réinitialiser le système.

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

Une fois le système réinitialisé, vous devez vérifier la configuration des interfaces.

```
ifconfig -a
# ifconfig -a lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu
8232 index 1
         inet 127.0.0.1 netmask ff000000
eri0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         inet 10.0.0.14netmask ff000000 broadcast 10.255.255.255
         ether 8:0:20:c1:8b:c3
qfe0:flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
      inet 192.168.84.3 netmask ffffff00 broadcast 192.255.255.255
      ether 8:0:20:c8:f4:1d
qfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 4
         inet 192.168.84.72 netmask ffffff00 broadcast 10.255.255.255
        ether 8:0:20:c8:f4:1e
```

Voir aussi

- Pour configurer une adresse IPv6 sur une interface, reportez-vous à la section "Activation d'une interface IPv6 pour la session actuelle" à la page 174.
- Pour configurer la détection de basculement et le rétablissement à l'aide d'IPMP (IP Network Multipathing, multiacheminement sur réseau IP), reportez-vous au Chapitre 31, "Administration d'IPMP (tâches)".

▼ Suppression d'une interface physique

1 **Sur le système sur lequel vous devez supprimer l'interface, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Supprimez l'interface physique.**

```
# ifconfig interface down unplumb
```

Par exemple, pour supprimer l'interface `qfe1`, tapez :

```
# ifconfig qfe1 down unplumb
```

▼ SPARC : Garantie de l'unicité de l'adresse MAC d'une interface

Pour configurer les adresses MAC, procédez comme suit.

Certaines applications exigent que les adresses MAC de toutes les interfaces d'un hôte soient uniques. Toutefois, les systèmes SPARC possèdent une adresse MAC à l'échelle du système appliquée à toutes les interfaces par défaut. Vous devez configurer les adresses MAC d'origine des interfaces d'un système SPARC dans les deux contextes suivants :

- Dans le cadre d'un regroupement de liens, vous devez utiliser les adresses MAC d'origine des interfaces de la configuration de regroupement.
- Dans le cadre des groupes IPMP, chaque interface doit posséder une adresse MAC unique. Ces interfaces doivent utiliser les adresses MAC d'origine.

Le paramètre EEPROM `local-mac-address?` détermine si les interfaces du système SPARC utilisent l'adresse MAC du système ou leur adresse MAC unique. La procédure suivante indique comment vérifier la valeur actuelle du paramètre `local-mac-address?` à l'aide de la commande `eeprom` et la modifier, au besoin.

1 **Sur le système sur lequel vous devez configurer les interfaces, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Déterminez si toutes les interfaces du système utilisent l'adresse MAC système.

```
# eeprom local-mac-address?
local-mac-address?=false
```

Dans cet exemple, la réponse à la commande `eeprom`, `local-mac-address?=false`, indique que toutes les interfaces utilisent l'adresse MAC du système. Pour que les interfaces puissent devenir membres d'un groupe IPMP, vous devez remplacer `local-mac-address?=false` par `local-mac-address?=true`. Vous devez également remplacer `local-mac-address?=false` par `local-mac-address?=true` pour les regroupements.

3 Si nécessaire, modifiez la valeur de `local-mac-address?` comme suit :

```
# eeprom local-mac-address?=true
```

À la réinitialisation du système, les interfaces avec adresses MAC d'origine utilisent celles-ci plutôt que l'adresse MAC du système. Les interfaces sans adresses MAC d'origine continuent d'utiliser les adresses MAC d'origine.

4 Vérifiez l'adresse MAC de toutes les interfaces du système.

Recherchez des cas dans lesquels plusieurs interfaces possèdent la même adresses MAC. Dans cet exemple, toutes les interfaces utilisent l'adresse MAC système `8:0:20:0:0:1`.

```
ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
      inet 127.0.0.1 netmask ff000000
hme0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 10.0.0.112 netmask ffffff80 broadcast 10.0.0.127
      ether 8:0:20:0:0:1
ce0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 10.0.0.114 netmask ffffff80 broadcast 10.0.0.127
      ether 8:0:20:0:0:1
ce1: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 10.0.0.118 netmask ffffff80 broadcast 10.0.0.127
      ether 8:0:20:0:0:1
```

Remarque – Passez à l'étape suivante uniquement si plusieurs interfaces réseau possèdent une même adresse MAC. Sinon, passez à la dernière étape.

---

5 Au besoin, configurez manuellement les interfaces restantes de sorte que chaque interface possède une adresse MAC unique.

Indiquez une adresse MAC unique dans le fichier `/etc/hostname.`*interface* pour l'interface en question.

Dans l'exemple de l'étape précédente, vous devez configurer les interfaces `ce0` et `ce1` avec des adresses MAC gérées localement. Par exemple, pour reconfigurer l'interface `ce1` avec l'adresse MAC gérée localement `06:05:04:03:02`, vous devez ajouter au fichier `/etc/hostname.ce1` la ligne suivante :

```
ether 06:05:04:03:02
```

Remarque – Pour éviter tout risque de conflit entre des adresses MAC configurées manuellement avec d'autres adresses MAC de votre réseau, configurez toujours les adresses MAC *administrées localement* tel que défini par la norme IEEE 802.3.

La commande `ifconfig ether` permet également de configurer l'adresse MAC d'une interface pour la session actuelle. Cependant, les modifications effectuées directement avec la commande `ifconfig` ne sont pas conservées après la réinitialisation. Consultez la page de manuel `ifconfig(1M)` pour obtenir des informations supplémentaires.

6 **Redémarrez le système.**

Administration de réseaux locaux virtuels

Un *réseau local virtuel (Virtual Local Network, VLAN)* est une sous-division d'un réseau local située sur la couche de liaison de données de la pile du protocole TCP/IP. Vous pouvez créer des VLAN pour tout réseau local utilisant la technologie de commutation. L'assignation de groupes d'utilisateurs à des VLAN permet d'améliorer l'administration et la sécurité du réseau local entier. Vous pouvez également assigner les interfaces d'un même système à des VLAN différents.

La création de VLAN est utile dans les cas suivants :

- Création de divisions logiques de groupes de travail

  Supposons par exemple que tous les hôtes d'un étage d'un immeuble sont connectés à un réseau local commuté. Vous pouvez dans ce cas créer un VLAN distinct pour chaque groupe de travail de cet étage.
- Application de stratégies de sécurité différentes selon les groupes de travail

  Par exemple, les besoins en matière de sécurité varient considérablement entre un service financier et un service informatique. Si les systèmes de ces deux services partagent le même réseau local, vous pouvez alors créer un VLAN distinct pour chaque service et appliquer la stratégie de sécurité qui convient à chaque VLAN.
- Division de groupes de travail en domaines de diffusion gérables

  Les VLAN réduisent la taille des domaines de diffusion et améliorent ainsi l'efficacité du réseau.

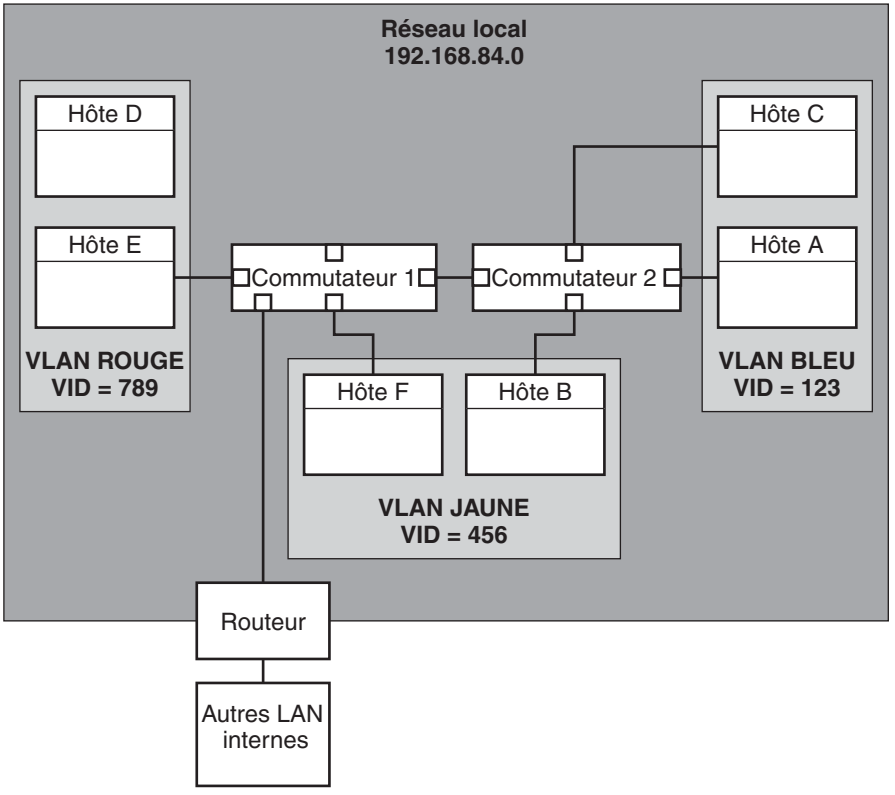
Présentation de la topologie du VLAN

La technologie de commutation du réseau local permet d'organiser les systèmes d'un réseau local en plusieurs VLAN. Pour diviser un réseau local en VLAN, vous devez obtenir des commutateurs qui prennent en charge la technologie de réseau local virtuel. Vous pouvez

configurer tous les ports d'un commutateur de manière à ce qu'ils servent un VLAN unique ou plusieurs VLAN (selon la topologie du réseau). La configuration des ports d'un commutateur varie en fonction du fabricant de ce dernier.

La figure suivante illustre un réseau local dont l'adresse de sous-réseau est `192.168.84.0`. Ce réseau local est divisé en trois VLAN (rouge, jaune et bleu).

FIGURE 6–1 Réseau local avec trois VLAN



La connectivité sur le LAN `192.168.84.0` est gérée par les commutateurs 1 et 2. Le VLAN rouge contient des systèmes dans le groupe de travail de la comptabilité. ceux des ressources humaines au VLAN jaune. Les systèmes du groupe de travail des technologies de l'information sont assignés au VLAN bleu.

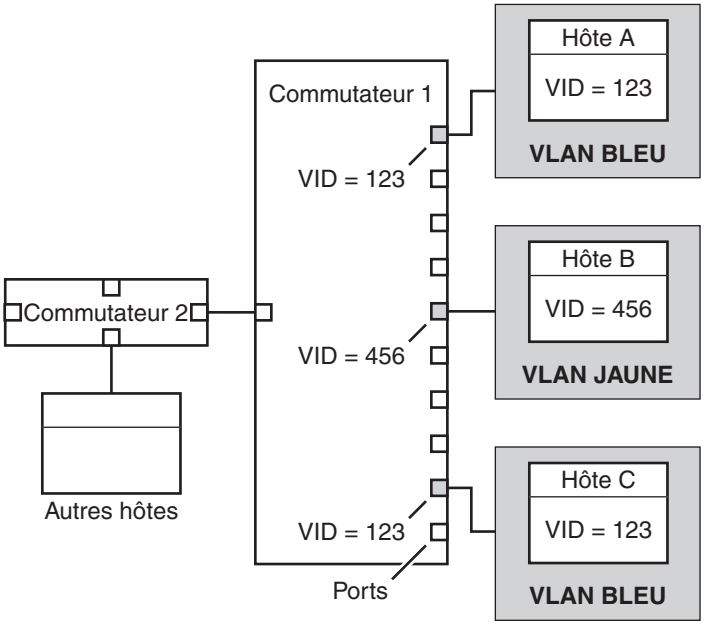
Points de connexions physiques et repères des VLAN

Chaque VLAN inclus dans un réseau local est identifié par un repère de VLAN, ou *ID de VLAN (VID)*. Le VID est assigné pendant la configuration du VLAN. Il s'agit d'un identificateur à

12 bits, compris entre 1 et 4094, qui fournit une identité unique à chaque VLAN. Sur la Figure 6–1, les VLAN possèdent les VID suivants : 123 (bleu), 456 (jaune) et 789 (rouge).

Pour que les commutateurs prennent en charge ces VLAN, vous devez leur assigner un VID à chaque port lors de la configuration. Le VID du port doit être identique à celui assigné à l'interface de connexion du port (voir figure suivante).

FIGURE 6–2 Configuration des commutateurs pour un réseau avec des VLAN



La Figure 6–2 présente plusieurs hôtes qui sont connectés à des VLAN. Deux hôtes appartiennent au même VLAN. Sur cette figure, les interfaces réseau principales des trois hôtes se connectent au commutateur 1. L'hôte A est membre du VLAN bleu. L'interface de l'hôte A est de ce fait configurée à l'aide du VID 123. Cette interface se connecte au port 1 du commutateur 1, qui est ensuite configuré à l'aide du VID 123. L'hôte B est membre du VLAN jaune dont le VID est 456. L'interface de l'hôte B se connecte au port 5 du commutateur 1, qui est configuré à l'aide du VID 456. Enfin, l'interface de l'hôte C se connecte au port 9 du commutateur 1. Le VLAN bleu est configuré à l'aide du VID 123.

Cette figure montre également qu'un seul hôte peut appartenir à plusieurs VLAN. Par exemple, l'hôte A comporte deux VLAN configurés sur l'interface. Le deuxième VLAN est configuré avec le numéro VID 456 et est connecté au port 3 qui est également configuré avec le numéro VID 456. Par conséquent, l'hôte A est membre des VLAN bleu et jaune.

Lors de la configuration d'un VLAN, vous devez spécifier le *point de connexion physique* du VLAN. La valeur du point de connexion physique s'obtient par la formule suivante :

driver-name `+ VID * 1000 +` *device-instance*

Remarque : le numéro de *instance périphérique* doit être inférieur à 1 000.

Exemple : la formule suivante permet de créer le point de connexion physique d'une interface `ce1` configurée sur le VLAN 456 :

```
ce + 456 * 1000 + 1= ce456001
```

Planification de plusieurs VLAN sur un réseau

Pour planifier la configuration des VLAN de votre réseau, suivez la procédure ci-dessous :

▼ Procédure de planification de la configuration de VLAN

1 **Observez la topologie du réseau local et déterminez les emplacements appropriés pour créer des VLAN.**

La Figure 6–1 illustre un exemple simple de topologie de réseau.

2 **Créez un schéma de numérotation pour les VID et assignez un VID à chaque VLAN.**

Remarque – Votre réseau dispose peut-être déjà d'un tel schéma de numérotation. Dans ce cas, créez des VID compris dans le schéma de numérotation existant.

---

3 **Sur chaque système, déterminez quelles interfaces seront membres de quel VLAN.**

a. **Déterminez les interfaces configurées sur un système.**

```
# dladm show-link
```

b. **Déterminez les VID associés aux liaisons de données du système.**

c. **Créez des points de connexion physiques pour chaque interface devant être configurée avec un VLAN.**

Vous pouvez configurer les interfaces d'un même système sur des VLAN différents.

4 **Vérifiez les connexions des interfaces sur les commutateurs du réseau.**

Notez le VID de chaque interface ainsi que le port du commutateur auquel elle est connectée.

5 **Configurez chaque port du commutateur avec le même VID que celui de l'interface à laquelle il est connecté.**

Reportez-vous aux instructions fournies par le fabricant du commutateur pour de plus amples informations sur la configuration.

Configuration des VLAN

Oracle Solaris prend désormais en charge les VLAN sur les types d'interface suivants :

- `ce`
- `bge`
- `xge`
- `e1000g`

Sur les interfaces héritées, seule l'interface `ce` peut devenir membre d'un VLAN. Vous pouvez configurer des interfaces de types différents sur le même VLAN.

Remarque – Vous pouvez configurer plusieurs VLAN dans un groupe IPMP. Pour plus d'informations sur les groupes IPMP, reportez-vous à la section "Configurations d'interfaces IPMP" à la page 767.

▼ Procédure de configuration d'un VLAN

1 **Connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Déterminez les types d'interface utilisés sur votre système.**

```
# dladm show-link
```

La sortie suivante énumère les types d'interface disponibles :

```
ce0             type: legacy    mtu: 1500       device: ce0
 ce1             type: legacy    mtu: 1500       device: ce1
 bge0            type: non-vlan  mtu: 1500       device: bge0
 bge1            type: non-vlan  mtu: 1500       device: bge1
 bge2            type: non-vlan  mtu: 1500       device: bge2
```

3 **Configurez une interface en tant que membre d'un VLAN.**

```
# ifconfig interface-PPA plumb IP-address up
```

Exemple : la commande suivante permet de configurer l'interface `ce1` avec l'adresse IP `10.0.0.2` sur un VLAN portant le VID 123 :

```
# ifconfig ce123001 plumb 10.0.0.2
up
```

Remarque – Vous pouvez assigner des adresses IPv4 et IPv6 à des VLAN tout comme pour les autres interfaces.

4 (Facultatif) Pour conserver les paramètres du VLAN à chaque réinitialisation, créez un fichier nommé `nom d'hôte.`*point de connexion physique* pour chaque interface membre du VLAN.

`# cat hostname.`*interface-PPA*
IPv4-address

5 Sur le commutateur, définissez les repères des VLAN ainsi que leurs ports afin qu'ils correspondent avec les VLAN configurés sur le système.

Exemple 6–3 Configuration d'un VLAN

L'exemple suivant illustre la commande de configuration des périphériques `bge1` et `bge2` sur un VLAN portant le VID 123.

```
# dladm show-link
ce0             type: legacy    mtu: 1500       device: ce0
ce1             type: legacy    mtu: 1500       device: ce1
bge0            type: non-vlan  mtu: 1500       device: bge0
bge1            type: non-vlan  mtu: 1500       device: bge1
bge2            type: non-vlan  mtu: 1500       device: bge2
# ifconfig bge123001 plumb 10.0.0.1 up
# ifconfig bge123002 plumb 10.0.0.2 up
# cat hostname.bge123001   10.0.0.1
# cat hostname.bge123002   10.0.0.2
# ifconfig -a
 lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
         inet 127.0.0.1 netmask ff000000
 bge123001: flags=201000803<UP,BROADCAST,MULTICAST,IPv4,CoS> mtu 1500 index 2
         inet 10.0.0.1 netmask ff000000 broadcast 10.255.255.255
         ether 0:3:ba:7:84:5e
bge123002:flags=201000803 <UP,BROADCAST,MULTICAST,IPv4,CoS> mtu 1500 index 3
         inet 10.0.0.2 netmask ff000000 broadcast 10.255.255.255
         ether 0:3:ba:7:84:5e
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 4
         inet 192.168.84.253 netmask ffffff00 broadcast 192.168.84.255
         ether 0:3:ba:7:84:5e
# dladm show-link
ce0             type: legacy    mtu: 1500       device: ce0
ce1             type: legacy    mtu: 1500       device: ce1
bge0            type: non-vlan  mtu: 1500       device: bge0
bge1            type: non-vlan  mtu: 1500       device: bge1
bge2            type: non-vlan  mtu: 1500       device: bge2
bge123001       type: vlan 123  mtu: 1500       device: bge1
bge123002       type: vlan 123  mtu: 1500       device: bge2
```

Présentation des groupements de liens

Remarque – Dans la version d'origine d'Oracle Solaris 10 et les versions précédentes, les groupements de liens n'étaient pas pris en charge. Pour créer des groupements de liens dans une version précédente d'Oracle Solaris, vous pouvez utiliser la fonction Sun Trunking (reportez-vous au *Sun Trunking 1.3 Installation and Users Guide*).

Oracle Solaris permet d'organiser les interfaces réseaux sous la forme de groupements de liens. Un *groupement de liens* est un ensemble de plusieurs interfaces d'un système configurées en une seule unité logique. Le groupement de liens, aussi appelé *jonction*, est défini par la norme IEEE 802.3ad Link Aggregation Standard (`http://www.ieee802.org/3/index.html`).

La norme IEEE 802.3ad décrit la manière d'associer les capacités de plusieurs liens Ethernet duplex intégral à un seul lien logique. Un tel groupement de liens est ensuite traité en tant que lien unique.

Le groupement de liens fournit les fonctions suivantes :

- **Plus grande bande passante** – Les capacités de plusieurs liens sont réunies en un seul lien logique.
- **Basculement/rétablissement automatique** – Le trafic sur un lien rompu est basculé vers un lien actif du groupement.
- **Équilibrage de charge** – Le trafic entrant et sortant est distribué en fonction des stratégies d'équilibrage de charge sélectionnées par l'utilisateur (par exemple, adresses sources et cibles MAC ou IP).
- **Prise en charge de la redondance** – Deux systèmes peuvent être configurés avec des groupements parallèles.
- **Administration améliorée** – Toutes les interfaces sont administrées de façon unitaire.
- **Réduction du nombre de drains dans le pool d'adresses réseau** – Le groupement entier peut être assigné à une seule adresse IP.

Notions de base sur les groupements de liens

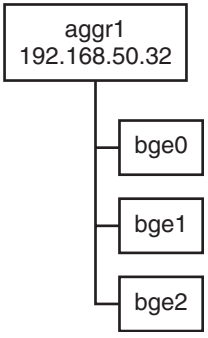
La topologie élémentaire d'un groupement de liens se définit par un ensemble unique contenant plusieurs interfaces physiques. La création de groupements de liens élémentaires est utile dans les cas suivants :

- Systèmes exécutant une application avec un trafic distribué intense. Dédiez dans ce cas un groupement de liens au trafic de cette application.
- Sites avec un nombre d'adresses IP limité, mais sur lesquels une large bande passante est nécessaire. Grâce au groupement de liens, vous pouvez réunir un grand nombre d'interfaces sous une seule adresse IP.

- Sites sur lesquels les interfaces internes doivent être masquées. Avec l'adresse IP d'un groupement de liens, les applications externes n'ont pas accès aux interfaces.

La Figure 6–3 illustre un groupement de liens créé sur un serveur hébergeant un site Web connu. La bande passante doit être élargie afin d'assurer le bon fonctionnement du trafic de requêtes entre les clients en ligne et le serveur de la base de données du site. Pour des raisons de sécurité, les interfaces individuelles de ce serveur doivent être masquées aux applications externes. La solution consiste à créer un groupement `aggr1` avec l'adresse IP `192.168.50.32`. Ce groupement se compose de trois interfaces, de `bge0` à `bge2`. Chaque interface est dédiée à la transmission du trafic sortant en réponse aux requêtes des clients. Toutes ces interfaces possèdent la même adresse sortante sur le trafic de paquets, `aggr1 : 192.168.50.32`.

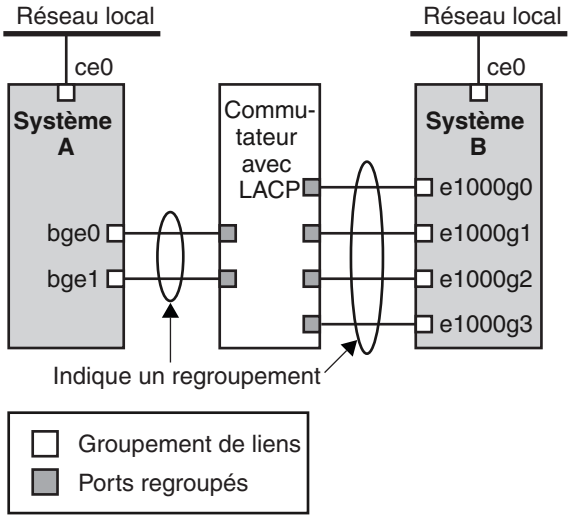
FIGURE 6–3 Topologie élémentaire d'un groupement de liens



La Figure 6–4 décrit un réseau local constitué de deux systèmes possédant chacun un groupement. Les deux systèmes sont connectés par un commutateur. Pour exécuter un groupement par le biais d'un commutateur, celui-ci doit prendre en charge la technologie de groupement. Ce type de configuration s'applique particulièrement bien aux systèmes à haute disponibilité ainsi qu'aux systèmes redondants.

Sur cette figure, le système A possède un groupement composé de deux interfaces, `bge0` et `bge1`. Ces interfaces sont connectées au commutateur par le biais de ports groupés. Le système B possède un groupement de quatre interfaces, allant de `e1000g0` à`e1000g3`. Ces interfaces sont également connectées au commutateur par le biais de ports groupés.

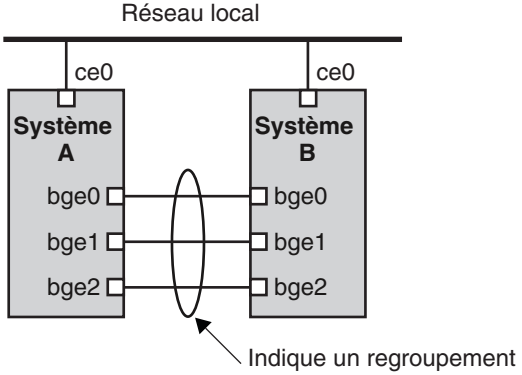
FIGURE 6–4 Topologie d'un groupement avec un commutateur



Groupements de liens dos à dos

La topologie d'un groupement de liens dos à dos consiste en deux systèmes distincts directement connectés l'un à l'autre (voir figure suivante). Ces systèmes exécutent deux groupements parallèles.

FIGURE 6–5 Topologie élémentaire d'un groupement dos à dos



Sur cette figure, le périphérique `bge0` du système A est directement connecté au périphérique `bge0` du système B, etc. Cela permet aux systèmes A et B de prendre en charge la redondance

ainsi que les services de haute disponibilité et d'assurer des communications haut débit entre les deux systèmes. Chaque système possède une interface `ce0` dédiée au flux du trafic au sein du réseau local.

Les groupements de liens dos à dos sont le plus fréquemment utilisés avec les serveurs de base de données mis en miroir. Chaque serveur doit être mis à jour en même temps que l'autre et nécessite pour cela une large bande passante ainsi qu'un flux haut débit et une grande fiabilité. Les groupements de liens dos à dos sont le plus fréquemment utilisés dans les centres de données.

Stratégies et équilibrage de charge

Avant de mettre en oeuvre un groupement de liens, définissez une stratégie pour le trafic sortant. Cette stratégie peut spécifier la manière dont les paquets doivent être distribués entre les différents liens disponibles dans le groupement, établissant ainsi un équilibrage de charge. Vous pouvez élaborer la stratégie pour le groupement avec l'un des spécificateurs de couche décrits ci-dessous :

- **L2** – Détermine le lien sortant en hachant l'en-tête MAC (L2) de chaque paquet.
- **L3** – Détermine le lien sortant en hachant l'en-tête IP (L3) de chaque paquet.
- **L4** – Détermine le lien sortant en hachant l'en-tête TCP, UDP ou autre en-tête ULP (L4) de chaque paquet.

Vous pouvez également combiner plusieurs de ces stratégies. L4 constitue la stratégie par défaut. Pour plus d'informations, reportez-vous à la page de manuel `dladm`(1M).

Mode de groupement et commutateurs

Si la topologie du groupement nécessite une connexion à un commutateur, vérifiez si le commutateur prend en charge le *protocole de contrôle des groupements de liens (Link Aggregation Control Protocol, LACP)*. Si c'est le cas, vous devez configurer le LACP de manière à ce qu'il fonctionne avec le commutateur et le groupement. Cependant, vous pouvez définir l'un des *modes* de fonctionnement suivants pour le LACP :

- **Off (inactif)** – Mode des groupements par défaut. Ce mode ne génère pas les paquets LACP, ou *PDULACP*.
- **Active (actif)** – Ce mode génère des PDULACP à une fréquence d'intervalle personnalisable.
- **Passive (passif)** – Ce mode ne génère un PDULACP que lorsqu'il en reçoit un du commutateur. Si le commutateur et le groupement sont définis sur le mode passif, ils ne peuvent échanger aucun PDULACP.

Pour plus d'informations sur la syntaxe à utiliser, reportez-vous à la page de manuel `dladm`(1M) ainsi qu'à la documentation fournie par le fabricant du commutateur.

Conditions requises pour la création de groupements de liens

Vous devez respecter les conditions suivantes pour configurer un groupement de liens :

- Le groupement doit être créé à l'aide de la commande `dladm`.
- Une interface montée ne peut pas être membre d'un groupement.
- Les interfaces doivent être de type GLDv3 : `xge`, `e1000g` et `bge`.
- Toutes les interfaces du groupement doivent s'exécuter à la même vitesse et en mode duplex intégral.
- Vous devez définir les adresses MAC sur True dans le paramètre EEPROM `local-mac-address?` (voir les instructions de la section Garantie de l'unicité de l'adresse MAC d'une interface).

▼ Procédure de création d'un groupement de liens

Avant de commencer

Remarque – Les groupements de liens ne fonctionnent qu'avec des liens de même vitesse, en mode duplex intégral et point à point. Assurez-vous que les interfaces de votre groupement répondent à ces critères.

Configurez les éléments suivants avant d'insérer un commutateur dans la topologie du groupement :

- Les ports du commutateur doivent pouvoir être utilisés dans un groupement.
- Si le commutateur prend en charge le LACP, celui-ci doit être configuré en mode actif ou passif.

1 Connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Identifiez les interfaces installées sur le système.

```
# dladm show-link
```

3 Identifiez les interfaces montées.

```
# ifconfig -a
```

4 Créez un groupement.

```
# dladm create-aggr -d interface -d interface [...]key
```

interface Nom du périphérique correspondant à l'interface membre du groupement.

clé Numéro identifiant le groupement. Le plus petit numéro de clé est 1. Une clé de ne peut avoir le numéro zéro.

Exemple :

```
# dladm create-aggr -d bge0 -d bge1 1
```

5 Configurez et montez le nouveau groupement créé.

```
# ifconfig aggrkey plumb IP-address up
```

Exemple :

```
# ifconfig aggr1  plumb 192.168.84.14 up
```

6 Vérifiez le statut du groupement que vous venez de créer.

```
# dladm show-aggr
```

La sortie suivante s'affiche :

```
key: 1 (0x0001) policy: L4      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby
```

Cette sortie indique qu'un groupement avec la clé 1 et la stratégie L4 a été créé.

7 (Facultatif) Pour conserver la configuration des adresses IP du groupement de liens à chaque réinitialisation :

a. Si le groupement possède des adresses IPv4, créez un fichier nommé `/etc/hostname.aggr`*clé*. Si le groupement possède des adresses IPv6, créez un fichier nommé `/etc/hostname6.aggr`*clé*.

b. Saisissez l'adresse IPv4 ou IPv6 du groupement de liens dans le fichier.

Par exemple, pour conserver la configuration des adresses IP du groupement créé dans cette procédure, créez le fichier suivant :

```
# vi /etc/hostname.aggr1
192.168.84.14
```

c. Effectuez une reconfiguration au démarrage.

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

d. Assurez-vous que la configuration du groupement de liens définie dans le fichier `/etc/hostname.aggr.`*key* a été appliquée.

```
# ifconfig -a
.
.
aggr1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 192.168.84.14 netmask ff000000 broadcast 192.255.255.
```

Exemple 6–4 Création d'un groupement de liens

Cet exemple présente les commandes à exécuter pour créer un groupement de liens constitués de deux périphériques, `bge0` et `bge1`, ainsi que la sortie obtenue.

```
# dladm show-link
ce0             type: legacy    mtu: 1500       device: ce0
ce1             type: legacy    mtu: 1500       device: ce1
bge0            type: non-vlan  mtu: 1500       device: bge0
bge1            type: non-vlan  mtu: 1500       device: bge1
bge2            type: non-vlan  mtu: 1500       device: bge2
# ifconfig -a
lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.84.253 netmask ffffff00 broadcast 192.168.84.255
        ether 0:3:ba:7:84:5e
# dladm create-aggr -d bge0 -d bge1 1
# ifconfig aggr1 plumb 192.168.84.14 up
# dladm show-aggr
key: 1 (0x0001) policy: L4      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby

# ifconfig -a
lo0: flags=2001000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.84.253 netmask ffffff00 broadcast 192.168.84.255
        ether 0:3:ba:7:84:5e
aggr1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 192.168.84.14 netmask ff000000 broadcast 192.255.255.255
        ether 0:3:ba:7:84:5e
```

Remarque : les deux interfaces utilisées pour ce groupement n'ont pas été montées au préalable par `ifconfig`.

▼ Procédure de modification d'un groupement

Cette procédure permet d'apporter les modifications suivantes à la définition d'un groupement :

- modification de la stratégie pour le groupement ;

- modification du mode pour le groupement.

1 Connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Modifiez le groupement afin de changer de stratégie.

```
# dladm modify-aggr -Ppolicy key
```

stratégie Nom de la stratégie ou des stratégies telles que L2, L3 et L4 (voir l'explication de la section “Stratégies et équilibrage de charge” à la page 165).

clé Numéro identifiant le groupement. Le plus petit numéro de clé est 1. Une clé de ne peut avoir le numéro zéro.

3 Si LACP est exécuté sur le commutateur auquel les périphériques du groupement sont connectés, modifiez le groupement afin qu'il prenne en charge le protocole LACP.

Si le commutateur exécute le LACP en mode passif, veillez à définir le groupement sur le mode actif.

```
# dladm modify-aggr -l LACP mode -t timer-value key
```

`-l` *mode LACP* Mode LACP dans lequel le groupement s'exécute. Les valeurs de cette variable sont les suivantes : `active`, `passive` et `off`.

`-t` *valeur d'horloge* Valeur de l'horloge du LACP (`short` ou `long`).

clé Numéro identifiant le groupement. Le plus petit numéro de clé est 1. Une clé de ne peut avoir le numéro zéro.

Exemple 6–5 Modification d'un groupement de liens

L'exemple suivant décrit la procédure à suivre pour modifier la stratégie de groupement `aggr1` en L2 et activer le mode LACP utilisé.

```
# dladm modify-aggr -P L2 1
# dladm modify-aggr -l active -t short 1
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby
```

▼ Procédure de suppression d'une interface d'un groupement

1 **Connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Supprimez une interface du groupement.**

```
# dladm remove-aggr -d interface
```

Exemple 6–6 Suppression d'interfaces d'un groupement

Cet exemple décrit la procédure de suppression des interfaces du groupement `aggr1`.

```
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby
# dladm remove-aggr -d bge1 1
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
```

▼ Procédure de suppression d'un groupement

1 **Connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Supprimez le groupement.**

```
# dladm delete-aggr key
```

clé Numéro identifiant le groupement. Le plus petit numéro de clé est 1. Une clé de ne peut avoir le numéro zéro.

Exemple 6–7 Procédure de suppression d'un groupement

Cet exemple décrit la procédure de suppression du groupement `aggr1`.

```
# dladm show-aggr
key: 1 (0x0001) policy: L2      address: 0:3:ba:7:84:5e (auto)
     device   address           speed     duplex  link    state
# dladm delete-aggr -d 1
```

▼ Configuration de réseaux VLAN via un groupement de liens

De la même manière que vous configurez des réseaux VLAN par le biais d'une interface, vous pouvez également créer des VLAN via un groupement de liens. Les réseaux VLAN sont décrits à la section "Administration de réseaux locaux virtuels" à la page 156. Cette section décrit la configuration des réseaux VLAN et les groupements de liens.

Avant de commencer Configurez d'abord le groupement de liens avec une adresse IP valide. Notez la valeur `key` du groupement. Vous en aurez besoin pour créer des réseaux VLAN via le groupement. Pour créer des groupements de liens, reportez-vous à la section "Procédure de création d'un groupement de liens" à la page 166.

1. **Si un groupement de liens a déjà été créé auparavant, retrouvez la clé de groupement correspondante.**

   ```
   # dladm show-aggr
   ```

2. **Créez les réseaux VLAN via le groupement de liens.**

   ```
   # ifconfig aggrVIDkey plumb
   ```

   où

   VID L'ID du VLAN

   clé La clé du groupement de liens par le biais duquel le réseau VLAN est créé. La clé doit comporter trois chiffres. Par exemple, si la clé du groupement est `1`, le numéro de clé inclus dans le nom du réseau local virtuel est `001`.

3. **Répétez l'étape 2 pour créer d'autres VLAN via le groupement.**

4. **Configurez les VLAN avec des adresses IP valides.**

5. **Pour créer des configurations persistantes VLAN, ajoutez les informations d'adresse IP correspondant aux fichiers de configuration `/etc/hostname.`*VLAN*.**

Exemple 6–8 Configuration de plusieurs réseaux locaux virtuels via un groupement de liens

Dans cet exemple, deux réseaux VLAN sont configurés sur un groupement de liens. Le résultat de la commande `dladm show-aggr` indique que la clé du groupement de liens est `1`. Les identifiants VLAN (VID) `193` et `194` sont respectivement assignés aux réseaux VLAN.

```
# dladm show-aggr
key: 1 (0x0001) policy: L4      address: 0:3:ba:7:84:5e (auto)
device   address           speed         duplex  link    state
bge0     0:3:ba:7:b5:a7    1000  Mbps    full    up      attached
bge1     0:3:ba:8:22:3b    0     Mbps    unknown down    standby

# ifconfig aggr193001 plumb
# ifconfig aggr193001 192.168.10.5/24 up

# ifconfig aggr194001 plumb
# ifconfig aggr194001 192.168.10.25/24 up

# vi /etc/hostname.aggr193001
192.168.10.5/24

# vi /etc/hostname.aggr194001
192.168.10.25/24
```

◆ ◆ ◆ CHAPITRE 7

Configuration d'un réseau IPv6 (tâches)

Ce chapitre contient les informations de configuration du protocole IPv6 sur un réseau. Il aborde les principaux thèmes suivants :

Pour une présentation des concepts IPv6, reportez-vous au Chapitre 3, "Présentation d'IPv6". Pour obtenir le détail des tâches de planification IPv6, reportez-vous au Chapitre 4, "Planification d'un réseau IPv6 (tâches)". Pour consulter des informations plus détaillées sur les tâches abordées dans ce chapitre, reportez-vous au Chapitre 11, "Présentation détaillée de IPv6 (référence)".

Configuration d'une interface IPv6

La première étape du processus de configuration IPv6 consiste à activer le protocole sur une interface. Vous pouvez activer la prise en charge du protocole IPv6 lors de l'installation d'Oracle Solaris ou de la configuration du protocole sur les interfaces d'un système installé.

Lors de l'installation d'Oracle Solaris, vous pouvez activer le protocole IPv6 sur une ou plusieurs interfaces d'un système. Une fois l'installation terminée, les fichiers et les tables IPv6 suivants sont définis :

- Chacune des interfaces sur lesquelles le protocole IPv6 a été activé est associée à un fichier `/etc/hostname6.`*interface* (par exemple, `hostname6.dmfe0`).

- Sur Solaris 10 11/06 et les versions précédentes, le fichier `/etc/inet/ipnodes` est créé. Une fois l'installation terminée, ce fichier contient en principe uniquement les adresses loopback IPv6 et IPv4.
- Le fichier `/etc/nsswitch.conf` est modifié de manière à autoriser les recherches à l'aide des adresses IPv6.
- La table des règles de sélection des adresses IPv6 est créée. Cette table définit l'ordre de priorité des formats d'adresse IP à utiliser pour la transmission des données sur une interface IPv6.

Cette section décrit la procédure d'activation du protocole IPv6 sur les interfaces d'un système installé.

Activation du protocole IPv6 sur une interface (liste des tâches)

Le tableau suivant répertorie les différentes tâches de configuration des interfaces IPv6. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Voir
Activation du protocole IPv6 sur une interface d'un système sur lequel Oracle Solaris est déjà installé.	Cette tâche permet d'activer le protocole IPv6 sur une interface après l'installation d'Oracle Solaris.	"Activation d'une interface IPv6 pour la session actuelle" à la page 174
Définition d'une interface IPv6 persistante après les réinitialisations.	Cette tâche permet de conserver l'adresse IPv6 de l'interface.	"Activation d'interfaces IPv6 persistantes" à la page 176
Désactivation de la configuration automatique de l'adresse IPv6.	Cette tâche permet de configurer manuellement l'ID d'interface de l'adresse IPv6.	"Procédure de désactivation de la configuration automatique des adresses IPv6" à la page 178

▼ Activation d'une interface IPv6 pour la session actuelle

La première étape du processus de configuration IPv6 consiste à activer le protocole sur les interfaces des systèmes à définir en tant que nœuds IPv6. En principe, l'adresse IPv6 de l'interface est définie via le processus de configuration automatique décrit à la section "Configuration automatique d'adresse IPv6" à la page 84. Vous pouvez alors personnaliser la configuration du nœud selon sa fonction au sein du réseau IPv6 (hôte, serveur ou routeur).

Remarque – Si l'interface est définie sur un lien sur lequel un routeur publie un préfixe IPv6, ce préfixe de site figure dans les adresses configurées automatiquement. Pour plus d'informations, reportez-vous à la section "Procédure de configuration d'un routeur compatible IPv6" à la page 180.

La procédure suivante explique comment activer le protocole IPv6 sur une interface ajoutée après l'installation d'Oracle Solaris.

Avant de commencer Effectuez les différentes procédures de planification du réseau IPv6 (mise à jour des composants matériels et logiciels, préparation du plan d'adressage, etc.). Pour plus d'informations, reportez-vous à la section "Planification IPv6 (liste des tâches)" à la page 87.

1. **Connectez-vous au futur nœud IPv6 en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Si l'interface n'existe pas, créez-la.**

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

3. **Activez le protocole IPv6 sur une interface.**

   ```
   # ifconfig inet6 interface plumb up
   ```

4. **Démarrez le démon IPv6 `in.ndpd`.**

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

Remarque – Pour afficher l'état des interfaces IPv6 d'un nœud, exécutez la commande `ifconfig-a6`.

Exemple 7–1 Activation d'une interface IPv6 après l'installation

Cet exemple illustre l'activation du protocole IPv6 sur l'interface `qfe0`. Avant de commencer, vérifiez l'état de toutes les interfaces configurées sur le système.

```
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
qfe0: flags=1000863 <UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500
           index 2
        inet 172.16.27.74 netmask ffffff00 broadcast 172.16.27.255
        ether 0:3:ba:13:14:e1
```

L'interface `qfe0` est la seule interface actuellement configurée sur le système. Pour activer le protocole IPv6 sur cette interface, effectuez la procédure suivante :

```
# ifconfig inet6 qfe0 plumb up
# /usr/lib/inet/in.ndpd
# ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 0:3:ba:13:14:e1
        inet6 fe80::203:baff:fe13:14e1/10
```

Cet exemple illustre l'état de l'interface du système avant et après l'activation du protocole IPv6 sur `qfe0`. L'option `-a6` de la commande `ifconfig` affiche uniquement les informations IPv6 de `qfe0` ainsi que l'interface de loopback. La sortie indique que seule l'adresse lien-local `fe80::203:baff:fe13:14e1/10` est configurée pour `qfe0`. Cette adresse signale que pour l'instant, aucun routeur ne publie de préfixe de site sur la liaison locale du nœud.

Une fois le protocole IPv6 activé, vous pouvez afficher les adresses IPv4 et IPv6 de toutes les interfaces d'un système à l'aide de la commande `ifconfig - a`.

Étapes suivantes

- Pour configurer le nœud IPv6 en tant que routeur, reportez-vous à la section "Configuration d'un routeur IPv6" à la page 179.
- Pour conserver la configuration de l'interface IPv6 après la réinitialisation du système, reportez-vous à la section "Activation d'interfaces IPv6 persistantes" à la page 176.
- Pour désactiver la configuration automatique sur le nœud, reportez-vous à la section "Procédure de désactivation de la configuration automatique des adresses IPv6" à la page 178.
- Pour personnaliser un nœud et le définir en tant que serveur, reportez-vous aux suggestions de la section "Administration d'interfaces compatibles IPv6 sur des serveurs" à la page 190.

▼ Activation d'interfaces IPv6 persistantes

Cette section décrit la procédure d'activation d'interfaces IPv6 persistantes après la réinitialisation du système avec configuration automatique des adresses IPv6.

Remarque – Si l'interface est définie sur un lien sur lequel un routeur publie un préfixe IPv6, ce préfixe de site figure dans les adresses configurées automatiquement. Pour plus d'informations, reportez-vous à la section "Procédure de configuration d'un routeur compatible IPv6" à la page 180.

---

1. **Connectez-vous au nœud IPv6 en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Créez des adresses IPv6 pour les interfaces ajoutées après l'installation.**

   a. **Créez le fichier de configuration.**

      ```
      # touch /etc/hostname6.interface
      ```

   b. **Ajoutez des adresses au fichier de configuration.**

      ```
      inet6 ipv6-address up
      addif inet6 ipv6-address up
      ...
      ```

3. **Créer une route IPv6 statique par défaut.**

   ```
   # /usr/sbin/route -p add -inet6 default ipv6-address
   ```

4. **(Facultatif) Créez un fichier `/etc/inet/ndpd.conf` définissant les paramètres des variables d'interface du nœud.**

   Si vous devez créer des adresses temporaires pour l'interface de l'hôte, reportez-vous à la section “Utilisation d'adresses temporaires pour une interface” à la page 184. Pour de plus amples informations sur `/etc/inet/ndpd.conf`, reportez-vous à la page de manuel `ndpd.conf(4)`, ainsi qu'à la section “Fichier de configuration `ndpd.conf`” à la page 268.

5. **Réinitialisez le nœud.**

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

   Le processus de réinitialisation envoie des paquets de découverte de routeur. Si un routeur répond avec un préfixe de site, le nœud peut configurer n'importe quelle interface associée à un fichier `/etc/hostname6.`*interface* avec une adresse IPv6 globale. Dans le cas contraire, les interfaces IPv6 sont configurées uniquement avec des adresses lien-local. La réinitialisation entraîne le redémarrage de `in.ndpd` et des autres démons réseau en mode IPv6.

Exemple 7–2 Définition d'une interface IPv6 persistante après les réinitialisations système

Cet exemple illustre la procédure de conservation de la configuration IPv6 de l'interface `qfe0` après réinitialisation. Dans cet exemple, un routeur situé sur la liaison locale publie le préfixe de site et l'ID de sous-réseau `2001:db8:3c4d:15/64`.

Commencez par vérifier l'état des interfaces du système.

```
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
```

```
qfe0: flags=1000863 <UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500
          index 2
        inet 172.16.27.74 netmask ffffff00 broadcast 172.16.27.255
        ether 0:3:ba:13:14:e1

# touch /etc/hostname6.qfe0
# vi /etc/hostname6.qfe0
inet6 fe80::203:baff:fe13:1431/10 up
addif inet6 2001:db8:3c4d:15:203:baff:fe13:14e1/64 up

# route -p add -inet6 default fe80::203:baff:fe13:1431
# reboot -- -r
```

Assurez-vous que l'adresse IPv6 configurée est toujours appliquée à l'interface `qfe0`.

```
# ifconfig -a6
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
       ether 0:3:ba:13:14:e1
       inet6 fe80::203:baff:fe13:14e1/10
 qfe0:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500
         index 2
        inet6 2001:db8:3c4d:15:203:baff:fe13:14e1/64
```

La sortie de `ifconfig -a6` indique deux entrées pour `qfe0`. L'entrée standard `qfe0` inclut l'adresse MAC et l'adresse lien-local. Une seconde entrée, `qfe0:1`, indique la création d'une pseudo-interface pour l'adresse IPv6 supplémentaire de l'interface `qfe0`. La nouvelle adresse IPv6 globale `2001:db8:3c4d:15:203:baff:fe13:14e1/64` inclut le préfixe de site et l'ID de sous-réseau publiés par le routeur local.

Étapes suivantes

- Pour configurer le nouveau nœud IPv6 en tant que routeur, reportez-vous à la section "Configuration d'un routeur IPv6" à la page 179.
- Pour désactiver la configuration automatique sur le nœud, reportez-vous à la section "Procédure de désactivation de la configuration automatique des adresses IPv6" à la page 178.
- Pour personnaliser le nouveau nœud et le définir en tant que serveur, reportez-vous aux suggestions de la section "Administration d'interfaces compatibles IPv6 sur des serveurs" à la page 190.

▼ Procédure de désactivation de la configuration automatique des adresses IPv6

En règle générale, la configuration automatique d'adresse permet de générer les adresses IPv6 pour les interfaces des hôtes et des serveurs. Cependant, la désactivation de la configuration automatique peut s'avérer nécessaire, en particulier pour configurer un jeton manuellement, suivant les explications de la section "Configuration d'un jeton IPv6" à la page 188.

1. **Connectez-vous au nœud IPv6 en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Créez un fichier `/etc/inet/ndpd.conf` pour le nœud.**

   Le fichier `/etc/inet/ndpd.conf` définit les variables d'interface pour le nœud. Pour désactiver la configuration automatique de la totalité des interfaces du serveur, le fichier doit contenir les éléments suivants :

   ```
   if-variable-name StatelessAddrConf false
   ```

   Pour de plus amples informations sur `/etc/inet/ndpd.conf`, reportez-vous à la page de manuel `ndpd.conf(4)`, ainsi qu'à la section "Fichier de configuration `ndpd.conf`" à la page 268.

3. **Mettez le démon IPv6 à jour avec vos modifications.**

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

Configuration d'un routeur IPv6

La première étape de configuration d'IPv6 sur un réseau consiste à configurer IPv6 sur un routeur. La configuration de routeur implique d'effectuer un certain nombre de tâches distinctes, lesquelles sont décrites dans cette section. Vous pouvez effectuer une partie ou la totalité de ces tâches, en fonction des exigences de votre site.

Configuration de routeur IPv6 (liste des tâches)

Effectuez les tâches suivantes selon leur ordre d'affichage dans le tableau suivant pour configurer le réseau IPv6. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Voir
1. Assurez-vous de bien remplir les conditions préalables avant de commencer la configuration d'IPv6.	Vous devez terminer la planification des tâches et l'installation d'Oracle Solaris avec des interfaces compatibles avec le protocole IPv6 avant de configurer un routeur compatible avec le protocole IPv6.	Chapitre 4, "Planification d'un réseau IPv6 (tâches)" et "Configuration d'une interface IPv6" à la page 173.
2. Configurez un routeur.	Définissez le préfixe de site pour le réseau.	"Procédure de configuration d'un routeur compatible IPv6" à la page 180

Tâche	Description	Voir
3. Configurez les interfaces de tunnel sur le routeur.	Paramétrez un tunnel manuel ou une interface de tunnel 6to4 sur le routeur. Les tunnels sont nécessaires car ils permettent au réseau local IPv6 de communiquer avec d'autres réseaux IPv6 isolés.	■ "Procédure de configuration d'un tunnel 6to4" à la page 195 ■ "Procédure de configuration manuelle de tunnels IPv6 sur un réseau IPv4" à la page 193 ■ "Procédure de configuration manuelle de tunnels IPv6 sur un réseau IPv6" à la page 194 ■ "Procédure de configuration de tunnels IPv4 sur un réseau IPv6" à la page 195
4. Configurez les commutateurs sur le réseau.	Si votre configuration réseau inclut des commutateurs, configurez-les pour IPv6 à ce stade du processus de configuration.	Reportez-vous à la documentation du fabricant du commutateur.
5. Configurez tout hub présent sur votre réseau.	Si votre configuration réseau inclut des hubs, configurez-les pour IPv6 à ce stade du processus de configuration.	Reportez-vous à la documentation du fabricant du commutateur.
6. Configurez le service de noms de réseau pour IPv6.	Configurez votre service de noms principal (DNS, NIS ou LDAP) afin de reconnaître les adresses IPv6 après la configuration du routeur pour IPv6.	"Procédure d'ajout d'adresses IPv6 à DNS" à la page 201
7. (Facultatif) Modifiez les adresses pour les interfaces compatibles IPv6 sur les hôtes et les serveurs.	Une fois la configuration du routeur IPv6, effectuez des modifications supplémentaires sur les hôtes et les serveurs compatibles IPv6.	"Modification de la configuration d'interface IPv6 pour les hôtes et les serveurs" à la page 184
Configurez les applications pour la prise en charge d'IPv6.	Différentes applications peuvent requérir différentes actions afin de prendre en charge IPv6.	Reportez-vous à la documentation des applications.

▼ Procédure de configuration d'un routeur compatible IPv6

Cette procédure suppose que toutes les interfaces du routeur ont été configurées en fonction du protocole IPv6 lors de l'installation d'Oracle Solaris.

1 Sur le système destiné à devenir le routeur IPv6, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Répertoriez les interfaces du routeur qui ont été configurées pour IPv6 lors de l'installation.

```
# ifconfig -a
```

Vérifiez la sortie afin de vous assurer que les interfaces que vous souhaitiez configurer pour IPv6 sont bien montées avec des adresses lien-local. L'exemple de sortie de la commande `ifconfig -a` indique les adresses IPv4 et IPv6 configurées pour les interfaces du routeur.

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
dmfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 172.16.26.232 netmask ffffff00 broadcast 172.16.26.255
        ether 0:3:ba:11:b1:15
dmfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4 mtu 1500 index 3
        inet 172.16.26.220 netmask ffffff00 broadcast 172.16.26.255
        ether 0:3:ba:11:b1:16
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
dmfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 0:3:ba:11:b1:15
        inet6 fe80::203:baff:fe11:b115/10
dmfe1: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 3
        ether 0:3:ba:11:b1:16
        inet6 fe80::203:baff:fe11:b116/10
```

La sortie indique également que l'interface réseau principale `dmfe0` et l'interface supplémentaire `dmfe1` ont été configurée lors de l'installation avec les adresses IPv6 lien-local `fe80::203:baff:fe11:b115/10` et `fe80::203:baff:fe11:b116/10`.

3 Configurez le transfert de paquets IPv6 sur toutes les interfaces du routeur.

Pour Solaris 10 11/03 et versions antérieures, utilisez la commande suivante :

```
# routeadm -e ipv6-forwarding -u
```

Utilisez l'un des éléments suivants pour activer le transfert de paquets :

- Utilisez la commande `routeadm` comme suit :

  ```
  # routeadm -e ipv6-forwarding -u
  ```

- Utilisez la commande SMF (Service Management Facility, utilitaire de gestion des services) suivante, comme suit :

  ```
  # svcadm enable ipv6-forwarding
  ```

4 Démarrez le démon de routage.

Le démon `in.ripngd` gère le routage IPv6.

Dans le cas de Solaris 10 11/06 et des versions antérieures, lancez `in.ripngd` en saisissant la commande suivante :

```
# routeadm -e ipv6-routing
# routeadm -u
```

Activez le routage IPv6 à l'aide de l'une des méthodes suivantes :

- Utilisez la commande `routeadm` comme suit :

```
# routeadm -e ipv6-routing -u
```

- Utilisez SMF pour activer le routage IPv6 :

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

Pour obtenir des informations sur la syntaxe de la commande `routeadm`, reportez-vous à la page de manuel `routeadm(1M)`.

5 Créez le fichier `/etc/inet/ndpd.conf`.

Spécifiez le préfixe de site que doit publier le routeur et les autres informations de configuration dans `/etc/inet/ndpd.conf`. Ce fichier est lu par le démon `in.ndpd`, qui implémente le protocole de détection de voisins IPv6.

Pour obtenir une liste des variables et des valeurs autorisables, reportez-vous à la section "Fichier de configuration `ndpd.conf`" à la page 268 et à la page de manuel `ndpd.conf(4)`.

6 Saisissez le texte suivant dans le fichier `/etc/inet/ndpd.conf` :

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

Ce texte indique au démon `in.ndpd` qu'il doit envoyer les publications de routeur à toutes les interfaces du routeur qui sont configurées pour IPv6.

7 Ajoutez du texte supplémentaire au fichier `/etc/inet/ndpd.conf` pour configurer le préfixe de site sur les différentes interfaces du routeur.

Le texte doit posséder le format suivant :

`prefix` *global-routing-prefix*`:`*subnet ID*`/64` *interface*

Le fichier d'exemple `/etc/inet/ndpd.conf` suivant configure le routeur de sorte qu'il publie le préfixe de site `2001:0db8:3c4d::/48` sur les interfaces `dmfe0` et `dmfe1`.

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on

if dmfe0 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:15::0/64 dmfe0

if dmfe1 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:16::0/64 dmfe1
```

8 Redémarrez le système.

Le routeur IPv6 commence la publication sur la liaison locale de tout préfixe de site dans le fichier `ndpd.conf`.

Exemple 7–3 Sortie `ifconfig` affichant des interfaces IPv6

L'exemple suivant illustre la sortie de la commande `ifconfig -a` telle que vous la recevriez une fois la procédure "Configuration d'un routeur IPv6" à la page 179 terminée.

```
lo0: flags=1000849 <UP LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
dmfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 172.16.15.232 netmask ffffff00 broadcast 172.16.26.255
        ether 0:3:ba:11:b1:15
dmfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4 mtu 1500 index 3
        inet 172.16.16.220 netmask ffffff00 broadcast 172.16.26.255
        ether 0:3:ba:11:b1:16
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
dmfe0: flags=2100841 <UP,RUNNING,MULTICAST,ROUTER,IPv6> mtu 1500 index 2
        ether 0:3:ba:11:b1:15
        inet6 fe80::203:baff:fe11:b115/10
dmfe0:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6> mtu 1500
          index 2
        inet6 2001:db8:3c4d:15:203:baff:fe11:b115/64
dmfe1: flags=2100841 <UP,RUNNING,MULTICAST,ROUTER,IPv6> mtu 1500 index 3
        ether 0:3:ba:11:b1:16
        inet6 fe80::203:baff:fe11:b116/10
dmfe1:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6> mtu 1500
           index 3
        inet6 2001:db8:3c4d:16:203:baff:fe11:b116/64
```

Dans cet exemple, chaque interface configurée pour IPv6 possède maintenant deux adresses. L'entrée avec le nom de l'interface, comme `dmfe0`, indique l'adresse lien-local de l'interface. L'entrée avec le format *interface:n*, tel que `dmfe0:1`, indique une adresse globale IPv6. Cette adresse inclut le préfixe de site que vous avez configuré dans le fichier `/etc/ndpd.conf`, en plus de l'ID d'interface.

Voir aussi

- Pour configurer des tunnels à partir des routeurs identifiés dans la topologie de réseau IPv6, reportez-vous à la section "Configuration de tunnels pour la prise en charge d'IPv6" à la page 192.
- Pour obtenir des informations sur la configuration de commutateurs et de hubs sur votre réseau, reportez-vous à la documentation du fabricant.
- Pour configurer les hôtes IPv6, reportez-vous à la section "Modification de la configuration d'interface IPv6 pour les hôtes et les serveurs" à la page 184.
- Pour améliorer la prise en charge d'IPv6 sur les serveurs, reportez-vous à la section "Administration d'interfaces compatibles IPv6 sur des serveurs" à la page 190.
- Pour plus d'informations sur les commandes, fichiers et démons IPv6, reportez-vous à la section "Implémentation IPv6 sous Oracle Solaris" à la page 267.

Modification de la configuration d'interface IPv6 pour les hôtes et les serveurs

Cette section explique comment modifier la configuration d'interfaces compatibles IPv6 sur les nœuds qui sont des hôtes ou des serveurs. Dans la plupart des cas, il est conseillé d'utiliser la configuration automatique d'interfaces compatibles IPv6, comme expliqué dans la section "Présentation de la configuration automatique sans état" à la page 84. Vous pouvez cependant, le cas échéant, modifier l'adresse IPv6 d'une interface comme expliqué dans les tâches décrites dans cette section.

Modification de la configuration d'une interface IPv6 (liste des tâches)

Le tableau suivant répertorie les différentes tâches permettant de modifier un réseau IPv6. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Voir
Désactivation de la configuration automatique de l'adresse IPv6.	Cette tâche permet de configurer manuellement l'ID d'interface de l'adresse IPv6.	"Procédure de désactivation de la configuration automatique des adresses IPv6" à la page 178
Créez une adresse temporaire pour un hôte.	Masquez l'ID d'interface de l'hôte en configurant une adresse temporaire créée de façon aléatoire, utilisée comme les 64 bits inférieurs de l'adresse.	"Procédure de configuration d'une adresse temporaire" à la page 185
Configurez un jeton pour l'ID d'interface d'un système.	Créez un jeton de 64 bits à utiliser en tant qu'ID d'interface dans une adresse IPv6.	"Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur" à la page 188

Utilisation d'adresses temporaires pour une interface

Une *adresse temporaire* IPv6 contient un numéro de 64 bits généré de manière aléatoire en tant qu'ID d'interface, plutôt que l'adresse MAC d'une interface. Vous pouvez utiliser des adresses temporaires pour toute interface d'un nœud IPv6 dont vous souhaitez préserver l'anonymat. Par exemple, il peut s'avérer utile d'employer des adresses temporaires pour les interfaces d'un hôte devant accéder à des serveurs Web publics. Les adresses temporaires implémentent des améliorations de confidentialité pour IPv6. Ces améliorations sont décrites dans le document RFC 3041, disponible à l'adresse "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" (`http://www.ietf.org/rfc/rfc3041.txt?number=3041`).

L'activation d'une adresse temporaire s'effectue dans le fichier `/etc/inet/ndpd.conf`, pour une ou plusieurs interfaces, le cas échéant. Cependant, à la différence des adresses IPv6 standard configurées automatiquement, une adresse temporaire se compose d'un préfixe de sous-réseau de 64 bits et d'un numéro de 64 bits généré de façon aléatoire. Ce numéro devient le segment correspondant à l'ID d'interface de l'adresse IPv6. Une adresse lien-local n'est pas générée avec l'adresse temporaire en tant qu'ID d'interface.

Notez que la *durée de vie préférée* par défaut des adresses temporaires est d'un jour. Lors de l'activation de la génération d'adresses temporaires, il est également possible de configurer les variables suivantes dans le fichier `/etc/inet/ndpd.conf` :

Durée de vie valide TmpValidLifetime	Durée d'existence de l'adresse temporaire ; une fois la durée écoulée, l'adresse est supprimée de l'hôte.
Durée de vie préférée TmpPreferredLifetime	Temps écoulé avant que l'adresse temporaire soit désapprouvée. Cette durée doit être inférieure à la durée de vie valide.
Régénération d'adresse	Durée avant l'expiration de la durée de vie préférée, pendant laquelle l'hôte devrait générer une nouvelle adresse temporaire.

La durée des adresses temporaires s'exprime comme suit :

n	*n* nombre de secondes, valeur par défaut
n `h`	*n* nombre d'heures (`h`)
n `d`	*n* nombre de jours (`d`)

▼ Procédure de configuration d'une adresse temporaire

1 Connectez-vous à l'hôte IPv6 en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Si nécessaire, activez IPv6 sur les interfaces de l'hôte.

Reportez-vous à la section “Activation d'une interface IPv6 pour la session actuelle” à la page 174.

3 Modifiez le fichier `/etc/inet/ndpd.conf` afin d'activer la génération d'adresses temporaires.

- Pour configurer des adresses temporaires sur les interfaces d'un hôte, ajoutez la ligne suivante au fichier `/etc/inet/ndpd.conf` :

```
ifdefault TmpAddrsEnabled true
```

- Pour configurer une adresse temporaire pour une interface spécifique, ajoutez la ligne suivante au fichier `/etc/inet/ndpd.conf` :

  ```
  if interface TmpAddrsEnabled true
  ```

4 (Facultatif) Spécifiez la durée de vie valide de l'adresse temporaire.

```
ifdefault TmpValidLifetime duration
```

Cette syntaxe spécifie la durée de vie valide de toutes les interfaces d'un hôte. La *durée* s'exprime en secondes, en heures ou en jours. La durée de vie valide par défaut est de 7 jours. Vous pouvez également utiliser `TmpValidLifetime` avec des mots-clés d'*interface* `if` afin de spécifier la durée de vie valide de l'adresse temporaire d'une interface en particulier.

5 (Facultatif) Spécifiez une durée de vie préférée pour l'adresse temporaire après laquelle celle-ci est désapprouvée.

```
if interface TmpPreferredLifetime duration
```

Cette syntaxe spécifie la durée de vie préférée de l'adresse temporaire d'une interface donnée. La durée de vie préférée par défaut est d'un jour. Vous pouvez également utiliser `TmpPreferredLifetime` avec le mot-clé `ifdefault` afin de spécifier la durée de vie préférée des adresses temporaires de toutes les interfaces d'un hôte.

Remarque – La sélection d'adresse par défaut attribue une priorité moindre aux adresses IPv6 désapprouvées. Si une adresse temporaire IPv6 est désapprouvée, la sélection d'adresses par défaut choisit une adresse qui n'a pas été désapprouvées en tant qu'adresse source d'un paquet. Une adresse non désapprouvée peut être l'adresse IPv6 générée automatiquement ou, éventuellement, l'adresse IPv4 de l'interface. Pour de plus amples informations sur la sélection d'adresses par défaut, reportez-vous à la section “Administration de la sélection des adresses par défaut” à la page 229.

---

6 (Facultatif) Spécifiez la durée de production en avance de la désapprobation d'adresse, pendant laquelle l'hôte devrait générer une nouvelle adresse temporaire.

```
ifdefault TmpRegenAdvance duration
```

Cette syntaxe spécifie le délai qui doit s'écouler avant la désapprobation d'adresse pour les adresses temporaires de toutes les interfaces d'un hôte. La valeur par défaut est 5 secondes.

7 Modifiez la configuration du démon `in.ndpd`.

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

8 **Vérifiez que les adresses temporaires ont été créées en exécutant la commande `ifconfig -a6`, tel que décrit dans l'Exemple 7–5.**

La sortie de `ifconfig` doit comporter le mot `TEMPORARY` dans la même ligne que la définition d'interface.

Exemple 7–4 Variables d'adresses temporaires dans le fichier `/etc/inet/ndpd.conf`

L'exemple suivant comporte un segment d'un fichier `/etc/inet/ndpd.conf` avec les adresses temporaires activées pour l'interface du réseau principal.

```
ifdefault TmpAddrsEnabled true

ifdefault TmpValidLifetime 14d

ifdefault TmpPreferredLifetime 7d

ifdefault TmpRegenAdvance 6s
```

Exemple 7–5 Sortie de commande `ifconfig -a6` avec adresses temporaires activées

Cet exemple indique la sortie de la commande `ifconfig` une fois les adresses temporaires créées.

```
# ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
     inet6 ::1/128
hme0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
     ether 8:0:20:b9:4c:54
     inet6 fe80::a00:20ff:feb9:4c54/10
hme0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
     inet6 2001:db8:3c4d:15:a00:20ff:feb9:4c54/64
hme0:2: flags=802080841<UP,RUNNING,MULTICAST,ADDRCONF,IPv6,TEMPORARY> mtu 1500 index 2
      inet6 2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64
```

Notez que la ligne suivant l'interface `hme0:2` comprend le mot `TEMPORARY`. Cette désignation indique que l'adresse `2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64` possède un ID d'interface temporaire.

Voir aussi

- Pour définir la prise en charge du service d'attribution de noms pour les adresses IPv6, reportez-vous à la section “Configuration de prise en charge de services d'attribution de noms pour IPv6” à la page 201.
- Pour configurer des adresses IPv6 pour un serveur, reportez-vous à la section “Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur” à la page 188.
- Pour contrôler les activités sur les nœuds IPv6, reportez-vous au Chapitre 8, “Gestion d'un réseau TCP/IP (tâches)”.

Configuration d'un jeton IPv6

L'ID d'interface 64 bits d'une adresse IPv6 est également nommé *jeton*, tel que décrit dans la section "Présentation de l'adressage IPv6" à la page 76. Lors de la configuration automatique d'adresses, le jeton est associé à l'adresse MAC de l'interface. Dans la plupart des cas, les nœuds qui n'effectuent pas de routage, c'est-à-dire les hôtes et les serveurs IPv6, doivent utiliser leurs jetons configurés automatiquement.

Cependant, l'utilisation de jetons configurés automatiquement peut être problématique pour les serveurs dont les interfaces sont régulièrement dans le cadre de la maintenance système. Lorsque la carte de l'interface est modifiée, l'adresse MAC l'est également. Cela peut entraîner des problèmes pour les serveurs qui dépendent d'adresses IP. Différentes parties de l'infrastructure de réseau, comme le DNS ou le NIS, peuvent disposer d'adresses IPv6 stockées pour les interfaces du serveur.

Pour les problèmes liés aux modifications d'adresses, vous pouvez configurer un jeton manuellement pour l'utiliser en tant qu'ID d'interface dans une adresse IPv6. Pour créer le jeton, spécifiez un numéro hexadécimal de 64 bits maximum afin d'occuper la portion d'ID d'interface de l'adresse IPv6. Par la suite, lors de la configuration automatique d'adresses, le protocole de détection de voisins ne crée pas d'ID d'interface basé sur l'adresse MAC de l'interface. Le jeton créé manuellement devient l'ID d'interface. Ce jeton reste assigné à l'interface, même en cas de remplacement d'une carte.

Remarque – La différence entre les jetons spécifiés par les utilisateurs et les adresses temporaires réside dans le fait que ces dernières sont générées de façon aléatoire et non pas créées explicitement par un utilisateur.

▼ Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur

Les instructions suivantes sont particulièrement utiles pour les serveurs dont les interfaces sont régulièrement remplacées. Elles sont également valides pour la configuration de jetons spécifiés par l'utilisateur sur tout nœud IPv6.

1 Assurez-vous que l'interface à configurer avec un jeton est montée.

Avant de configurer un jeton pour l'adresse IPv6 d'une interface, vous devez monter l'interface.

```
# ifconfig a6
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 0:3:ba:13:14:e1
        inet6 fe80::203:baff:fe13:14e1/10
```

Cette sortie indique que l'interface réseau `qfe0` est montée et dispose d'une adresse lien-local `fe80::203:baff:fe13:14e1/10`. Cette adresse a été configurée automatiquement lors de l'installation.

2. **Créez un ou plusieurs numéros hexadécimaux de 64 bits à utiliser en tant que jetons pour l'interface du nœud. Pour des exemples de jetons, reportez-vous à la section "Adresse unicast lien-local" à la page 81.**

3. **Configurez chaque interface avec un jeton.**

   Utilisez le format suivant de la commande `ifconfig` pour chaque interface afin de disposer d'un ID d'interface spécifiée par l'utilisateur (jeton) :

   `ifconfig` *interface* `inet6 token` *address/64*

   Par exemple, exécutez la commande suivante afin de configurer l'interface `qfe0` avec un jeton :

   ```
   # ifconfig qfe0 inet6 token ::1a:2b:3c:4d/64
   ```

   Répétez cette étape pour chaque interface disposant d'un jeton spécifié par l'utilisateur.

4. **(Facultatif) Configurez les adresses IPv6 de sorte qu'elles persistent après réinitialisation.**

   a. **Modifiez ou créez un fichier `/etc/hostname6.`*interface* pour chaque interface configurée avec un jeton.**

   b. **Ajoutez le texte suivant au bas du fichier `/etc/hostname.6` *interface* :**

      `token ::`*token-name*`/64`**

      Par exemple, vous pouvez ajouter le texte suivant au bas du fichier `/etc/hostname6.`*interface* :

      ```
      token ::1a:2b:3c:4d/64
      ```

   Une fois le système réinitialisé, le jeton configuré dans le fichier `/etc/hostname6.` *interface* est appliqué à l'adresse IPv6 de l'interface. Cette adresse IPv6 persiste après réinitialisation.

5. **Mettez le démon IPv6 à jour avec vos modifications.**

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

Exemple 7–6 Configuration d'un jeton spécifié par l'utilisateur sur une interface IPv6

Dans l'exemple suivant, l'interface `bge0:1` possède une adresse IPv6 configurée automatiquement. Le préfixe de sous-réseau `2001:db8:3c4d:152:/64` est publié par un routeur sur la liaison locale du nœud. L'ID d'interface `2c0:9fff:fe56:8255` est généré à partir de l'adresse MAC de `bge0:1`.

```
# ifconfig -a6
lo0: flags=2002000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
        inet6 ::1/128
bge0: flags=2100801 <UP,MULTICAST,IPv6> mtu 1500 index 5
        inet6 fe80::2c0:9fff:fe56:8255/10
        ether 0:c0:9f:56:82:55
```

```
bge0:1: flags=2180801 <UP, MULTICAST,ADDRCONF,IPv6>mtu 1500 index 5
        inet6 2001:db8:3c4d:152:c0:9fff:fe56:8255/64
# ifconfig bge0 inet6 token ::1a:2b:3c:4d/64
# vi /etc/hostname6.bge0
token ::1a:2b:3c:4d/64
# pkill -HUP -in.ndpd
# ifconfig -a6
lo0: flags=2002000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
        inet6 ::1/128
bge0: flags=2100801 <UP,MULTICAST,IPv6> mtu 1500 index 5
        inet6 fe80::2c0:9fff:fe56:8255/10
        ether 0:c0:9f:56:82:55
bge0:1: flags=2180801 <UP, MULTICAST,ADDRCONF,IPv6>mtu 1500 index 5
        inet6 2001:db8:3c4d:152:1a:2b:3c:4d/64
```

Une fois le jeton configuré, l'adresse globale sur la seconde ligne d'état `bge0:1` dispose alors de `1a:2b:3c:4d` configuré pour son ID d'interface.

Voir aussi

- Pour la mise à jour des services d'attribution de noms pour les adresses IPv6 du serveur, reportez-vous à la section "Configuration de prise en charge de services d'attribution de noms pour IPv6" à la page 201.
- Pour contrôler les performances de serveur, reportez-vous au Chapitre 8, "Gestion d'un réseau TCP/IP (tâches)".

Administration d'interfaces compatibles IPv6 sur des serveurs

Lors de la planification d'IPv6 sur un serveur, vous devez prendre un certain nombre de décisions relatives à l'activation d'IPv6 sur les interfaces du serveur. Vos décisions affectent la stratégie à utiliser pour la configuration des ID d'interface, également appelés *jetons*, de l'adresse IPv6 d'une interface.

▼ Procédure d'activation d'IPv6 sur les interfaces d'un serveur

Avant de commencer

Cette procédure suppose les conditions suivantes :

- Oracle Solaris est déjà installé sur le serveur.
- Vous avez activé le protocole IPv6 sur les interfaces du serveur lors de l'installation d'Oracle Solaris ou par la suite, selon les procédures décrites dans la section "Configuration d'une interface IPv6" à la page 173.

Le cas échéant, mettez le logiciel de l'application à niveau afin d'assurer la prise en charge d'IPv6. Notez que de nombreuses applications s'exécutant sur la pile de protocole IPv4 s'exécutent également sur IPv6. Pour de plus amples informations, reportez-vous à la section "Procédure de préparation de services réseau pour la prise en charge d'IPv6" à la page 92.

1 **Sur le serveur, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Assurez-vous qu'un préfixe de sous-réseau IPv6 est configuré sur un routeur situé sur la même liaison que le serveur.**

Pour plus d'informations, reportez-vous à la section “Configuration d'un routeur IPv6” à la page 179.

3 **Utilisez la stratégie adéquate pour l'ID des interfaces compatibles IPv6 du serveur.**

Par défaut, la configuration automatique d'adresses IPv6 utilise l'adresse MAC d'une interface lors de la création de la partie ID d'interface de l'adresse IPv6. Si l'adresse IPv6 de l'interface est bien connue, remplacer une interface par une autre peut entraîner des problèmes. L'adresse MAC de la nouvelle interface sera différente. Un nouvel ID d'interface est généré lors de la configuration automatique d'adresses.

- Dans le cas d'une interface compatible IPv6 que vous ne souhaitez pas remplacer, utilisez l'adresse IPv6 configurée automatiquement, tel que présenté dans la section “Configuration automatique d'adresse IPv6” à la page 84.
- Dans le cas d'interfaces compatibles IPv6 devant apparaître anonymes hors du réseau local, vous pouvez utiliser un jeton généré de façon aléatoire comme ID d'interface. Pour obtenir des instructions et un exemple, reportez-vous à la section “Procédure de configuration d'une adresse temporaire” à la page 185.
- Dans le cas d'interfaces compatibles IPv6 que vous pensez échanger régulièrement, créez des jetons pour les ID d'interface. Pour obtenir des instructions et un exemple, reportez-vous à la section “Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur” à la page 188.

Tâches de configuration de tunnels pour la prise en charge d'IPv6 (liste des tâches)

Le tableau suivant répertorie les différentes tâches permettant de configurer différents types de tunnels IPv6. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Voir
Configuration manuelle de tunnels IPv6 sur IPv4.	Créez un tunnel IPv6 sur un réseau IPv4 manuellement. Cette solution permet d'atteindre des réseaux IPv6 distants au sein d'un réseau d'entreprise de plus grande taille, principalement IPv4.	"Procédure de configuration manuelle de tunnels IPv6 sur un réseau IPv4" à la page 193
Configuration manuelle de tunnels IPv6 sur IPv6.	Configurez manuellement un tunnel IPv6 sur un réseau IPv6. Cette solution est généralement utilisée au sein d'un réseau d'entreprise de grande taille.	"Procédure de configuration manuelle de tunnels IPv6 sur un réseau IPv6" à la page 194
Configuration manuelle de tunnels IPv4 sur IPv6.	Configurez manuellement un tunnel IPv4 sur un réseau IPv6. Cette solution est utile pour des réseaux de grande taille disposant de réseaux IPv4 et IPv6.	"Procédure de configuration de tunnels IPv4 sur un réseau IPv6" à la page 195
Configuration automatique de tunnels IPv6 sur IPv4 (tunnels 6to4).	Créez un tunnel automatique 6to4. Cette solution permet d'atteindre un site IPv6 externe sur Internet.	"Procédure de configuration d'un tunnel 6to4" à la page 195
Configuration d'un tunnel entre un routeur 6to4 et un routeur relais 6to4.	Activez un tunnel pour un routeur relais 6to4 à l'aide de la commande `6to4relay`.	"Procédure de configuration d'un tunnel 6to4 relié à un routeur relais 6to4" à la page 199

Configuration de tunnels pour la prise en charge d'IPv6

Les réseaux IPv6 sont souvent des entités isolées au sein d'un univers IPv4 de plus grande taille. Les nœuds situés sur votre réseau IPv6 peuvent avoir besoin de communiquer avec des nœuds situés sur des réseaux IPv6 isolés, soit au sein de votre entreprise, soit à distance. En règle générale, un tunnel se configure entre routeurs IPv6, mais les hôtes IPv6 peuvent également fonctionner en tant qu'extrémités de tunnels. Pour obtenir des informations relatives à la planification de tunnels, reportez-vous à la section "Planification de tunnels dans la topologie réseau" à la page 94.

Vous pouvez définir des tunnels configurés automatiquement ou manuellement pour les réseaux IPv6. L'implémentation d'Oracle Solaris IPv6 prend en charge les types d'encapsulation de tunnel suivants :

- tunnels IPv6 sur IPv4 ;
- tunnels IPv6 sur IPv6 ;
- tunnels IPv4 sur IPv6 ;
- tunnels 6to4.

Pour obtenir des descriptions conceptuelles de tunnels, reportez-vous à la section "Tunnels IPv6" à la page 290.

▼ Procédure de configuration manuelle de tunnels IPv6 sur un réseau IPv4

Cette procédure permet de configurer un tunnel entre un noeud IPv6 et un noeud IPv6 distant faisant partie d'un réseau IPv4.

1. **Connectez-vous au point d'extrémité local du tunnel en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Créez le fichier `/etc/hostname6.ip.tun` *n*.**

   Remplacez *n* par le numéro du tunnel (le premier tunnel possédant le numéro zéro). Ajoutez les entrées suivantes :

   a. **Ajoutez l'adresse source et l'adresse cible du tunnel.**

      `tsrc` *IPv4-source-address* `tdst` *IPv4-destination-address* `up`

   b. **(Facultatif) Ajoutez une interface logique pour l'adresse source et l'adresse cible du tunnel IPv6.**

      `addif` *IPv6-source-address* *IPv6-destination-address*

      Ignorez cette étape si vous souhaitez que ces adresses soient configurées automatiquement. Il n'est pas nécessaire de configurer les adresses locales des liens pour le tunnel.

3. **Redémarrez le système.**

4. **Répétez cette procédure sur l'autre point d'extrémité du tunnel.**

Exemple 7–7 Entrée à saisir dans le fichier `/etc/hostname6.ip.tun` pour configurer manuellement un tunnel IPv6 sur IPv4

L'exemple de fichier `/etc/hostname6.ip.tun` suivant est celui d'un tunnel dont les adresses source et cible globales ont été configurées manuellement.

```
tsrc 192.168.8.20 tdst 192.168.7.19 up
addif 2001:db8:3c4d:8::fe12:528 2001:db8:3c4d:7:a00:20ff:fe12:1234 up
```

▼ Procédure de configuration manuelle de tunnels IPv6 sur un réseau IPv6

Cette procédure permet de configurer un tunnel entre un nœud IPv6 et un nœud IPv6 distant faisant partie d'un réseau IPv6.

1 **Connectez-vous au point d'extrémité local du tunnel en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Créez le fichier `/etc/hostname6.ip6.tun`*n*.**

Remplacez *n* par les valeurs 0, 1, 2, etc. Ajoutez les entrées suivantes :

a. **Ajoutez l'adresse source et l'adresse cible du tunnel.**

`tsrc` *IPv6-source-address* `tdst` *IPv6-destination-address*
IPv6-packet-source-address *IPv6-packet-destination-address* `up`

b. **(Facultatif) Ajoutez une interface logique pour l'adresse source et l'adresse cible du tunnel IPv6.**

`addif` *IPv6-source-address* *IPv6-destination-address* `up`

Ignorez cette étape si vous souhaitez que ces adresses soient configurées automatiquement. Il n'est pas nécessaire de configurer les adresses locales des liens pour le tunnel.

3 **Redémarrez le système.**

4 **Répétez cette procédure sur l'autre point d'extrémité du tunnel.**

Exemple 7–8 Entrée à saisir dans le fichier `/etc/hostname6.ip6.tun` pour configurer un tunnel IPv6 sur IPv6

Cet exemple décrit la commande à saisir pour configurer un tunnel IPv6 sur un réseau IPv6.

```
tsrc 2001:db8:3c4d:22:20ff:0:fe72:668c tdst 2001:db8:3c4d:103:a00:20ff:fe9b:a1c3
fe80::4 fe80::61 up
```

▼ Procédure de configuration de tunnels IPv4 sur un réseau IPv6

Cette procédure permet de configurer un tunnel entre deux hôtes IPv4 sur un réseau IPv6. Elle s'applique aux réseaux hétérogènes possédant des sous-réseaux IPv4 séparant des sous-réseaux IPv6.

1. **Connectez-vous au point d'extrémité local du tunnel IPv4 en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Créez le fichier `/etc/hostname.ip6.tun`*n*.**

   Remplacez *n* par les valeurs 0, 1, 2, etc. Ajoutez les entrées suivantes :

   a. **Ajoutez l'adresse source et l'adresse cible du tunnel.**

      `tsrc` *IPv6-source-address* `tdst` *IPv6-destination-address*

   b. **(Facultatif) Ajoutez une interface logique pour l'adresse source et l'adresse cible du tunnel IPv6.**

      `addif` *IPv6-source-address* *IPv6-destination-address* `up`

3. **Redémarrez l'hôte local.**

4. **Répétez cette procédure sur l'autre point d'extrémité du tunnel.**

Exemple 7–9 Entrée à saisir dans le fichier `/etc/hostname6.ip6.tun` pour configurer un tunnel IPv4 sur IPv6

Cet exemple décrit la commande à saisir pour configurer un tunnel IPv4 sur un réseau IPv6.

```
tsrc 2001:db8:3c4d:114:a00:20ff:fe72:668c tdst 2001:db8:3c4d:103:a00:20ff:fe9b:a1c3
10.0.0.4 10.0.0.61 up
```

▼ Procédure de configuration d'un tunnel 6to4

Si un réseau IPv6 doit communiquer avec un réseau IPv6 distant, il est recommandé de configurer des tunnels 6to4 automatiques. Le processus de configuration d'un tunnel 6to4 inclut la définition du routeur de bordure en tant que routeur *6to4*. Ce routeur joue le rôle de point d'extrémité du tunnel 6to4 entre le réseau local et le point d'extrémité du réseau IPv6 distant.

Avant de commencer

Avant de configurer le routage 6to4 sur un réseau IPv6, effectuez les opérations suivantes :

- Configurez le réseau IPv6 sur tous les noeuds adéquats du site 6to4 concerné, comme décrit à la section "Modification de la configuration d'interface IPv6 pour les hôtes et les serveurs" à la page 184.
- Sélectionnez au moins un routeur avec une connexion sur un réseau IPv4 et définissez-le en tant que routeur 6to4.
- Configurez une adresse IPv4 unique pour la future interface du routeur 6to4 sur le réseau IPv4. L'adresse IPv4 doit être statique.

Remarque – N'utilisez pas d'adresse IPv4 allouée de façon dynamique, comme décrit au Chapitre 12, "À propos de DHCP (présentation)". Les adresses dynamiques varient, ce qui peut entraver la planification d'adresses IPv6.

---

1 Connectez-vous sur le routeur 6to4 en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Configurez une pseudointerface 6to4 sur le routeur en créant un fichier nommé `/etc/hostname6.ip.6to4tun0`.

- Si vous envisagez d'utiliser la convention recommandée (ID de sous-réseau=0 et ID d'hôte=1), choisissez le format court (short) pour le fichier `/etc/hostname6.ip.6to4tun0` :

  `tsrc` *IPv4-address* `up`

- Si vous envisagez d'utiliser une autre convention pour les ID hôte et sous-réseau, choisissez le format long pour le fichier `/etc/hostname6.ip.6to4tun0` :

  `tsrc` *IPv4-address* `2002:`*IPv4-address*`:`*subnet-ID*`:`*interface-ID*`:/64 up`

Les paramètres suivants sont requis pour le fichier `/etc/hostname6.ip.6to4tun0` :

`tsrc`	Indique que cette interface est utilisée en tant que source du tunnel.
adresse-IPv4	Spécifie (au format décimal avec points) l'adresse IPv4 configurée sur l'interface physique devant servir de pseudointerface 6to4.

Les autres paramètres sont facultatifs. Cependant, si vous décidez d'en spécifier certains, vous devrez tous les spécifier.

`2002`	Spécifie le préfixe 6to4.
adresse IPv4	Spécifie (au format hexadécimal) l'adresse IPv4 de la pseudointerface.
ID sous-réseau	Spécifie (au format hexadécimal) un sous-réseau différent de zéro.
ID-interface	Spécifie un ID d'interface différent de 1.

`/64`	Indique que le préfixe 6to4 possède une longueur de 64 bits.
`up`	Définit l'interface 6to4 sur "up".

Remarque – Les deux tunnels IPv6 du réseau doivent posséder une adresse source et une adresse cible unique. Des paquets sont déposés en conséquence. Ce type d'événement peut se produire si un routeur 6to4 crée également des tunnels par le biais de la commande `atun`. Pour plus d'informations sur la commande `atun`, reportez-vous à la page de manuel `tun(7M)`.

3 (Facultatif) Créez des pseudointerfaces 6to4 supplémentaires sur le routeur.

Chacune d'entre elles doit posséder une adresse IPv4 déjà configurée et unique.

4 Redémarrez le routeur 6to4.

5 Vérifiez le statut de l'interface.

```
# ifconfig ip.6to4tun0 inet6
```

Si l'interface est correctement configurée, une sortie similaire à celle-ci s'affiche :

```
ip.6to4tun0: flags=2200041<UP,RUNNING,NONUD,IPv6>mtu 1480 index 11
        inet tunnel src 111.222.33.44
        tunnel hop limit 60
        inet6 2002:6fde:212c:10:/64
```

6 Pour publier le routage 6to4, modifiez le fichier `/etc/inet/ndpd.conf`.

Pour plus d'informations, reportez-vous à la page de manuel `ndpd.conf(4)`.

a. Sur la première ligne, spécifiez le sous-réseau devant recevoir la publication.

Créez une entrée `if` au format suivant :

`if` *subnet-interface* `AdvSendAdvertisements 1`

Exemple : pour publier le routage 6to4 sur un sous-réseau connecté à l'interface `hme0`, remplacez *interface sous-réseau* par `hme0`.

```
if hme0 AdvSendAdvertisements 1
```

b. Sur la deuxième ligne du fichier de publication, ajoutez le préfixe 6to4.

Créez une entrée `prefix` au format suivant :

`prefix 2002:`*IPv4-address*`:`*subnet-ID*`::/64` *subnet-interface*

7 **Redémarrez le routeur.**

Vous pouvez également exécuter la commande `sighup` sur le démon de `/etc/inet/in.ndpd` pour commencer la publication du routeur. Les noeuds IPv6 de chaque sous-réseau devant recevoir le préfixe 6to4 sont alors automatiquement définis sur les nouvelles adresses 6to4 dérivées.

8 **Ajoutez ces nouvelles adresses au service de noms utilisé par le site 6to4.**

Vous trouverez les instructions correspondantes dans la section "Configuration de prise en charge de services d'attribution de noms pour IPv6" à la page 201.

Exemple 7–10 Configuration du routeur 6to4 (forme courte)

L'exemple suivant présente le fichier `/etc/hostname6.ip.6to4tun0` dans sa forme courte :

```
# cat /etc/hostname6.ip.6to4tun0
tsrc 111.222.33.44 up
```

Exemple 7–11 Configuration du routeur 6to4 (forme longue)

Voici un exemple du fichier `/etc/hostname6.ip.6to4tun0` dans sa forme longue :

```
# cat /etc/hostname6.ip.6to4tun0
tsrc 111.222.33.44 2002:6fde:212c:20:1/64 up
```

Exemple 7–12 Sortie de la commande `ifconfig` avec une pseudointerface 6to4

L'exemple suivant présente la sortie de la commande `ifconfig` pour une pseudointerface 6to4 :

```
# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NONUD,IPv6> mtu 1480 index 11
        inet tunnel src 192.168.87.188
        tunnel hop limit 60
        inet6 2002:c0a8:57bc::1/64
```

Exemple 7–13 Publications 6to4 dans `/etc/inet/ndpd.conf`

L'exemple de fichier `/etc/inet/ndpd.conf` suivant publie le routage 6to4 sur deux sous-réseaux :

```
if qfe0 AdvSendAdvertisements 1
prefix  2002:c0a8:57bc:10::/64 qfe0

if qfe1 AdvSendAdvertisements 1
prefix  2002:c0a8:57bc:2::/64 qfe1
```

Informations supplémentaires

Configuration de plusieurs routeurs sur le site 6to4

Si le site dispose de plusieurs routeurs, ceux qui se trouvent derrière le routeur 6to4 doivent pouvoir prendre en charge le routage 6to4. Si ce n'est pas le cas, configurez-les. Si le site utilise RIP, configurez la route statique du routeur 6to4 sur les autres routeurs. S'il utilise un protocole de routage commercial, il n'est pas nécessaire de créer de route statique vers le routeur 6to4.

▼ Procédure de configuration d'un tunnel 6to4 relié à un routeur relais 6to4

Attention – Pour des raisons de sécurité, la prise en charge des routeurs relais 6to4 est désactivée par défaut dans Oracle Solaris. Voir "Problèmes de sécurité lors de la création d'un tunnel vers un routeur relais 6to4" à la page 236.

Avant de commencer

Avant de configurer un tunnel relié à un routeur relais 6to4, vous devez avoir effectué les tâches suivantes :

- configuration d'un routeur 6to4 sur site, comme expliqué à la section "Procédure de configuration d'un tunnel 6to4" à la page 195 ;
- vérification des problèmes de sécurité susceptibles de se produire avec un tunnel relié à un routeur relais 6to4.

1 Connectez-vous sur le routeur 6to4 en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Vous pouvez relier un tunnel à un routeur relais 6to4 de deux façons :

- Liaison a un routeur relais 6to4 de type anycast.

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

  L'option `-e` configure un tunnel entre le routeur 6to4 et un routeur relais 6to4 anycast. Les routeurs relais 6to4 anycast possèdent l'adresse IPv4 courante `192.88.99.1`. Le routeur relais anycast le plus proche (physiquement) de votre site devient le point d'extrémité du tunnel 6to4. Ce routeur relais gère ensuite l'envoi des paquets entre votre site 6to4 et un site IPv6 natif.

Pour de plus amples informations sur les routeurs relais 6to4 Anycast, reportez-vous à la page RFC 3068, "An Anycast Prefix for 6to4 Relay Routers" (`ftp://ftp.rfc-editor.org/in-notes/rfc3068.txt`).

- Liaison a un routeur relais 6to4 de type spécifique.

  ```
  # /usr/sbin/6to4relay -e -a relay-router-address
  ```

  L'option `-a` est toujours suivie d'une adresse de routeur spécifique. Remplacez *adresse routeur relais* par l'adresse IPv4 du routeur relais 6to4 spécifique que vous souhaitez relier au tunnel.

Le tunnel relié au routeur relais 6to4 reste actif pendant la suppression de la pseudointerface du tunnel 6to4.

3 Supprimez le tunnel relié au routeur relais 6to4 lorsqu'il n'est plus nécessaire :

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

4 (Facultatif) Configurez un tunnel au routeur relais 6to4 qui conserve ses paramètres après chaque redémarrage.

Si votre site requiert, pour quelque raison qu'il soit, que les paramètres du tunnel relié au routeur relais 6to4 soient redéclarés à chaque redémarrage du routeur, effectuez la procédure suivante :

a. Modifiez le fichier `/etc/default/inetinit`.

La ligne à modifier se trouve à la fin du fichier.

b. Remplacez la valeur "NO" de la ligne `ACCEPT6TO4RELAY=NO` par "YES".

c. (Facultatif) Créez un tunnel relié à un routeur relais 6to4 spécifique dont les paramètres sont conservés après chaque redémarrage.

Pour le paramètre `RELAY6TO4ADDR`, remplacez l'adresse `192.88.99.1` par l'adresse IPv4 du routeur relais 6to4 à utiliser.

Exemple 7–14 Obtention d'informations sur le statut de la prise en charge des routeurs relais 6to4

La commande `/usr/bin/6to4relay` vous permet de savoir si les routeurs relais 6to4 sont pris en charge ou non par votre site. L'exemple suivant présente la sortie obtenue lorsque les routeurs relais 6to4 ne sont pas pris en charge (sortie par défaut d'Oracle Solaris) :

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is disabled.
```

Lorsque les routeurs relais 6to4 sont pris en charge, la sortie suivante s'affiche :

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is enabled.
IPv4 remote address of Relay Router=192.88.99.1
```

Configuration de prise en charge de services d'attribution de noms pour IPv6

Cette section décrit la procédure de configuration des services d'attribution de noms DNS et NIS pour la prise en charge de services IPv6.

Remarque – LDAP prend en charge IPv6 sans aucune configuration supplémentaire nécessaire.

Pour obtenir des informations détaillées sur l'administration DNS, NIS et LDAP, reportez-vous à la section *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

▼ Procédure d'ajout d'adresses IPv6 à DNS

1 **Connectez-vous au serveur DNS principal ou secondaire en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Modifiez le fichier de zone DNS adéquat en ajoutant les enregistrements AAAA pour chaque nœud compatible IPv6 :**

host-name `IN AAAA` *host-address*

3 **Modifiez les fichiers de zone inversée DNS et ajoutez des enregistrements PTR :**

host-address `IN PTR` *hostname*

Pour obtenir des informations détaillées sur l'administration de DNS, reportez-vous à la section *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Exemple 7–15 Fichier de zone inversée DNS

Cet exemple représente une adresse IPv6 dans le fichier de zone inversée.

```
$ORIGIN    ip6.int.
8.2.5.0.2.1.e.f.f.f.9.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.0.0.2.0.0.0 \
    IN        PTR        vallejo.Eng.apex.COM.
```

Ajout d'adresses IPv6 au service de noms NIS

Dans Solaris 10 11/06 et les versions antérieures, deux cartes ont été ajoutées au service de noms NIS : `ipnodes.byname` et `ipnodes.byaddr`. Ces cartes contiennent des noms d'hôtes IPv4 et IPv6 ainsi que des associations d'adresses. Les outils compatibles IPv6 utilisent les cartes NIS `ipnodes.` Les cartes `hosts.byname` et `hosts.byaddr` ne contiennent que les noms d'hôtes IPv4 et des associations d'adresses. Ces cartes ne sont pas modifiées. Ainsi, elles peuvent être utilisées pour les applications existantes. L'administration des cartes `ipnodes` est similaire à celle des cartes `hosts.byname` et `hosts.byaddr.` Pour Solaris 10 11/06, lors de la mise à jour des cartes *hosts* avec des adresses IPv4, mettez les cartes *ipnode* à jour avec les mêmes informations.

Remarque – Les versions suivantes d'Oracle Solaris 10 n'utilisent pas les cartes `ipnodes`. La fonctionnalité IPv6 des cartes `ipnodes` est à présent maintenue dans les cartes `hosts`.

Pour obtenir des instructions sur l'administration de cartes NIS, reportez-vous au Chapitre 5, “Paramétrage et configuration du service NIS” du *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

▼ Procédure d'affichage des informations relatives au service d'attribution de noms IPv6

La commande `nslookup` permet d'afficher des informations relatives au service d'attribution de noms IPv6.

1 **Après vous être connecté à l'aide de votre compte utilisateur, exécutez la commande `nslookup`.**

```
% /usr/sbin/nslookup
```

Le nom et l'adresse par défaut du serveur s'affichent, suivis du crochet d'invite de la commande `nslookup`.

2 **Pour obtenir des informations sur un hôte en particulier, saisissez les commandes suivantes à partir du crochet d'invite :**

```
>set q=any
>host-name
```

3. **Saisissez la commande suivante afin d'afficher les enregistrements AAAA :**

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

4. **Quittez la commande `nslookup` en saisissant `exit`.**

Exemple 7–16 Utilisation de `nslookup` pour l'affichage d'informations IPv6

Cet exemple illustre les résultats de l'exécution de `nslookup` dans un environnement de réseau 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
```

▼ Procédure de vérification de la mise à jour correcte des enregistrements PTR DNS IPv6

Dans cette procédure, utilisez la commande `nslookup` afin d'afficher les enregistrements PTR pour le service DNS IPv6.

1. **Une fois connecté à votre compte utilisateur, exécutez la commande `nslookup`.**

   ```
   % /usr/sbin/nslookup
   ```

   Le nom et l'adresse par défaut du serveur s'affichent, suivis du crochet d'invite de la commande `nslookup`.

2. **Saisissez ce qui suit devant le crochet d'invite afin de visualiser les enregistrements PTR :**

   ```
   >set q=PTR
   ```

3. **Quittez la commande en saisissant `exit`.**

Exemple 7–17 Utilisation de `nslookup` pour l'affichage d'enregistrements PTR

L'exemple suivant illustre l'affichage d'enregistrements PTR à l'aide de la commande `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.0.6.5.2.9.0.0.0.0.0.0.0.0.2.0.0.0.ip6.int

8.2.5.0.2.1.e.f.f.f.0.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.0.0.2.0.0.0.ip6.int name =
vallejo.ipv6.Eng.apex.COM
ip6.int nameserver = space1999.Eng.apex.COM
> exit
```

▼ Procédure d'affichage d'informations IPv6 à l'aide de NIS

Dans cette procédure, la commande `ypmatch` permet d'afficher des informations IPv6 par le biais de NIS :

- **Une fois connecté à votre compte utilisateur, saisissez ce qui suit afin d'afficher les adresses IPv6 dans NIS :**

  `% ypmatch` *hostname* `hosts ipnodes.`*byname*

  Les informations sur l'hôte *hostname* spécifié s'affichent.

Remarque – Les versions suivantes d'Oracle Solaris 11/06 ne contiennent plus les cartes `ipnodes`. La maintenance de la fonctionnalité IPv6 de `ipnodes` s'effectue à présent dans les cartes `hosts`.

Exemple 7–18 Sortie d'adresses IPv6 de la commande `ypmatch`

Dans le cas de Solaris 10 11/06 et versions antérieures, l'exemple suivant illustre les résultas d'une opération de `ypmatch` sur la base de données `ipnodes.byname`.

```
% ypmatch farhost hosts ipnodes.byname
2001:0db8:3c4d:15:a00:20ff:fe12:5286       farhost
```

▼ Procédure d'application d'informations IPv6 indépendantes du service d'attribution de noms

Cette procédure s'utilise uniquement pour Solaris 10 11/06 et les versions antérieures. Pour les versions ultérieures, vous pouvez effectuer la même opération sur la base de données `hosts`.

- **Une fois connecté à votre compte utilisateur, saisissez la commande suivante :**

  `% getent ipnodes` *hostname*

  Les informations sur l'hôte *nom-hôte* s'affichent.

Exemple 7–19 Affichage d'informations IPv6 dans la base de données `ipnodes`

L'exemple suivant illustre la sortie de la commande `getent` :

```
% getent ipnodes vallejo

2001:0db8:8512:2:56:a00:fe87:9aba    myhost myhost
fe80::56:a00:fe87:9aba     myhost myhost
```

◆ ◆ ◆ CHAPITRE 8

Gestion d'un réseau TCP/IP (tâches)

Ce chapitre présente les tâches permettant d'administrer un réseau TCP/IP. Il aborde les sujets suivants :

Remarque – Pour en savoir plus sur le contrôle des interfaces réseau, reportez-vous à la section "Contrôle de la configuration de l'interface avec la commande `ifconfig`" à la page 209.

L'exécution des tâches présentées dans ce chapitre nécessite l'installation d'un réseau TCP/IP opérationnel sur votre site (IPv4 uniquement ou IPv4/IPv6 double pile). Pour plus d'informations sur l'implémentation d'un réseau IPv6, reportez-vous aux chapitres suivants :

- Pour planifier une implémentation IPv6, reportez-vous au Chapitre 4, "Planification d'un réseau IPv6 (tâches)".
- Pour configurer un réseau IPv6 et créer un environnement double pile, reportez-vous au Chapitre 7, "Configuration d'un réseau IPv6 (tâches)".

Principales tâches d'administration TCP/IP (liste des tâches)

Le tableau suivant répertorie les autres tâches permettant de gérer le réseau après la configuration initiale, notamment l'affichage des informations réseau. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Référence
Affichage des informations de configuration d'une interface.	Déterminez la configuration actuelle des différentes interfaces du système.	"Méthode d'obtention d'informations sur une interface spécifique" à la page 209
Affichage des assignations d'adresses d'interface.	Déterminez les assignations d'adresse de toutes les interfaces du système local.	"Procédure d'affichage des assignations d'adresses de l'interface" à la page 211
Affichage des statistiques par protocole.	Contrôlez les performances des protocoles réseau sur un système donné.	"Affichage des statistiques par protocole" à la page 213
Affichage du statut du réseau.	Contrôlez le système en affichant tous les sockets et toutes les entrées de table de routage. La sortie inclut la famille d'adresses inet pour les réseaux IPv4 et la famille d'adresses inet6 pour les réseaux IPv6.	"Affichage du statut des sockets" à la page 216
Affichage du statut des interfaces réseau.	Contrôlez les performances des interfaces réseau, notamment afin de dépanner les transmissions de données.	"Affichage du statut de l'interface réseau" à la page 216
Affichage du statut de transmission des paquets.	Contrôlez le statut des paquets lors de leur transmission sur le réseau câblé.	"Affichage du statut des transmissions de paquets associés à un type d'adresse spécifique" à la page 218
Contrôle de l'affichage des sorties de commandes IPv6.	Contrôlez la sortie des commandes `ping`, `netstat`, `ifconfig` et `traceroute`. Créez un fichier intitulé `inet_type`. Définissez la variable `DEFAULT_IP` de ce fichier.	"Contrôle de la sortie d'affichage des commandes IP" à la page 221
Contrôle du trafic réseau.	Affichez tous les paquets IP à l'aide de la commande `snoop`.	"Contrôle du trafic réseau IPv6" à la page 229
Affichage de toutes les routes connues par les routeurs du réseau.	Affichez toutes les routes à l'aide de la commande `traceroute`.	"Affichage du suivi de toutes les routes" à la page 225

Contrôle de la configuration de l'interface avec la commande ifconfig

La commande ifconfig vous permet d'assigner des adresses IP à des interfaces et de configurer des paramètres d'interface manuellement. De plus, les scripts de démarrage Oracle Solaris exécutent la commande ifconfig pour configurer des pseudo-interfaces, telles que des points d'extrémité de tunnels 6to4.

Ce manuel décrit les nombreuses tâches qui s'accomplissent avec les diverses options de la commande ifconfig. Pour de plus amples informations sur cette commande, ses options et ses variables, reportez-vous à la page de manuel ifconfig(1M) La commande ifconfig possède la syntaxe de base suivante :

ifconfig *interface [famille protocole]*

Méthode d'obtention d'informations sur une interface spécifique

La commande ifconfig permet de déterminer les informations de base relatives aux interfaces d'un système particulier. Par exemple, une simple requête ifconfig peut indiquer les informations suivantes :

- noms des périphériques de toutes les interfaces d'un système ;
- toutes les adresses IPv4 et IPv6 (le cas échéant) assignées aux interfaces ;
- statut de configuration de ces interfaces.

La procédure suivante décrit la façon dont la commande ifconfig doit être utilisée pour fournir des informations de configuration de base sur les interfaces d'un système.

1. **Sur l'hôte local, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Récupérez les informations sur l'interface qui vous intéresse.**

   # ifconfig *interface*

   La commande ifconfig affiche la sortie suivante :

   - Ligne relative au statut

La première ligne de la sortie de la commande `ifconfig` indique le nom de l'interface ainsi que le statut qui lui est actuellement associé (par le biais d'un indicateur). Sur cette ligne figurent également l'unité de transmission maximale configurable sur l'interface ainsi qu'un numéro d'index. La ligne relative au statut vous permet de connaître l'état actuel de l'interface.

- Ligne d'informations sur l'adresse IP

  La deuxième ligne de la sortie de la commande `ifconfig` inclut l'adresse IPv4 ou IPv6 configurée sur l'interface. S'il s'agit d'une adresse IPv4, cette ligne indique également le masque de réseau configuré et l'adresse de diffusion.

- Ligne relative à l'adresse MAC

  Lorsque vous exécutez la commande `ifconfig` en tant que superutilisateur ou avec un rôle similaire, la sortie contient une troisième ligne. Si une adresse IPv4 est configurée, cette ligne indique l'adresse MAC (adresse de couche Ethernet) assignée à l'interface. S'il s'agit d'une adresse IPv6, cette troisième ligne contient l'adresse locale du lien que le démon IPv6 `in.ndpd` génère à partir de l'adresse MAC.

Exemple 8–1 Obtention d'informations de base sur l'interface avec la commande `ifconfig`

L'exemple suivant décrit la syntaxe de la commande `ifconfig` à rédiger pour obtenir des informations sur l'interface `eri` configurée sur un hôte particulier.

```
# ifconfig eri
eri0: flags=863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 1
      inet 10.0.0.112 netmask ffffff80 broadcast 10.8.48.127
      ether 8:0:20:b9:4c:54
```

Le tableau suivant décrit les informations de la variable de la requête de la commande `ifconfig` et comprend également la description de la variable qui peut s'afficher à l'écran et le type d'informations fournies. Il se base sur l'exemple de sortie précédent.

Variable	Sortie écran	Description
Nom de l'interface	`eri0`	Indique le nom du périphérique de l'interface dont le statut a été requis par la commande `ifconfig`.
Statut de l'interface	`flags=863<UP`	Indique le statut de l'interface et spécifie notamment les indicateurs actuellement associés à celle-ci. Cette information vous permet de savoir si l'interface est initialisée (`UP`) ou non (`DOWN`).
Statut de la diffusion	`BROADCAST`	Indique si l'interface prend en charge les diffusions sur IPv4.
Etat de transmission	`RUNNING`	Indique si le système transmet actuellement des paquets via l'interface.

Variable	Sortie écran	Description
Statut de la multidiffusion	`MULTICAST, IPv4`	Indique si l'interface prend en charge les transmissions multidiffusions. Dans cet exemple, l'interface prend en charge les transmissions multidiffusions IPv4.
Unité de transmission maximale	`mtu 1500`	Indique que la taille de transfert maximale de cette interface est de 1 500 octets.
Adresse IP	`inet 10.0.0.112`	Indique l'adresse IPv4 ou IPv6 assignée à l'interface. Dans cet exemple, l'interface `eri0` possède l'adresse IPv4 `10.0.0.112`.
Masque de réseau	`netmask ffffff80`	Indique le masque de réseau IPv4 de l'interface. Notez que les adresses IPv6 n'utilisent pas de masques de réseau.
Adresse MAC	`ether 8:0:20:b9:4c:54`	Indique l'adresse de couche Ethernet de l'interface.

▼ Procédure d'affichage des assignations d'adresses de l'interface

Les routeurs et hôtes multiréseaux possèdent plusieurs interfaces auxquelles sont souvent assignées plus d'une adresse IP. La commande `ifconfig` vous permet dans ce cas d'afficher toutes les adresses assignées aux interfaces d'un système. Elle peut n'indiquer que les assignations d'adresses IPv4 ou IPv6. Pour afficher également les adresses MAC des interfaces, vous devez d'abord vous connecter en tant que superutilisateur ou assumer un rôle similaire.

Pour de plus amples informations sur la commande `ifconfig`, reportez-vous à la page de manuel `ifconfig(1M)`.

1 Sur le système local, connectez-vous en tant qu'administrateur réseau ou superutilisateur.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour de plus amples informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Récupérez les informations sur toutes les interfaces.

Vous pouvez exécuter la commande `ifconfig -a` pour obtenir les informations suivantes :

- adresses de toutes les interfaces du système ;

  ```
  # ifconfig -a
  ```

- toutes les adresses IPv4 assignées aux interfaces du système ;

  ```
  # ifconfig -a4
  ```

- toutes les adresses IPv6 assignées aux interfaces du système, à condition que celui-ci soit compatible avec IPv6.

```
ifconfig -a6
```

Exemple 8–2 Affichage des informations sur les adresses de toutes les interfaces

L'exemple suivant correspond à un hôte ne possédant qu'une interface du réseau principal nommée `qfe0`. La sortie de la commande `ifconfig` indique néanmoins que trois formes d'adresses sont actuellement assignées à `qfe0` : loopback (`lo0`), IPv4 (`inet`) et IPv6 (`inet6`). Dans la section de la sortie relative à IPv6, la ligne de l'interface `qfe0` indique une adresse IPv6 locale du lien. La seconde adresse de `qfe0` figure sur la ligne `qfe0:1`.

```
% ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
qfe0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.112 netmask ffffff80 broadcast 10.0.0.127
        ether 8:0:20:b9:4c:54
lo0: flags=2000849 <UP,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 8:0:20:b9:4c:54
        inet6 fe80::a00:20ff:feb9:4c54/10
qfe0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
        inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64
```

Exemple 8–3 Affichage des informations sur les adresses de toutes les interfaces IPv4

Dans l'exemple suivant, l'adresse IPv4 est configurée pour un hôte multiréseau. Pour exécuter ce type de commande `ifconfig`, vous devez vous connecter en tant que superutilisateur.

```
% ifconfig -a4
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
qfe0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.112 netmask ffffff80 broadcast 10.0.0.127
        ether 8:0:20:b9:4c:54
qfe1: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 10.0.0.118 netmask ffffff80 broadcast 10.0.0.127
        ether 8:0:20:6f:5e:17
```

Exemple 8–4 Affichage des informations sur les adresses de toutes les interfaces IPv6

Cet exemple n'indique que les adresses IPv6 configurée pour un hôte particulier. Pour exécuter ce type de commande `ifconfig`, vous devez vous connecter en tant que superutilisateur.

```
% ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        ether 8:0:20:b9:4c:54
        inet6 fe80::a00:20ff:feb9:4c54/10
qfe0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
        inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64
```

Cet exemple de sortie `ifconfig` indique les trois types d'adresse IPv6 assignés à une seule interface d'un hôte :

`lo0`
: Adresse de loopback IPv6.

`inet6 fe80::a00:20ff:feb9:4c54/10`
: Adresse locale du lien assignée à l'interface du réseau principal.

`inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64`
: Adresse IPv6 (y compris le préfixe de sous-réseau). Le terme `ADDRCONF` qui figure dans la sortie indique que cette adresse a été automatiquement configurée par l'hôte.

Contrôle du statut du réseau à l'aide de la commande `netstat`

La commande `netstat` génère des affichages illustrant le statut du réseau ainsi que les statistiques des protocoles. Vous pouvez afficher le statut des points d'extrémité TCP, SCTP et UDP sous forme de table. Vous pouvez également afficher les informations de table de routage ainsi que les informations d'interface.

La commande `netstat` permet d'afficher différents types d'informations sur le réseau, suivant l'option de ligne de commande sélectionnée. Les affichages obtenus constituent la principale référence pour l'administration du système. L'exemple ci-dessous illustre la syntaxe de base de la commande `netstat` :

`netstat` [`-m`] [`-n`] [`-s`] [`-i` | `-r`] [`-f` *famille-adresses*]

Cette section décrit les options fréquemment utilisées avec la commande `netstat`. Pour obtenir une description détaillée des toutes les options `netstat`, reportez-vous à la page de manuel `netstat(1M)`.

▼ Affichage des statistiques par protocole

L'option `-s` de la commande `netstat` permet d'afficher les statistiques des protocoles UDP, TCP, SCTP, ICMP et IP.

Remarque – Vous pouvez obtenir la sortie de la commande `netstat` à l'aide du compte utilisateur Oracle Solaris.

- **Affichez le statut du protocole.**

```
$ netstat -s
```

Exemple 8–5 Statistiques des protocoles réseau

L'exemple suivant illustre la sortie de la commande `netstat -s`. Certaines parties de la sortie ont été tronquées. La sortie peut signaler les opérations ayant généré des problèmes pour les différents protocoles. Par exemple, les statistiques affichées pour ICMPv4 et ICMPv6 peuvent signaler les opérations ayant généré des erreurs pour le protocole ICMP.

```
RAWIP
        rawipInDatagrams    =  4701     rawipInErrors       =     0
        rawipInCksumErrs    =     0     rawipOutDatagrams   =     4
        rawipOutErrors      =     0

UDP
        udpInDatagrams      = 10091     udpInErrors         =     0
        udpOutDatagrams     = 15772     udpOutErrors        =     0

TCP     tcpRtoAlgorithm     =     4     tcpRtoMin           =   400
        tcpRtoMax           = 60000     tcpMaxConn          =    -1
        .
        .
        tcpListenDrop       =     0     tcpListenDropQ0     =     0
        tcpHalfOpenDrop     =     0     tcpOutSackRetrans   =     0

IPv4    ipForwarding        =     2     ipDefaultTTL        =   255
        ipInReceives        =300182     ipInHdrErrors       =     0
        ipInAddrErrors      =     0     ipInCksumErrs       =     0
        .
        .
        ipsecInFailed       =     0     ipInIPv6            =     0
        ipOutIPv6           =     3     ipOutSwitchIPv6     =     0

IPv6    ipv6Forwarding      =     2     ipv6DefaultHopLimit =   255
        ipv6InReceives      = 13986     ipv6InHdrErrors     =     0
        ipv6InTooBigErrors  =     0     ipv6InNoRoutes      =     0
        .
        .
        rawipInOverflows    =     0     ipv6InIPv4          =     0

       ipv6OutIPv4         =     0     ipv6OutSwitchIPv4   =     0

ICMPv4  icmpInMsgs          = 43593     icmpInErrors        =     0
        icmpInCksumErrs     =     0     icmpInUnknowns      =     0
        .
        .
        icmpInOverflows     =     0

ICMPv6  icmp6InMsgs         = 13612     icmp6InErrors       =     0
        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
```

▼ Affichage du statut des protocoles de transport

La commande `netstat` permet d'afficher le statut des protocoles de transport. Pour plus d'informations, reportez-vous à la page de manuel `netstat(1M)`.

1 Affichez le statut des protocoles de transport TCP et SCTP sur un système.

```
$ netstat
```

2 Affichez le statut d'un protocole de transport donné sur un système.

```
$ netstat -P transport-protocol
```

La variable *protocole-transport* peut être définie sur les valeurs suivantes : `tcp`, `sctp` ou `udp`.

Exemple 8–6 Affichage du statut des protocoles de transport TCP et SCTP

L'exemple ci-dessous illustre la sortie de base de la commande `netstat`. Les informations contenues dans la sortie se rapportent uniquement à 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
```

Exemple 8–7 Affichage du statut d'un protocole de transport donné

L'exemple ci-dessous illustre le résultat obtenu suite à l'exécution de la commande `netstat` avec l'option `-P`.

```
$ 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
```

▼ Affichage du statut de l'interface réseau

L'option `i` de la commande `netstat` illustre le statut des interfaces réseau configurées sur le système local. Cette option permet de déterminer le nombre de paquets transmis et reçus sur un système sur les différents réseaux.

- **Affichez le statut des interfaces sur le réseau.**

```
$ netstat -i
```

Exemple 8–8 Affichage du statut d'interface réseau

L'exemple suivant illustre le statut du flux de paquets IPv4 et IPv6 sur les interfaces de l'hôte.

Par exemple, le nombre de paquets entrants (`Ipkts`) affiché pour un serveur peut augmenter à chaque tentative de démarrage d'un client alors que le nombre de paquets sortants (`Opkts`) reste inchangé. Ce résultat suggère que le serveur détecte les paquets de requête de démarrage envoyés par le client, mais qu'il ne parvient pas à formuler la réponse appropriée. Cette erreur peut être liée à la spécification d'une adresse incorrecte dans la base de données `hosts`, `ipnodes` ou `ethers`.

En revanche, si le nombre de paquets entrants reste inchangé sur la durée, l'ordinateur ne détecte même pas l'envoi des paquets. Ce résultat suggère un autre type d'erreur, vraisemblablement lié à un problème d'ordre matériel.

```
Name  Mtu  Net/Dest      Address        Ipkts  Ierrs Opkts  Oerrs Collis Queue
lo0   8232 loopback      localhost      142    0     142    0     0      0
hme0  1500 host58        host58        1106302 0     52419  0     0      0

Name  Mtu  Net/Dest      Address                   Ipkts  Ierrs Opkts  Oerrs Collis
lo0   8252 localhost     localhost                  142    0     142    0     0
hme0  1500 fe80::a00:20ff:feb9:4c54/10 fe80::a00:20ff:feb9:4c54 1106305 0 52422 0  0
```

▼ Affichage du statut des sockets

L'option `-a` de la commande `netstat` permet d'afficher le statut des sockets sur l'hôte local.

- **Pour afficher le statut des sockets et des entrées de table de routage, saisissez la commande suivante :**

  L'exécution de cette option de la commande `netstat` peut s'effectuer à l'aide du compte utilisateur.

  ```
  % netstat -a
  ```

Exemple 8–9 Affichage de l'ensemble des sockets et des entrées de table de routage

La sortie de la commande `netstat -a` contient de nombreuses statistiques. L'exemple ci-dessous illustre certaines parties d'une sortie classique de la commande `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
```

▼ Affichage du statut des transmissions de paquets associés à un type d'adresse spécifique

L'option `-f` de la commande `netstat` permet d'afficher les statistiques relatives aux transmissions de paquets associées à une famille d'adresses donnée.

- **Affichez les statistiques relatives aux transmissions de paquets IPv4 ou IPv6.**

  `$ netstat -f` *inet* | *inet6*

  Pour afficher les informations relatives aux transmissions IPv4, définissez l'argument `inet` pour la commande `netstat -f`. Pour afficher les informations relatives aux transmissions IPv6, définissez l'argument `inet6` pour la commande `netstat -f`.

Exemple 8–10 Statut de transmission de paquets IPv4

L'exemple suivant illustre la sortie de la commande `netstat - f inet`.

```
TCP: IPv4
   Local Address        Remote Address    Swind Send-Q Rwind Recv-Q  State
-------------------- -------------------- ----- ------ ----- ------ -------
host58.734         host19.nfsd       49640      0 49640      0 ESTABLISHED
host58.38063       host19.32782      49640      0 49640      0 CLOSE_WAIT
host58.38146       host41.43601      49640      0 49640      0 ESTABLISHED
host58.996         remote-host.login 49640      0 49206      0 ESTABLISHED
```

Exemple 8–11 Statut de transmission de paquets IPv6

L'exemple suivant illustre la sortie de la commande `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    ESTABLISHED
localhost.32792        localhost.38065       49152   0 49152      0    ESTABLISHED
localhost.38089        localhost.38057       49152   0 49152      0    ESTABLISHED
```

▼ Affichage du statut des routes connues

L'option `-r` de la commande `netstat` permet d'afficher la table de routage de l'hôte local. Cette table représente le statut de toutes les routes connues de l'hôte. L'exécution de cette option de la commande `netstat` peut s'effectuer à l'aide du compte utilisateur.

- **Affichez la table de routage IP.**

```
$ netstat -r
```

Exemple 8–12 Sortie de table de routage obtenue à l'aide de la commande `netstat`

L'exemple suivant illustre la sortie de la commande `netstat -r`.

```
Routing Table: IPv4
  Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
host15               myhost               U         1  31059  hme0
10.0.0.14            myhost               U         1      0  hme0
default              distantrouter        UG        1      2  hme0
localhost            localhost            UH        42019361  lo0

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 hme0:1
fe80::/10                fe80::1a2b:3c4d:5e6f:12a2    U       1     23 hme0
ff00::/8                 fe80::1a2b:3c4d:5e6f:12a2    U       1      0 hme0
default                  fe80::1a2b:3c4d:5e6f:12a2    UG      1      0 hme0
localhost                localhost                    UH      9  21832 lo0
```

Le tableau suivant décrit les différents paramètres de la sortie à l'écran de la commande `netstat –r`.

Paramètre	Description
`Destination` `Destination/Mask`	Spécifie l'hôte correspondant au point d'extrémité de destination de la route. Dans la table de routage IPv6, le point d'extrémité de destination est représenté par un préfixe de point d'extrémité de tunnel 6to4 (`2002:0a00:3010:2::/64`).
`Gateway`	Spécifie la passerelle de transmission des paquets.
`Flags`	Indique le statut actuel de la route. L'indicateur `U` signifie que la route fonctionne. L'indicateur `G` signifie que la route mène à une passerelle.
`Use`	Affiche le nombre de paquets envoyés.

Paramètre	Description
Interface	Indique l'interface de l'hôte local correspondant au point d'extrémité source de la transmission.

Test des hôtes distants à l'aide de la commande ping

La commande ping permet de déterminer le statut d'un hôte distant. Lors de l'exécution de la commande ping, le protocole ICMP envoie un datagramme à l'hôte spécifié et attend la réponse. Le protocole ICMP permet de gérer les erreurs se produisant sur les réseaux TCP/IP. L'exécution de la commande ping permet de déterminer l'existence d'une connexion IP pour l'hôte distant spécifié.

L'exemple suivant illustre la syntaxe de base de la commande ping :

/usr/sbin/ping *hôte [délai]*

Dans cette syntaxe, la variable *hôte* correspond au nom de l'hôte distant. L'argument *délai* indique la durée en secondes pendant laquelle la commande ping tente de contacter l'hôte distant. La valeur par défaut est de 20 secondes. Pour plus d'informations sur la syntaxe et les options de la commande, reportez-vous à la page de manuel ping(1M)

▼ Vérification de l'exécution d'un hôte distant

- **Tapez la commande ping suivante :**

  $ **ping** *hostname*

  Si l'hôte *nom-hôte* accepte les transmissions ICMP, le message suivant s'affiche :

  hostname is alive

  Ce message indique que *nom-hôte* a répondu à la requête ICMP. En revanche, si *nom-hôte* ne fonctionne pas ou ne reçoit pas les paquets ICMP, la commande ping génère la réponse suivante :

  no answer from *hostname*

▼ Détection de l'abandon de paquets sur un hôte

L'option -s de la commande ping permet de vérifier qu'un hôte distant est en cours d'exécution et de détecter toute perte de paquet sur cet hôte.

- **Tapez la commande ping suivante :**

  $ **ping -s** *hostname*

Exemple 8–13 Sortie de la commande `ping` permettant la détection de l'abandon de paquet

La commande `ping -s` *nom-hôte* envoie des paquets en continu à l'hôte spécifié pendant un laps de temps donné ou jusqu'à l'envoi d'un caractère d'interruption. Les réponses affichées sont comparables à celles de l'écran suivant :

```
& 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 statistique de perte de paquet indique si l'hôte a abandonné des paquets. Si la commande `ping` échoue, vérifiez le statut du réseau indiqué dans les sorties des commandes `ifconfig` et `netstat`. Reportez-vous aux sections "Contrôle de la configuration de l'interface avec la commande `ifconfig`" à la page 209 et "Contrôle du statut du réseau à l'aide de la commande `netstat`" à la page 213.

Administration et journalisation des affichages de statut du réseau

Les tâches suivantes illustrent les procédures de vérification du statut du réseau à l'aide de commandes de réseau standard.

▼ Contrôle de la sortie d'affichage des commandes IP

Vous pouvez définir la sortie des commandes `netstat` et `ifconfig` de manière à afficher uniquement les informations IPv4 ou à afficher les informations IPv4 et IPv6.

1. **Créez le fichier `/etc/default/inet_type`.**

2. **Ajoutez l'une des entrées suivantes au fichier `/etc/default/inet_type` :**

   - Pour afficher uniquement les informations IPv4 :

     ```
     DEFAULT_IP=IP_VERSION4
     ```

   - Pour afficher les informations IPv4 et IPv6 :

```
DEFAULT_IP=BOTH
```

Ou

```
DEFAULT_IP=IP_VERSION6
```

Pour plus d'informations sur le fichier `inet_type`, reportez-vous à la page de manuel `inet_type(4)`.

Remarque – Les indicateurs `-4` et `-6` de la commande `ifconfig` ont priorité sur les valeurs définies dans le fichier `inet_type`. L'indicateur `-f` de la commande `netstat` a également priorité sur les valeurs définies dans le fichier `inet_type`.

Exemple 8–14 Contrôle de la sortie pour la sélection des informations IPv4 et IPv6

- Si vous spécifiez la variable `DEFAULT_IP=BOTH` ou la variable `DEFAULT_IP=IP_VERSION6` dans le fichier `inet_type`, la sortie suivante s'affiche :

```
% ifconfig -a
lo0: flags=1000849 mtu 8232 index 1
        inet 10.10.0.1 netmask ff000000
qfe0: flags=1000843 mtu 1500 index 2
        inet 10.46.86.54 netmask ffffff00 broadcast 10.46.86.255
        ether 8:0:20:56:a8
lo0: flags=2000849 mtu 8252 index 1
        inet6 ::1/128
qfe0: flags=2000841 mtu 1500 index 2
        ether 8:0:20:56:a8
        inet6 fe80::a00:fe73:56a8/10
qfe0:1: flags=2080841 mtu 1500 index 2
        inet6 2001:db8:3c4d:5:a00:fe73:56a8/64
```

- Si vous spécifiez la variable `DEFAULT_IP=IP_VERSION4` dans le fichier `inet_type`, la sortie suivante s'affiche :

```
% ifconfig -a
lo0: flags=849 mtu 8232
        inet 10.10.0.1 netmask ff000000
qfe0: flags=843 mtu 1500
        inet 10.46.86.54 netmask ffffff00 broadcast 10.46.86.255
        ether 8:0:20:56:a8
```

▼ Journalisation des actions du démon de routage IPv4

Si vous pensez que le démon de routage IPv4 `routed` ne fonctionne pas correctement, vous pouvez créer un journal permettant d'effectuer le suivi de l'activité correspondante. Le journal inclut tous les transferts de paquets à compter du démarrage du démon `routed`.

1. **Sur l'hôte local, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Créez un fichier journal permettant d'effectuer le suivi des opérations du démon :**

   ```
   # /usr/sbin/in.routed /var/log-file-name
   ```

Attention – Sur les réseaux à forte activité, la sortie de cette commande peut être générée sur une base quasi continue.

Exemple 8–15 Journal réseau du démon `in.routed`

L'exemple suivant illustre le début du journal créé à l'aide de la procédure “Journalisation des actions du démon de routage IPv4” à la page 222.

```
-- 2003/11/18 16:47:00.000000 --
Tracing actions started
RCVBUF=61440
Add interface lo0  #1   127.0.0.1      -->127.0.0.1/32
   <UP|LOOPBACK|RUNNING|MULTICAST|IPv4> <PASSIVE>
Add interface hme0 #2   10.10.48.112    -->10.10.48.0/25
    <UP|BROADCAST|RUNNING|MULTICAST|IPv4>
turn on RIP
Add    10.0.0.0        -->10.10.48.112      metric=0  hme0  <NET_SYN>
Add    10.10.48.85/25  -->10.10.48.112      metric=0  hme0  <IF|NOPROP>
```

▼ Suivi des activités du démon de détection des voisins IPv6

Si vous pensez que le démon IPv6 `in.ndpd` ne fonctionne pas correctement, vous pouvez générer le suivi de l'activité correspondante. Le suivi s'affiche sur la sortie standard jusqu'à l'arrêt du processus. Il inclut tous les transferts de paquets à compter du démarrage du démon `in.ndpd`.

1. **Connectez-vous au nœud IPv6 local en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Générez le suivi du démon `in.ndpd`.**

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

3 Pour arrêter le processus de suivi, appuyez sur les touches Ctrl-C.

Exemple 8–16 Suivi de l'activité du démon `in.ndpd`

La sortie suivante illustre le début du suivi du démon `in.ndpd`.

```
# /usr/lib/inet/in.ndpd -t
Nov 18 17:27:28 Sending solicitation to  ff02::2 (16 bytes) on hme0
Nov 18 17:27:28         Source LLA: len 6 <08:00:20:b9:4c:54>
Nov 18 17:27:28 Received valid advert from fe80::a00:20ff:fee9:2d27 (88 bytes) on hme0
Nov 18 17:27:28         Max hop limit: 0
Nov 18 17:27:28         Managed address configuration: Not set
Nov 18 17:27:28         Other configuration flag: Not set
Nov 18 17:27:28         Router lifetime: 1800
Nov 18 17:27:28         Reachable timer: 0
Nov 18 17:27:28         Reachable retrans timer: 0
Nov 18 17:27:28         Source LLA: len 6 <08:00:20:e9:2d:27>
Nov 18 17:27:28         Prefix: 2001:08db:3c4d:1::/64
Nov 18 17:27:28                 On link flag:Set
Nov 18 17:27:28                 Auto addrconf flag:Set
Nov 18 17:27:28                 Valid time: 2592000
Nov 18 17:27:28                 Preferred time: 604800
Nov 18 17:27:28         Prefix: 2002:0a00:3010:2::/64
Nov 18 17:27:28                 On link flag:Set
Nov 18 17:27:28                 Auto addrconf flag:Set
Nov 18 17:27:28                 Valid time: 2592000
Nov 18 17:27:28                 Preferred time: 604800
```

Affichage des informations de routage à l'aide de la commande `traceroute`

La commande `traceroute` permet d'obtenir le suivi de la route empruntée par un paquet IP pour accéder à un système distant. Pour plus d'informations sur la commande `traceroute`, reportez-vous à la page de manuel `traceroute(1M)`.

La commande `traceroute` permet de détecter les erreurs de configuration de routage et les échecs de chemin de routage. Si un hôte est inaccessible, la commande `traceroute` permet d'afficher le chemin suivi par les paquets afin de détecter les emplacements susceptibles d'être à l'origine de l'échec.

La commande `traceroute` affiche également le délai d'aller-retour de chaque passerelle sur le chemin d'accès à l'hôte cible. Ces informations permettent notamment de déterminer l'emplacement des ralentissements de trafic entre les deux hôtes.

▼ Détermination de la route menant à un hôte distant

- **Pour déterminer la route menant à un hôte distant, exécutez la commande suivante :**

  `% traceroute` *destination-hostname*

L'exécution de cette forme de la commande traceroute peut s'effectuer à l'aide du compte utilisateur.

Exemple 8–17 Affichage de la route menant à un hôte distant à l'aide de la commande traceroute

La sortie suivante de la commande traceroute affiche le chemin à sept sauts suivi par les paquets pour circuler du système local nearhost vers le système distant farhost. La sortie illustre également le temps nécessaire à un paquet pour traverser les différents sauts.

```
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
```

▼ Affichage du suivi de toutes les routes

Cette procédure permet d'afficher le suivi de toutes les routes à l'aide de l'option -a de la commande traceroute.

- **Exécutez la commande suivante sur le système local :**

  % **traceroute -a***host-name*

  L'exécution de cette forme de la commande traceroute peut s'effectuer à l'aide du compte utilisateur.

Exemple 8–18 Affichage du suivi de toutes les routes menant à un hôte double pile

L'exemple ci-dessous illustre toutes les routes possibles pour accéder à un hôte double pile.

```
% 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 *
```

Contrôle du transfert des paquets à l'aide de la commande snoop

La commande snoop permet de contrôler le statut des transferts de données. La commande snoop permet de capturer les paquets réseau et d'afficher leur contenu au format spécifié. Les paquets peuvent être affichés dès leur réception ou dès l'enregistrement dans un fichier. L'écriture des données dans un fichier intermédiaire par la commande snoop permet de réduire la probabilité de perte de paquet liée à l'activité de suivi. Le fichier est alors également interprété par la commande snoop.

Pour capturer des paquets en provenance et à destination de l'interface par défaut en mode promiscuité, vous devez vous connecter en tant qu'administrateur réseau ou superutilisateur. Dans sa forme contractée, la commande snoop affiche uniquement les données en rapport avec le protocole principal. Par exemple, un paquet NFS affiche uniquement les informations NFS. Les informations RPC, UDP, IP et Ethernet sont supprimées, mais vous pouvez y accéder en sélectionnant l'une des options détaillées de la commande.

L'exécution répétée à intervalles fréquents de la commande snoop permet d'identifier les comportements normaux du système. Pour obtenir de l'aide sur l'analyse des paquets, consultez les livres blancs et documents RFC récents et demandez conseil aux experts dans les domaines concernés (par exemple, NFS ou NIS). Pour plus d'informations sur l'utilisation de la commande snoop et des options associées, reportez-vous à la page de manuel snoop(1M)

▼ Vérification des paquets en provenance de toutes les interfaces

1. **Sur l'hôte local, connectez-vous en tant qu'administrateur réseau ou superutilisateur.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Imprimez les informations sur les interfaces connectées au système.**

   ```
   # ifconfig -a
   ```

   La commande snoop utilise normalement le premier périphérique non-loopback (en principe, l'interface réseau principale).

3. **Commencez la capture des paquets en exécutant la commande snoop sans argument, comme illustré dans l'Exemple 8–19.**

4. **Pour arrêter le processus, appuyez sur les touches Ctrl-C.**

Exemple 8–19 Sortie de la commande snoop

La commande snoop standard renvoie une sortie comparable à l'écran suivant (pour un hôte double pile).

```
% snoop
Using device /dev/hme (promiscuous mode)
router5.local.com -> router5.local.com ARP R 10.0.0.13, router5.local.com is
    0:10:7b:31:37:80
router5.local.com -> BROADCAST     TFTP Read "network-confg" (octet)
farhost.remote.com -> myhost       RLOGIN C port=993
myhost ->   nisserve2          NIS C MATCH 10.0.0.64 in ipnodes.byaddr
nisserve2 ->    myhost             NIS R MATCH No such key
blue-112 -> slave-253-2        NIS C MATCH 10.0.0.112 in ipnodes.byaddr
myhost -> DNSserver.local.com      DNS C 192.168.10.10.in-addr.arpa. Internet PTR ?
DNSserver.local.com  myhost        DNS R 192.168.10.10.in-addr.arpa. Internet PTR
   niserve2.
.
.
.
fe80::a00:20ff:febb:e09 -> ff02::9 RIPng R (5 destinations)
```

Les paquets capturés dans cette sortie comprennent une section de connexion à distance, qui contient des requêtes vers les serveurs NIS et DNS pour la résolution d'adresse. Ils comprennent également des paquets ARP périodiques en provenance du routeur local et des publications de l'adresse IPv6 lien-local sur `in.ripngd`.

▼ Capture de la sortie de la commande snoop dans un fichier

1 Sur l'hôte local, connectez-vous en tant qu'administrateur réseau ou superutilisateur.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Capturez une session de commande snoop dans un fichier.

```
# snoop -o filename
```

Exemple :

```
# snoop -o /tmp/cap
Using device /dev/eri (promiscuous mode)
30 snoop: 30 packets captured
```

Dans cet exemple, 30 paquets sont capturés dans le fichier `/tmp/cap`. Ce fichier peut se trouver dans tout répertoire contenant suffisamment d'espace disque. Le nombre de paquets capturés s'affiche sur la ligne de commande. Vous pouvez dès lors appuyez sur les touches Ctrl-C à tout moment pour arrêter le processus.

La commande snoop génère une charge réseau conséquente, ce qui risque de fausser légèrement les résultats. Pour garantir la précision des résultats, exécutez la commande snoop à partir d'un système tiers.

3 **Consultez le fichier de capture de sortie de la commande snoop.**

```
# snoop -i filename
```

Exemple 8–20 Contenu du fichier de capture de sortie de la commande snoop

La sortie suivante illustre diverses captures susceptibles d'être obtenues suite à l'exécution de la commande snoop -i.

```
# snoop -i /tmp/cap
1   0.00000 fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fecd: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
```

▼ Vérification des paquets transmis entre un client et un serveur IPv4

1 **Définissez un système snoop à partir d'un hub connecté soit au serveur soit au client.**

Le système tiers (système snoop) vérifie tous les types de trafic entre les deux ordinateurs. Le suivi obtenu grâce à la commande snoop reflète donc le transfert réel de données.

2 **Sur le système snoop, connectez-vous en tant qu'administrateur réseau ou superutilisateur.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 **Exécutez la commande snoop associée aux options appropriées, puis enregistrez la sortie dans un fichier.**

4 **Consultez et interprétez la sortie.**

Reportez-vous au document RFC 1761, Snoop Version 2 Packet Capture File Format (http://www.ietf.org/rfc/rfc1761.txt?number=1761) pour plus d'informations sur le fichier de capture snoop.

▼ Contrôle du trafic réseau IPv6

La commande `snoop` permet d'afficher les paquets IPv6 uniquement.

1 **Sur le nœud local, connectez-vous en tant qu'administrateur réseau ou superutilisateur.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Capturez les paquets IPv6.**

```
# snoop ip6
```

Pour plus d'informations sur la commande `snoop`, reportez-vous à la page de manuel `snoop`(1M).

Exemple 8–21 Affichage du trafic réseau IPv6 uniquement

L'exemple suivant illustre la sortie standard susceptible d'être obtenue suite à l'exécution de la commande `snoop ip6` sur un nœud.

```
# snoop ip6
fe80::a00:20ff:fecd:4374 -> ff02::1:ffe9:2d27 ICMPv6 Neighbor solicitation
fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fecd:4375 ICMPv6 Neighbor
      solicitation
fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fecd:4375 ICMPv6 Neighbor
      solicitation
fe80::a00:20ff:febb:e09 -> ff02::9      RIPng R (11 destinations)
fe80::a00:20ff:fee9:2d27 -> ff02::1:ffcd:4375 ICMPv6 Neighbor solicitation
```

Administration de la sélection des adresses par défaut

Oracle Solaris permet à une interface unique de disposer de plusieurs adresses IP. Par exemple, certaines fonctionnalités telles que la fonctionnalité IPMP (multiacheminement sur réseau IP) permettent la connexion de plusieurs cartes d'interface réseau (NIC, network interface card) sur la même couche de liaison IP. Cette liaison peut être associée à une ou plusieurs adresses IP. Les interfaces des systèmes IPv6 possèdent également une adresse IPv6 lien-local, au moins une adresse de routage IPv6 ainsi qu'une adresse IPv4 pour au moins une interface.

Lorsque le système génère une transaction, une application envoie un appel vers le socket `getaddrinfo`. `getaddrinfo` détecte les adresses susceptibles d'être utilisées sur le système de destination. Le noyau établit alors l'ordre de priorité de cette liste afin de déterminer la destination appropriée pour le paquet. Ce processus est appelé *classement des adresses de destination*. Le noyau Oracle Solaris sélectionne le format approprié pour l'adresse source en fonction de l'adresse de destination déterminée pour le paquet. Ce processus est appelé *sélection des adresses*. Pour plus d'informations sur le classement des adresses de destination, reportez-vous à la page de manuel `getaddrinfo`(3SOCKET).

Le processus de sélection des adresses par défaut doit s'effectuer sur les systèmes IPv4 uniquement ainsi que sur les systèmes double pile IPv4/IPv6. Dans la plupart des cas, il n'est pas nécessaire de modifier les mécanismes de sélection des adresses par défaut. Toutefois, vous devrez peut-être modifier l'ordre de priorité des formats d'adresse de manière à prendre en charge la fonctionnalité IPMP ou à préférer les formats d'adresse 6to4, par exemple.

▼ Administration de la table des règles de sélection d'adresses IPv6

La section ci-dessous décrit la procédure de modification de la table des règles de sélection d'adresses. Pour plus d'informations concernant la sélection des adresses IPv6 par défaut, reportez-vous à la section "Commande `ipaddrsel`" à la page 273.

Attention – La table des règles de sélection d'adresses IPv6 doit uniquement être modifiée sur la base des motifs décrits dans la tâche suivante. Les erreurs de définition de la table des règles risquent d'entraîner des problèmes de fonctionnement du réseau. Veillez à enregistrer une copie de sauvegarde de la table des règles, comme indiqué à la procédure suivante.

1 Connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Consultez la table de stratégie de sélection d'adresse IPv6 actuelle.

```
# ipaddrsel
# Prefix                 Precedence Label
::1/128                          50 Loopback
::/0                             40 Default
2002::/16                        30 6to4
::/96                            20 IPv4_Compatible
::ffff:0.0.0.0/96                10 IPv4
```

3 Effectuez une copie de la table des règles de sélection d'adresses par défaut.

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

4 Apportez les modifications souhaitées au fichier `/etc/inet/ipaddrsel.conf` dans un éditeur de texte.

Utilisez la syntaxe suivante pour les entrées de fichier `/etc/inet/ipaddrsel` :

prefix/prefix-length precedence label [# comment]

Les exemples ci-dessous illustrent les modifications susceptibles d'être apportées le plus souvent à la table des règles :

- Définition des adresses 6to4 sur la priorité la plus élevée :

```
2002::/16                       50 6to4
::1/128                         45 Loopback
```

  Le format d'adresse 6to4 dispose dorénavant de la plus haute priorité (50). Loopback, qui disposait auparavant d'une priorité de 50, dispose dorénavant d'une priorité de 45. Les autres formats d'adresse restent inchangés.

- Définition d'une adresse source spécifique pour les communications avec une adresse de destination donnée :

```
::1/128                         50 Loopback
2001:1111:1111::1/128           40 ClientNet
2001:2222:2222::/48             40 ClientNet
::/0                            40 Default
```

  Ce type de configuration s'utilise notamment pour les hôtes associés à une seule interface physique. Dans cet exemple, l'adresse source `2001:1111:1111::1/128` est définie en tant qu'adresse prioritaire pour les paquets adressés aux destinations du réseau `2001:2222:2222::/48`. L'adresse source `2001:1111:1111::1/128` est associée à la priorité 40, priorité supérieure à celle des autres formats d'adresse configurés pour l'interface.

- Préférence des adresses IPv4 par rapport aux adresses IPv6 :

```
::ffff:0.0.0.0/96               60 IPv4
::1/128                         50 Loopback
.
.
```

  La priorité par défaut du format IPv4 `::ffff:0.0.0.0/96` passe de 10 à 60, soit la priorité la plus élevée de la table.

5 Chargez la table de règles modifiée dans le noyau.

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

6 Si la table des règles modifiée génère des erreurs, restaurez la table des règles de sélection des adresses IPv6 par défaut.

```
# ipaddrsel -d
```

▼ Modification de la table des règles de sélection des adresses IPv6 pour la session en cours uniquement

Les modifications apportées au fichier `/etc/inet/ipaddrsel.conf` sont conservées lors des sessions suivantes. Si vous souhaitez modifier la table des règles uniquement pour la session en cours, effectuez la procédure suivante.

1. **Connectez-vous en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Copiez le contenu du fichier `/etc/inet/ipaddrsel` dans le fichier *nom-fichier*, où *nom-fichier* désigne le nom de votre choix.**

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

3. **Apportez les modifications souhaitées à la table des règles dans le fichier *nom-fichier*.**

4. **Chargez la table de règles modifiée dans le noyau.**

   ```
   # ipaddrsel -f filename
   ```

   Le noyau utilise la nouvelle table des règles jusqu'au prochain redémarrage du système.

◆ ◆ ◆ CHAPITRE 9

Dépannage des problèmes de réseau (tâches)

Ce chapitre apporte des solutions aux problèmes se produisant couramment sur les réseaux. Il aborde les sujets suivants :

Nouveaux dépannages de problèmes de réseau

Dans Solaris 10 7/07, le fichier `/etc/inet/ipnodes` devient obsolète. Comme expliqué dans chaque procédure, utilisez le chemin `/etc/inet/ipnodes` uniquement pour les versions précédentes d'Oracle Solaris 10.

Conseils d'ordre général pour le dépannage réseau

La non-communication entre des hôtes d'un réseau constitue l'un des signes annonciateurs d'un problème de réseau. S'il est impossible de communiquer avec un hôte qui vient d'être ajouté au réseau, le problème provient probablement des fichiers de configuration. La carte d'interface réseau peut également être en cause. En effet, si un seul hôte pose problème, la carte d'interface réseau est peut-être défectueuse. Si plusieurs hôtes du réseau peuvent communiquer entre eux, mais pas avec d'autres réseaux, le routeur ou un autre réseau peut être à l'origine du problème.

La commande `ifconfig` vous permet d'obtenir des informations sur les interfaces réseau. Exécutez la commande `netstat` pour afficher les tables de routage et les statistiques de protocoles. Les programmes tiers de diagnostic de réseau fournissent divers outils de dépannage. Pour plus d'informations, reportez-vous à la documentation de ces produits.

D'autres causes moins évidentes peuvent réduire les performances du réseau. Par exemple, l'outil `ping` permet de quantifier des problèmes tels que la perte de paquets par un hôte.

Réalisation de diagnostics de base

Pour résoudre un problème de réseau, vous pouvez réaliser un certain nombre de vérifications logicielles et dépanner les problèmes élémentaires liés aux logiciels.

▼ Vérification logicielle de base sur un réseau

1. **Sur le système local, connectez-vous en tant qu'administrateur réseau ou superutilisateur.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Pour obtenir des informations sur le réseau, exécutez la commande `netstat`.**

   Pour obtenir de plus amples informations sur la commande `netstat` et sur sa syntaxe, reportez-vous à la section "Contrôle du statut du réseau à l'aide de la commande `netstat`" à la page 213 ainsi qu'à la page de manuel `netstat(1M)`.

3. **Vérifiez la base de données `hosts` (ainsi que la base de données `ipnodes` si vous exécutez Solaris 10 11/06 ou une version précédente avec IPv6) et assurez-vous que les entrées sont correctes et actuelles.**

   Pour plus d'informations sur la base de données `/etc/inet/hosts`, reportez-vous à la section "Base de données `hosts`" à la page 239 ainsi qu'à la page de manuel `hosts(4)` Pour plus d'informations sur la base de données `/etc/inet/ipnodes`, reportez-vous à la section "Base de données `ipnodes`" à la page 243 ainsi qu'à la page de manuel `ipnodes(4)`.

4. **Si vous exécutez le protocole RARP (Reverse Address Resolution Protocol), vérifiez les adresses Ethernet de la base de données `ethers` et assurez-vous que les entrées sont correctes et actuelles.**

5. **Essayez de vous connecter à l'hôte local au moyen de la commande `telnet`.**

   Pour obtenir de plus amples informations sur la commande `telnet` et sur sa syntaxe, reportez-vous à la page de manuel `telnet(1)`.

6. **Assurez-vous que le démon réseau `inetd` est en cours d'exécution.**

   ```
   # ps -ef | grep inetd
   ```

   La sortie suivante permet de vérifier que le démon `inetd` est en cours d'exécution :

   ```
   root 57 1 0 Apr 04 ? 3:19 /usr/sbin/inetd -s
   ```

7. **Si le protocole IPv6 est activé sur le réseau, assurez-vous que le démon `in.ndpd` est en cours d'exécution :**

   ```
   # ps -ef | grep in.ndpd
   ```

La sortie suivante permet de vérifier que le démon `in.ndpd` est en cours d'exécution :

```
root 123  1 0  Oct 27 ?  0:03 /usr/lib/inet/in.ndpd
```

Problèmes courants lors du déploiement de IPv6

Cette section décrit les problèmes que vous pouvez rencontrer lors du déploiement de IPv6 sur votre site. Pour toute question liée aux tâches de planification réelles, reportez-vous au Chapitre 4, “Planification d'un réseau IPv6 (tâches)”.

Impossible de mettre à niveau un routeur IPv4 vers IPv6

Si votre équipement ne peut pas être mis à niveau, vous devrez vous procurer un équipement compatible avec IPv6. Lisez attentivement la documentation du fabricant afin de connaître les procédures de prise en charge spécifiques à l'équipement.

Certains routeurs IPv4 ne peuvent pas être mis à niveau vers IPv6. Si votre topologie se trouve dans cette situation, raccordez un routeur IPv6 au routeur IPv4. Vous pourrez alors créer un tunnel sur le routeur IPv4 partant du routeur IPv6. Pour une description des tâches de configuration des tunnels, reportez-vous à la section “Tâches de configuration de tunnels pour la prise en charge d'IPv6 (liste des tâches)” à la page 191.

Problèmes survenant après la mise à niveau de services vers IPv6

Vous pouvez rencontrer les problèmes suivants lors de la préparation des services au protocole IPv6 :

- Certaines applications préparées pour IPv6 ne prennent pas en charge IPv6 par défaut. Vous devez activer IPv6 sur ces applications pour que la prise en charge soit effective.
- Des problèmes peuvent survenir sur un serveur exécutant plusieurs types de services (certains ne prenant en charge qu'IPv4, d'autres prenant en charge IPv4 et IPv6). En effet, certains clients nécessitent l'utilisation de ces deux types de services, ce qui peut semer la confusion au niveau du serveur.

Le FAI actuel ne prend pas en charge IPv6

Si vous envisagez de déployer IPv6 sur votre réseau alors que votre FAI actuel ne prend pas en charge l'adressage IPv6, vous pouvez remplacer votre FAI actuel ou opter pour l'un des choix suivants :

- Louer un FAI fournissant au site une seconde ligne dédiée aux communications IPv6. Cette solution est onéreuse.
- Acquérir un *FAI virtuel*. Les FAI virtuels fournissent un accès IPv6 sans connexion physique. La connexion s'effectue de fait par le biais d'un tunnel reliant le FAI virtuel et le site à travers le FAI IPv4.
- Créer un tunnel 6to4 vers d'autres sites IPv6 à travers le FAI actuel. Configurez l'adresse IPv4 enregistrée du routeur 6to4 en tant qu'entité topologique publique de l'adresse IPv6.

Problèmes de sécurité lors de la création d'un tunnel vers un routeur relais 6to4

De par sa nature, un tunnel reliant un routeur 6to4 à un routeur relais 6to4 ne constitue pas une connexion sécurisée. Les problèmes de sécurité suivants sont inhérents à ce type de tunnel :

- Les routeurs relais 6to4 encapsulent et décapsulent des paquets, mais ne vérifient pas leur contenu.
- La mystification d'adresses est l'un des problèmes majeurs des tunnels sur routeurs relais 6to4. En effet, lorsque le routeur 6to4 reçoit des données du trafic entrant, il est incapable de faire correspondre l'adresse IPv4 du routeur relais et l'adresse IPv6 de la source. L'adresse de l'hôte IPv6 peut alors être facilement mystifiée. Il en va de même pour l'adresse du routeur relais 6to4.
- Par défaut, il n'existe aucun mécanisme de validation entre le routeur 6to4 et le routeur relais 6to4. Un routeur 6to4 ne peut donc pas déterminer si le routeur relais 6to4 est digne de confiance ou s'il est légitime. Une relation de confiance doit exister entre la source 6to4 et la destination IPv6 pour que ces deux sites ne s'exposent pas à d'éventuelles attaques.

Tous les problèmes de sécurité inhérents aux routeurs relais 6to4, y compris ceux cités précédemment, sont expliqués dans le brouillon Internet intitulé *Security Considerations for 6to4*. D'une manière générale, n'activez la prise en charge des routeurs relais 6to4 que dans l'un des cas suivants :

- Votre site 6to4 tente de communiquer avec un réseau IPv6 de confiance privé. Par exemple, activez la prise en charge du routeur relais 6to4 sur un réseau universitaire constitué de sites 6to4 isolés et de sites IPv6 natifs.
- Il est essentiel que votre site 6to4 communique avec certains hôtes IPv6 natifs.
- Vous avez implémenté les modèles de vérification et de validation suggérés dans le brouillon Internet intitulé *Security Considerations for 6to4*.

◆ ◆ ◆ CHAPITRE 10

Présentation détaillée de TCP/IP et IPv4 (référence)

Ce chapitre fournit des informations de référence sur les fichiers de configuration réseau pour les réseaux TCP/IP, notamment les types de réseau, leur objectif et le format d'entrée des fichiers. Les bases de données réseau existantes sont également décrites en détails. En outre, ce chapitre explique comment la structure des adresses IPv4 est définie à partir de classifications réseau et de numéros de sous-réseaux.

Le présent chapitre contient les informations suivantes :

Nouveautés de TCP/IP et IPv4 - présentation détaillée

Dans Solaris 10 7/07, le fichier `/etc/inet/ipnodes` devient obsolète. Comme expliqué dans chaque procédure, utilisez le chemin `/etc/inet/ipnodes` uniquement pour les versions précédentes d'Oracle Solaris 10.

Fichiers de configuration TCP/IP

Chaque système du réseau obtient ses informations de configuration TCP/IP des fichiers de configuration TCP/IP et bases de données réseau ci-dessous :

- fichier `/etc/hostname.`*interface* ;
- fichier `/etc/nodename` ;
- fichier `/etc/defaultdomain` ;
- fichier `/etc/defaultrouter` (facultatif) ;
- base de données `hosts` ;

- dans Solaris 10 11/06 et les versions antérieures, base de données `ipnodes` ;
- base de données `netmasks` (facultatif).

Lors de l'installation, le programme d'installation d'Oracle Solaris crée ces fichiers. Vous pouvez également les modifier manuellement, comme indiqué dans cette section. Les bases de données réseau `hosts` et `netmasks` sont lues par les services de noms disponibles sur les réseaux Oracle Solaris. Le concept de base de données réseau est décrit à la section "Bases de données réseau et fichier `nsswitch.conf`" à la page 248 Dans Solaris 10 11/06 et les versions antérieures, pour plus d'informations sur le fichier `ipnodes`, reportez-vous à la section "Base de données `ipnodes`" à la page 243.

Fichier `/etc/hostname.`*interface*

Ce fichier définit les interfaces réseau physique sur l'hôte local. Au moins un fichier `/etc/hostname.`*interface* doit exister sur le système local. Le programme d'installation d'Oracle Solaris crée un fichier `/etc/hostname.`*interface* pour la première interface détectée lors de l'installation. Cette interface possède généralement le plus petit numéro de périphérique, par exemple `eri0`. Elle constitue l'*interface réseau principale*. Si le programme d'installation détecte d'autres interfaces, vous pouvez également les configurer au cours du processus d'installation.

Remarque – Si vous créez d'autres fichiers de nom d'hôte pour la même interface, ces fichiers doivent également suivre le format de nom `hostname.[0-9]*`, par exemple : `hostname.qfe0.a123`. Des noms tels que `hostname.qfe0.bak` ou `hostname.qfe0.old` ne sont pas valides et seront ignorés par les scripts pendant l'initialisation du système.

Une interface ne doit contenir qu'un seul fichier de nom d'hôte correspondant. Si vous créez un autre fichier de nom d'hôte pour une interface avec un nom de fichier valide, tels que `/etc/hostname.qfe` et `/etc/hostname.qfe.a123` , les scripts d'initialisation tenteront de configurer les données en référençant le contenu des deux fichiers de nom d'hôte et cela peut générer des erreurs. Pour éviter ce genre d'erreurs, indiquez un nom de fichier non valide pour le fichier de nom d'hôte à ne pas utiliser dans la configuration.

Si vous ajoutez une interface réseau supplémentaire au système après l'installation, vous devez créer un fichier `/etc/hostname.`*interface* pour cette interface, comme indiqué à la section "Configuration d'une interface physique après l'installation du système" à la page 150. En outre, pour que le logiciel Oracle Solaris reconnaisse et utilise la nouvelle interface réseau, le pilote de périphérique de l'interface doit être chargé dans le répertoire correspondant. Reportez-vous à la documentation accompagnant la nouvelle interface réseau pour obtenir le nom d'*interface* adéquat et les instructions du pilote de périphérique.

Le fichier `/etc/hostname.`*interface* de base contient une entrée : l'adresse IPv4 ou le nom d'hôte associé à l'interface réseau. L'adresse IPv4 peut s'exprimer au format décimal avec points classique ou en notation CIDR. Si l'entrée du fichier `/etc/hostname.`*interface* est un nom d'hôte, celui-ci doit également se trouver dans le fichier `/etc/inet/hosts`.

Par exemple, soit `smc0` l'interface réseau principale d'un système appelé `tenere`. L'entrée du fichier `/etc/hostname.smc0` peut être une adresse IPv4 selon la numérotation décimale avec points ou en notation CIDR, ou le nom d'hôte `tenere`.

Remarque – IPv6 définit les interfaces réseau à l'aide du fichier `/etc/hostname6.`*interface*. Pour plus d'informations, reportez-vous à la section "Fichier de configuration d'interface IPv6" à la page 271.

Fichier `/etc/nodename`

Ce fichier doit contenir une entrée : le nom d'hôte du système local. Par exemple, sur le système `timbuktu`, le fichier `/etc/nodename` contiendrait l'entrée `timbuktu`.

Fichier `/etc/defaultdomain`

Ce fichier doit contenir une entrée : le nom complet du domaine administratif auquel appartient le réseau de l'hôte local. Vous pouvez fournir ce nom au programme d'installation Oracle Solaris ou modifier le fichier plus tard. Pour plus d'informations sur les domaines de réseau, reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Fichier `/etc/defaultrouter`

Ce fichier peut contenir une entrée pour chaque routeur directement connecté au réseau. L'entrée doit correspondre au nom de l'interface réseau servant de routeur entre les réseaux. La présence du fichier `/etc/defaultrouter` indique que le système prend en charge le routage statique.

Base de données `hosts`

La base de données `hosts` contient les adresses IPv4 et noms d'hôtes des systèmes résidant sur le réseau. Si vous utilisez le service de noms NIS ou DNS, ou le service d'annuaire LDAP, la base de données `hosts` est mise à jour dans une base de données conçue pour les informations d'hôte. Par exemple, sur un réseau exécutant NIS, la base de données `hosts` est mise à jour dans le fichier `hostsbyname`.

Si vous utilisez des fichiers locaux en tant que service de noms, la base de données `hosts` est mise à jour dans le fichier `/etc/inet/hosts`. Ce fichier contient les noms d'hôtes et les adresses IPv4 de l'interface réseau principale, des autres interfaces réseau connectées au système et toute autre adresse réseau que le système doit vérifier.

Remarque – Pour assurer la compatibilité avec les systèmes d'exploitation BSD, le fichier `/etc/hosts` définit un lien symbolique vers `/etc/inet/hosts`.

Format de fichier `/etc/inet/hosts`

Le fichier `/etc/inet/hosts` utilise la syntaxe de base ci-dessous. Pour obtenir les informations complètes relatives à cette syntaxe, reportez-vous à la page de manuel `hosts(4)`.

adresse-IPv4 nom-hôte [pseudo] [#commentaire]

adresse-IPv4	Contient l'adresse IPv4 de chaque interface que l'hôte local doit reconnaître.
nom-hôte	Contient le nom d'hôte attribué au système lors de la configuration, ainsi que les noms d'hôtes attribués aux interfaces réseau supplémentaires que l'hôte local doit reconnaître.
[pseudo]	Champ facultatif contenant un pseudo pour l'hôte.
[#commentaire]	Champ de commentaire facultatif.

Fichier `/etc/inet/hosts` initial

Lors de l'exécution du programme d'installation Oracle Solaris sur un système, le programme configure le fichier `/etc/inet/hosts` initial. Ce fichier contient les entrées minimales requises par l'hôte local. Les entrées incluent l'adresse loopback, l'adresse IPv4 de l'hôte et le nom d'hôte.

Par exemple, le programme d'installation Oracle Solaris peut créer le fichier `/etc/inet/hosts` suivant pour le système `tenere` indiqué dans la Figure 5–1 :

EXEMPLE 10–1 Fichier `/etc/inet/hosts` pour système `tenere`

```
127.0.0.1     localhost         loghost    #loopback address
192.168.200.3   tenere                      #host name
```

Adresse loopback

Dans l'Exemple 10–1, l'adresse IPv4 `127.0.0.1` constitue l'*adresse loopback*. L'adresse loopback est l'interface réseau réservée utilisée par le système local pour permettre les communications entre processus. L'hôte utilise cette adresse pour s'envoyer des paquets à lui-même. La commande `ifconfig` utilise l'adresse loopback pour la configuration et les tests, comme expliqué à la section "Contrôle de la configuration de l'interface avec la commande `ifconfig`" à la page 209. Tout système du réseau TCP/IP doit utiliser l'adresse IP `127.0.0.1` pour le loopback IPv4 sur l'hôte local.

Nom de l'hôte

L'adresse IPv4 `192.168.200.1` et le nom `tenere` constituent l'adresse et le nom d'hôte du système local. Ils sont attribués à l'interface réseau principale du système.

Interfaces réseau multiples

Certains systèmes possèdent plusieurs interfaces réseau, car ils constituent des routeurs ou des hôtes multiréseau. Chaque interface réseau connectée au système requiert sa propre adresse IP et le nom associé. À l'installation, vous devez configurer l'interface réseau principale. Si un système présente plusieurs interfaces lors de l'installation, le programme d'installation Oracle Solaris vous invite à configurer également ces interfaces supplémentaires. Vous pouvez configurer les interfaces supplémentaires ou une partie d'entre elles à l'installation, ou les configurer manuellement plus tard.

Une fois l'installation d'Oracle Solaris terminée, vous pouvez configurer des interfaces supplémentaires pour un routeur ou un hôte multiréseau en ajoutant ces informations au fichier `/etc/inet/hosts` du système. Pour de plus amples informations sur la configuration de routeurs et d'hôtes multiréseau, reportez-vous aux sections "Configuration d'un routeur IPv4" à la page 124 et "Configuration des hôtes multiréseaux" à la page 132.

L'Exemple 10–2 présente le fichier `/etc/inet/hosts` du système `timbuktu` illustré sur la Figure 5–1.

EXEMPLE 10–2 Fichier `/etc/inet/hosts` pour le système `timbuktu`

```
127.0.0.1        localhost     loghost
192.168.200.70   timbuktu      #This is the local host name
192.168.201.10   timbuktu-201  #Interface to network 192.9.201
```

Avec ces deux interfaces, `timbuktu` connecte les réseaux `192.168.200` et `192.168.201` en tant que routeur.

Impact des services de noms sur la base de données `hosts`

Les services de noms NIS et DNS, et le service d'annuaire LDAP mettent à jour les adresses et les noms d'hôtes sur un ou plusieurs serveurs. Ces serveurs mettent à jour les bases de données `hosts` contenant les informations de tous les hôtes et routeurs (le cas échéant) du réseau du serveur. Pour de plus amples informations sur ces services, reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Service de nom assuré par les fichiers locaux

Sur un réseau utilisant des fichiers locaux pour le service de noms, les systèmes s'exécutant en mode de fichiers locaux consultent leurs fichiers `/etc/inet/hosts` individuels pour connaître

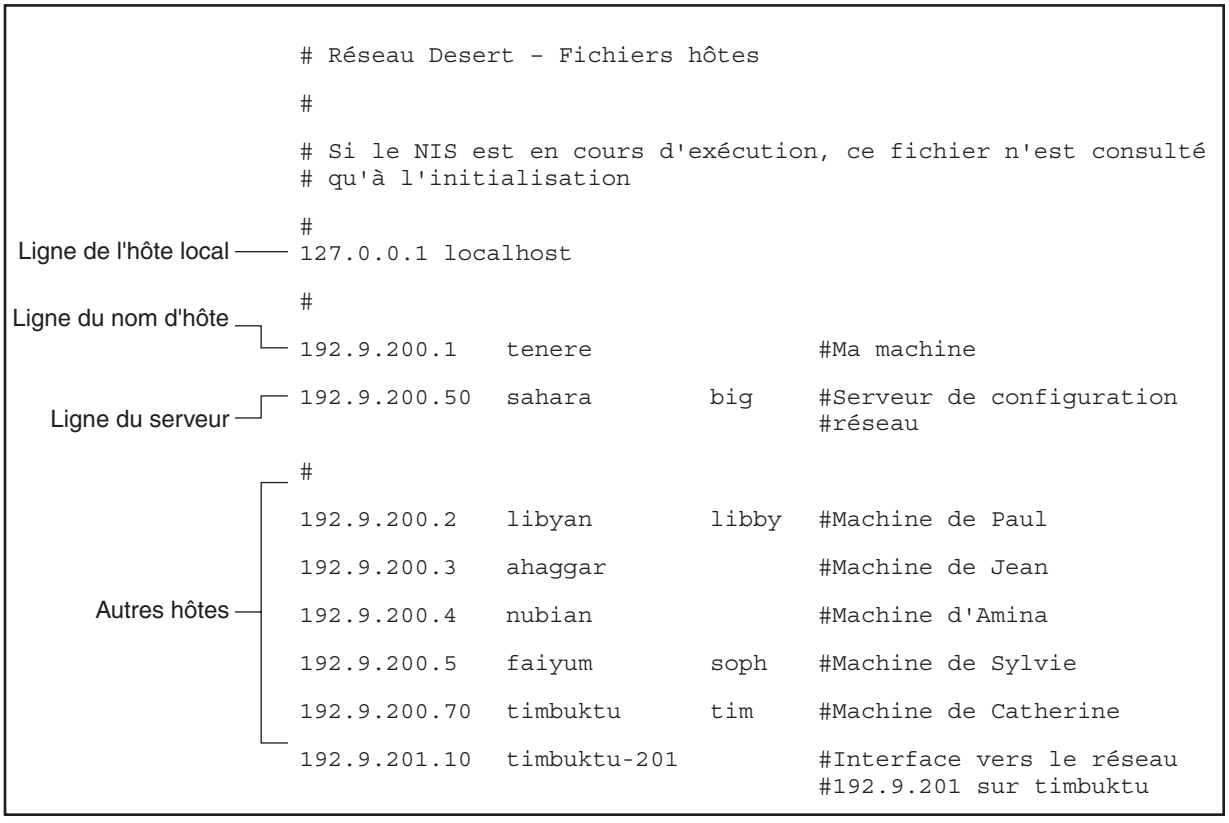
les adresses IPv4 et noms d'hôtes des autres systèmes du réseau. Par conséquent, les fichiers `/etc/inet/hosts` de ces systèmes doivent contenir les informations suivantes :

- adresse loopback ;
- adresse IPv4 et nom d'hôte du système local (interface réseau principale) ;
- adresse IPv4 et nom d'hôte des interfaces réseau supplémentaires connectées à ce système, le cas échéant ;
- adresses IPv4 et noms d'hôtes des hôtes résidant sur le réseau local ;
- adresses IPv4 et noms d'hôtes de tout routeur que ce système doit connaître, le cas échéant ;
- adresse IPv4 de tout système auquel le système doit faire référence via son nom d'hôte.

La Figure 10–1 présente le fichier `/etc/inet/hosts` du système `tenere`. Ce système s'exécute en mode fichiers locaux. Comme vous pouvez le constater, le fichier contient les adresses IPv4 et noms d'hôtes de tous les systèmes du réseau `192.9.200`. Il contient également l'adresse IPv4 et le nom d'interface `timbuktu-201`. Cette interface connecte le réseau `192.9.200` au réseau `192.9.201`.

Un système configuré en tant que client réseau consulte le fichier local `/etc/inet/hosts` pour connaître son adresse loopback et son adresse IPv4.

FIGURE 10–1 Fichier `/etc/inet/hosts` pour un système s'exécutant en mode fichiers locaux




```
# Réseau Desert - Fichiers hôtes
#
# Si le NIS est en cours d'exécution, ce fichier n'est consulté
# qu'à l'initialisation
#
127.0.0.1 localhost
#
192.9.200.1    tenere                  #Ma machine
192.9.200.50   sahara         big      #Serveur de configuration
                                        #réseau
#
192.9.200.2    libyan          libby    #Machine de Paul
192.9.200.3    ahaggar                  #Machine de Jean
192.9.200.4    nubian                   #Machine d'Amina
192.9.200.5    faiyum          soph     #Machine de Sylvie
192.9.200.70   timbuktu        tim      #Machine de Catherine
192.9.201.10   timbuktu-201             #Interface vers le réseau
                                        #192.9.201 sur timbuktu
```

Base de données `ipnodes`

Remarque – La base de données `ipnodes` n'est plus incluse dans les versions supérieures à Solaris 10 11/06. Dans ces versions, les fonctions IPv6 de `ipnodes` migrent vers la base de données `hosts`.

Le fichier `/etc/inet/ipnodes` conserve les adresses IPv4 et IPv6. En outre, vous pouvez enregistrer les adresses IPv4 en numérotation décimale avec points classique ou selon la notation CIDR. Ce fichier sert de base de données locale et associe les noms des hôtes à leurs adresses IPv4 et IPv6. N'enregistrez pas les noms d'hôtes ni leurs adresses dans des fichiers statiques, par exemple `/etc/inet/ipnodes`. Toutefois, à des fins de test, enregistrez les adresses

IPv6 dans un fichier de la même façon que les adresses IPv4 sont enregistrées dans `/etc/inet/hosts`. Le fichier `ipnodes` applique les mêmes conventions de format que le fichier `hosts`. Pour de plus amples informations sur `/etc/inet/hosts`, reportez-vous à la section "Base de données `hosts`" à la page 239. Le fichier `ipnodes` est décrit dans la page de manuel `ipnodes(4)`.

Les applications compatibles IPv6 font appel à la base de données `/etc/inet/ipnodes`. La base de données `/etc/hosts` existante, contenant exclusivement des adresses IPv4, reste identique afin de servir les applications existantes. Si la base de données `ipnodes` n'existe pas, les applications IPv6 font appel à la base de données `hosts` existante.

Remarque – Pour ajouter des adresses IPv4, insérez-les à la fois dans les fichiers `hosts` et `ipnodes`. Insérez les adresses IPv6 dans le fichier `ipnodes` uniquement.

EXEMPLE 10–3 Fichier `/etc/inet/ipnodes`

Groupez les adresses de nom d'hôte selon le nom d'hôte, comme indiqué dans cet exemple.

```
#
# Internet IPv6 host table
# with both IPv4 and IPv6 addresses
#
::1     localhost
2001:db8:3b4c:114:a00:20ff:fe78:f37c   farsite.com farsite farsite-v6
fe80::a00:20ff:fe78:f37c     farsite-11.com farsitell
192.168.85.87                    farsite.com farsite farsite-v4
2001:db8:86c0:32:a00:20ff:fe87:9aba   nearsite.com nearsite nearsite-v6
fe80::a00:20ff:fe87:9aba     nearsite-11.com nearsitell
10.0.0.177                   nearsite.com nearsite nearsite-v4 loghost
```

Base de données `netmasks`

La base de données `netmasks` ne doit être modifiée à la configuration du réseau *que* si vous avez configuré la création de sous-réseaux sur le réseau. La base de données `netmasks` est constituée d'une liste de réseaux et des masques de sous-réseau associés.

Remarque – Lors de la création de sous-réseaux, chaque nouveau réseau doit constituer un réseau physiquement distinct. Vous ne pouvez pas appliquer la création de sous-réseaux à un réseau physique unique.

Qu'est-ce que la création de sous-réseaux ?

La *création de sous-réseaux* permet d'optimiser l'espace d'adressage IPv4 32 bits limité et de réduire la taille des tables de routage d'un interréseau étendu. Quelle que soit la classe d'adresse,

la création de sous-réseaux permet d'allouer une partie de l'espace d'adressage hôte à des adresses réseau, afin d'utiliser des réseaux supplémentaires. La partie de l'espace d'adressage hôte allouée aux nouvelles adresses réseau est appelée *numéro de sous-réseau*.

Outre une utilisation plus efficace de l'espace d'adressage IPv4, la création de sous réseau offre de nombreux avantages administratifs. Le routage peut devenir très compliqué lorsque les réseaux deviennent nombreux. Dans une petite organisation, par exemple, un numéro de classe C peut être attribué à chaque réseau local. Lorsque l'organisation s'étend, l'administration de nombreux numéros de réseau peut devenir complexe. Il s'avère alors judicieux d'allouer quelques numéros de réseau de classe B à chaque grande division de l'organisation. Par exemple, allouez un réseau de classe B au service Ingénierie, un réseau de classe B au service Opérations, etc. Ensuite, vous pouvez diviser chaque réseau de classe B en réseaux supplémentaires, à l'aide des numéros de réseau supplémentaires, obtenus grâce à la création de sous-réseaux. Cette division permet également de réduire le volume d'informations de routage transférées entre les routeurs.

Création du masque de réseau des adresses IPv4

Lors de la création de sous-réseaux, vous devez sélectionner un *masque de réseau* englobant le réseau. Le masque de réseau détermine les bits de l'espace d'adressage hôte qui représentent le numéro de sous-réseau et les bits qui représentent le numéro d'hôte. Pour rappel, l'adresse IPv4 complète est constituée de 32 bits. Selon la classe d'adresse, de 8 à 24 bits sont disponibles pour représenter l'espace d'adressage hôte. Le masque de réseau est spécifié dans la base de données `netmasks`.

Si vous souhaitez utiliser des sous-réseaux, définissez le masque de réseau avant de configurer TCP/IP. Si vous souhaitez installer le système d'exploitation au sein d'une configuration réseau, vous devez indiquer le masque du réseau au programme d'installation Oracle Solaris.

Comme décrit à la section “Conception d'un schéma d'adressage IPv4” à la page 58, les adresses IP 32 bits se décomposent en une partie réseau et une partie hôte. Les 32 bits sont divisés en 4 octets. Chaque octet est attribué au numéro de réseau ou au numéro d'hôte, selon la classe à laquelle appartient le réseau.

Par exemple, dans une adresse IPv4 de classe B, les 2 octets de gauche sont attribués au numéro de réseau, tandis que les 2 octets de droite sont attribués au numéro d'hôte. Dans l'adresse IPv4 de classe B `172.16.10`, vous pouvez attribuer les 2 octets de droite aux hôtes.

Pour implémenter la création de sous-réseaux, vous devez appliquer aux adresses de sous-réseau une partie des bits correspondant aux octets attribués au numéro d'hôte. Par exemple, un espace d'adressage hôte de 16 bits assure l'adressage de 65 534 hôtes. Si vous appliquez le troisième octet aux adresses de sous-réseau et le quatrième octet aux adresses d'hôte, vous pouvez adresser jusqu'à 254 réseaux, contenant chacun 254 hôtes maximum.

Les bits des octets d'adresse hôte appliqués aux adresses de sous-réseau et ceux qui sont appliqués aux adresses d'hôte sont déterminés par un *masque de sous-réseau*. Les masques de sous-réseau permettent de sélectionner des bits à partir de tout octet pour les utiliser en tant qu'adresses de sous-réseau. Les bits de masque de réseau doivent être contigus, mais ils n'ont pas besoin de s'aligner sur les limites d'octet.

Le masque de réseau peut s'appliquer à une adresse IPv4 à l'aide de l'opérateur de bit logique AND. Cette opération permet de sélectionner les positions du numéro de réseau et du numéro de sous-réseau dans l'adresse.

Les masques de réseau peuvent s'exprimer à l'aide de leur représentation binaire. Vous pouvez effectuer la conversion de notation binaire à décimale à l'aide d'une calculatrice. L'exemple suivant présente les formes binaires et décimales du masque de réseau.

Si le masque de réseau `255.255.255.0` est appliqué à l'adresse IPv4 `172.16.41.101`, le résultat est l'adresse IPv4 de `172.16.41.0`.

`172.16.41.101` & `255.255.255.0` = `172.16.41.0`

En notation binaire, l'opération est la suivante :

10000001.10010000.00101001.01100101 (adresse IPv4)

AND

11111111.11111111.11111111.00000000 (masque de réseau)

À présent, le système recherche le numéro de réseau `172.16.41` au lieu du numéro de réseau `172.16`. Si le réseau possède le numéro `172.16.41`, il correspond à ce que le système recherche. Comme vous pouvez attribuer jusqu'à 254 valeurs au troisième octet de l'espace d'adressage IPv4, la création de sous-réseaux permet de créer un espace d'adressage pour 254 réseaux alors que, auparavant, l'espace n'était disponible que pour un réseau.

Si vous fournissez l'espace d'adressage à deux réseaux supplémentaires seulement, vous pouvez utiliser le masque de sous-réseau suivant :

`255.255.192.0`

Le résultat de ce masque de réseau est le suivant :

11111111.11111111.1100000.00000000

Ce résultat laisse encore 14 bits disponibles pour les adresses hôte. Comme tous les 0 et les 1 sont réservés, au moins 2 bits doivent être réservés pour le numéro d'hôte.

Fichier /etc/inet/netmasks

Si le réseau exécute NIS ou LDAP, les serveurs de ces services de noms mettent à jour les bases de données `netmasks`. Pour les réseaux utilisant des fichiers locaux comme service de noms, cette information est enregistrée dans le fichier `/etc/inet/netmasks`.

Remarque – Pour assurer la compatibilité avec les systèmes d'exploitation BSD, le fichier `/etc/netmasks` correspond à un lien symbolique vers `/etc/inet/netmasks`.

L'exemple suivant présente le fichier `/etc/inet/netmasks` d'un réseau de classe B.

EXEMPLE 10–4 Fichier `/etc/inet/netmasks` pour un réseau de classe B

```
# The netmasks file associates Internet Protocol (IPv4) address
# masks with IPv4 network numbers.
#
#     network-number    netmask
#
# Both the network-number and the netmasks are specified in
# “decimal dot” notation, e.g:
#
#        128.32.0.0   255.255.255.0
192.168.0.0  255.255.255.0
```

Si le fichier `/etc/netmasks` n'existe pas, créez-le à l'aide d'un éditeur de texte. Utilisez la syntaxe suivante :

network-number netmask-number

Pour des informations plus détaillées, reportez-vous à la page de manuel `netmasks(4)`.

À la création de numéros de masque de réseau, saisissez le numéro de réseau attribué par le FAI ou l'IR (Internet Registry, registre Internet) (et non le numéro de sous-réseau) et le numéro de masque de réseau dans `/etc/inet/netmasks`. Chaque masque de sous-réseau doit être spécifié sur une ligne distincte.

Exemple :

```
128.78.0.0        255.255.248.0
```

Vous avez également la possibilité de saisir des noms symboliques correspondant aux numéros de réseau dans le fichier `/etc/inet/hosts`. Ensuite, vous pouvez utiliser ces noms de réseau au lieu des numéros de réseau en tant que paramètres de commandes.

Démon de services Internet inetd

Le démon inetd lance les services Internet standard à l'initialisation du système et peut redémarrer un service lorsque le système est en cours d'exécution. Le SMF (Service Management Facility, utilitaire de gestion de service) permet de modifier les services Internet standard et d'indiquer au démon inetd de démarrer d'autres services, le cas échéant.

Exécutez les commandes SMF suivantes pour gérer les services démarrés par inetd :

svcadm — Permet d'effectuer des tâches administratives sur un service, telle que l'activation, la désactivation et le redémarrage. Pour de plus amples informations, reportez-vous à la page de manuel svcadm(1M).

svcs — Permet d'effectuer des requêtes relatives au statut d'un service. Pour de plus amples informations, reportez-vous à la page de manuel svcs(1).

inetadm — Permet d'afficher et modifier les propriétés d'un service. Pour de plus amples informations, reportez-vous à la page de manuel inetadm(1M).

La valeur du champ proto dans le profil inetadm d'un service particulier indique le protocole de couche de transport sur lequel le service s'exécute. Si le service gère exclusivement des requêtes IPv4, le champ proto doit être défini sur tcp, udp ou sctp.

- Pour plus d'informations sur les commandes SMF, reportez-vous aux "Utilitaires d'administration en ligne de commande SMF" du *Guide d'administration système : administration de base*.
- Pour une tâche utilisant les commandes SMF afin d'ajouter un service s'exécutant sur SCTP, reportez-vous à la section "Ajout de services utilisant le protocole SCTP" à la page 141.
- Pour obtenir des informations sur l'ajout de services gérant à la fois des requêtes IPv4 et des requêtes IPv6, reportez-vous à la section "Démon de services Internet inetd" à la page 248

Bases de données réseau et fichier nsswitch.conf

Les bases de données réseau sont des fichiers fournissant des informations requises pour configurer le réseau. Les bases de données réseau sont les suivantes :

- hosts ;
- netmasks ;
- base de données ethers ;
- bootparams ;
- protocols ;
- services ;
- networks.

À la configuration, vous modifiez les bases de données hosts et netmasks, si le réseau se décompose en sous-réseaux. Deux bases de données réseau, bootparams et ethers, permettent de configurer les systèmes en tant que clients réseau. Les autres bases de données sont employées par le système d'exploitation et requièrent rarement des modifications.

Le fichier nsswitch.conf ne constitue pas une base de données réseau, mais vous devez le configurer avec la base de données réseau adéquate. nsswitch.conf spécifie le service de noms à utiliser pour un système particulier : fichiers locaux, NIS, DNS ou LDAP.

Impact des services de noms sur les bases de données réseau

Le format de la base de données réseau dépend du type de service de noms sélectionné pour le réseau. Par exemple, la base de données hosts contient au moins le nom d'hôte et l'adresse IPv4 du système local, ainsi que toute interface réseau directement connectée au système local. Cependant, la base de données hosts peut contenir d'autres adresses IPv4 et noms d'hôtes, selon le type de service de noms utilisé sur le réseau.

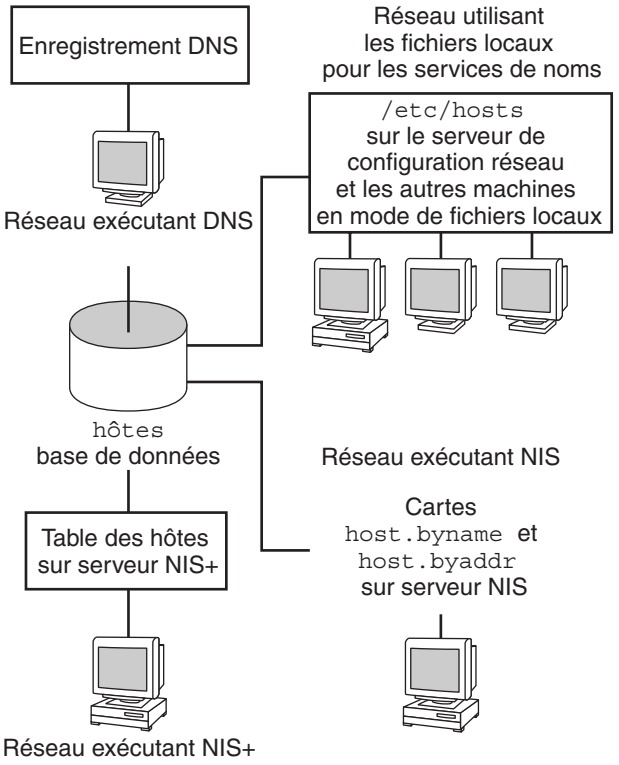
Les bases de données réseau s'utilisent comme suit :

- Les réseaux employant des fichiers locaux comme service de noms se basent sur des fichiers des répertoires /etc/inet et /etc.
- NIS utilise des bases de données appelées cartes NIS.
- DNS utilise les enregistrements avec des informations d'hôte.

Remarque – Les fichiers de données et d'initialisation DNS ne correspondent pas exactement aux bases de données réseau.

La figure ci-dessous présente les différentes formes de base de données hosts utilisées par ces services de noms.

FIGURE 10–2 Formes de base de données hosts utilisées par les services de noms



Le tableau ci-dessous répertorie les bases de données réseau, ainsi que les fichiers locaux et cartes NIS correspondants.

Remarque – La base de données ipnodes a été supprimée des versions Oracle Solaris suivant la version 10 11/06.

TABLEAU 10–1 Bases de données réseau et fichiers de service de noms correspondants

Base de données réseau	Fichiers locaux	Cartes NIS
hosts	/etc/inet/hosts	hosts.byaddr hosts.byname
ipnodes	/etc/inet/ipnodes	ipnodes.byaddr ipnodes.byname
netmasks	/etc/inet/netmasks	netmasks.byaddr
ethers	/etc/ethers	ethers.byname ethers.byaddr
bootparams	/etc/bootparams	bootparams ;

TABLEAU 10–1 Bases de données réseau et fichiers de service de noms correspondants *(Suite)*

Base de données réseau	Fichiers locaux	Cartes NIS
protocols	/etc/inet/protocols	protocols.byname protocols.bynumber
services	/etc/inet/services	services.byname
networks	/etc/inet/réseaux	networks.byaddr networks.byname

Ce manuel décrit les bases de données réseau telles qu'elles sont perçues par les réseaux utilisant des fichiers locaux pour les services de noms.

- Vous trouverez des informations sur la base de données `hosts` à la section "Base de données hosts" à la page 239.
- Vous trouverez des informations sur la base de données `netmasks` à la section "Base de données netmasks" à la page 244.
- Pour Solaris 10 11/06 et les versions antérieures, vous trouverez des informations sur la base de données `ipnodes` à la section "Base de données ipnodes" à la page 243.

Pour de plus amples informations sur les correspondances de bases de données réseau dans NIS, DNS et LDAP, reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Fichier `nsswitch.conf`

Le fichier `/etc/nsswitch.conf` définit l'ordre de recherche des bases de données réseau. Le programme d'installation Oracle Solaris crée un fichier `/etc/nsswitch.conf` par défaut pour le système local, selon le service de noms indiqué lors de l'installation. Si vous avez sélectionné l'option Aucun, en indiquant les fichiers locaux à utiliser pour le service de noms, le fichier `nsswitch.conf` obtenu est similaire à l'exemple ci-dessous.

EXEMPLE 10–5 `nsswitch.conf` pour réseaux utilisant des fichiers pour le service de noms

```
# /etc/nsswitch.files:
#
# An example file that could be copied over to /etc/nsswitch.conf;
# it does not use any naming service.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file contains "switch.so" as a
# nametoaddr library for "inet" transports.

passwd:          files
group:           files
hosts:           files
networks:        files
protocols:       files
rpc:             files
ethers:          files
```

EXEMPLE 10–5 nsswitch.conf pour réseaux utilisant des fichiers pour le service de noms *(Suite)*

```
netmasks:        files
bootparams:      files
publickey:       files
# At present there isn't a 'files' backend for netgroup; the
# system will figure it out pretty quickly,
# and won't use netgroups at all.
netgroup:        files
automount:       files
aliases:         files
services:        files
sendmailvars:    files
```

La page de manuel nsswitch.conf(4) décrit le fichier en détail. La syntaxe de base est la suivante :

base-de-données service-de-noms-à-rechercher

Le champ *base-de-données* indique l'un des divers types de bases de données recherchés par le système d'exploitation. Par exemple, le champ peut spécifier une base de données affectant les utilisateurs, telle que passwd ou aliases, ou une base de données réseau. Le paramètre *nom-de-service-à-rechercher* peut prendre les valeurs files, nis ou nis+ pour les bases de données réseau. La base de données hosts peut également rechercher le service de noms dns. Vous avez également la possibilité de répertorier plusieurs services de noms, par exemple nis+ et files.

Dans l'Exemple 10–5, la seule option de recherche indiquée est files. Par conséquent, outre les informations de base de données réseau, les fichiers résidant dans les répertoires /etc et /etc/inet du système local lui fournissent les informations de sécurité et de montage automatique.

Modification de nsswitch.conf

Le répertoire /etc contient le fichier nsswitch.conf créé par le programme d'installation Oracle Solaris. Ce répertoire contient également des fichiers de modèles pour les services de noms suivants :

- nsswitch.files ;
- nsswitch.nis ;

Pour passer d'un service de noms à un autre, copiez le modèle adéquat dans nsswitch.conf. Vous pouvez également modifier le fichier nsswitch.conf et changer le service de noms par défaut pour rechercher individuellement des bases de données.

Par exemple, sur un réseau exécutant NIS, il peut s'avérer nécessaire de modifier le fichier nsswitch.conf sur les clients du réseau. Le chemin de recherche pour les bases de données bootparams et ethers doit indiquer files comme première option, puis nis. L'exemple suivant présente les chemins de recherche corrects.

EXEMPLE 10–6 nsswitch.conf pour un client d'un réseau exécutant NIS

```
# /etc/nsswitch.conf:#
.
.
passwd:         files nis
group:          files nis

# consult /etc "files" only if nis is down.
hosts:          nis     [NOTFOUND=return] files
networks:       nis     [NOTFOUND=return] files
protocols:      nis     [NOTFOUND=return] files
rpc:            nis     [NOTFOUND=return] files
ethers:         files   [NOTFOUND=return] nis
netmasks:       nis     [NOTFOUND=return] files
bootparams:     files   [NOTFOUND=return] nis
publickey:      nis
netgroup:       nis

automount:      files nis
aliases:        files nis

# for efficient getservbyname() avoid nis
services:       files nis
sendmailvars:   files
```

Pour de plus amples informations sur le basculement entre les services de noms, reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Base de données bootparams

La base de données bootparams contient des informations utilisées par les systèmes configurés pour s'initialiser en mode client réseau. Vous devez modifier cette base de données si le réseau possède des clients réseau. Les procédures sont expliquées à la section "Configuration des clients réseau" à la page 111 La base de données est élaborée à partir des informations saisies dans le fichier /etc/bootparams.

La page de manuel bootparams(4) indique la syntaxe complète de cette base de données. La syntaxe de base est la suivante :

nom-système fichier-clés nom-serveur:chemin

Pour chaque système client du réseau, l'entrée peut contenir les informations suivantes : le nom du client, une liste de clés, les noms des serveurs et des chemins. Le premier élément de chaque entrée est le nom du système client. Tous les autres éléments sont facultatifs. Reportez-vous à l'exemple ci-dessous.

EXEMPLE 10–7 Base de données bootparams

```
myclient   root=myserver : /nfsroot/myclient  \
swap=myserver : /nfsswap//myclient \
dump=myserver : /nfsdump/myclient
```

Dans cet exemple, le terme dump= indique aux hôtes client de ne pas rechercher un fichier de vidage.

Entrée de caractère générique pour bootparams

Dans la plupart des cas, utilisez l'entrée de caractère générique lors de la modification de la base de données bootparams pour prendre en charge les clients. Cette entrée se présente comme suit :

```
*  root=server:/path dump=:
```

L'astérisque (*) indique que cette entrée s'applique à tous les clients non spécifiquement nommés dans la base de données bootparams.

Base de données ethers

La base de données ethers est élaborée à partir d'informations entrées dans le fichier /etc/ethers. Cette base de données associe les noms d'hôtes à leurs adresses MAC (*Media Access Control*, contrôle d'accès média). Ne créez une base de données ethers que si vous exécutez le démon RARP. En d'autres termes, vous devez créer cette base de données si vous configurez des clients réseau.

RARP utilise le fichier pour mapper les adresses MAC aux adresses IP. Si vous exécutez le démon RARP in.rarpd, vous devez configurer le fichier ethers et mettre à jour ce fichier sur tous les hôtes exécutant le démon afin de refléter les modifications réalisées sur le réseau.

La page de manuel ethers(4) indique la syntaxe complète de cette base de données. La syntaxe de base est la suivante :

MAC-address hostname #comment

adresse-MAC	Adresse MAC de l'hôte
nom-hôte	Nom officiel de l'hôte
#commentaire	Toute note que vous souhaitez joindre à une entrée du fichier

Le constructeur de l'équipement fournit l'adresse MAC. Si un système n'affiche pas l'adresse MAC lors de l'initialisation du système, reportez-vous aux manuels du matériel pour obtenir de l'aide.

Lors de l'ajout d'entrées à la base de données ethers, assurez-vous que les noms d'hôtes correspondent aux noms principaux dans la base de données hosts et, pour Solaris 10 11/06 et les versions antérieures, la base de données ipnodes, non les pseudos, comme indiqué ci-dessous.

EXEMPLE 10–8 Entrées de la base de données ethers

```
8:0:20:1:40:16  fayoum
8:0:20:1:40:15  nubian
8:0:20:1:40:7   sahara    # This is a comment
8:0:20:1:40:14  tenere
```

Autres bases de données réseau

Les autres bases de données réseau ont rarement besoin d'être modifiées.

Base de données networks

La base de données networks associe les noms de réseau à des numéros de réseau, afin de permettre à certaines applications d'utiliser et d'afficher les noms au lieu des numéros. La base de données networks se base sur les informations du fichier /etc/inet/réseaux. Ce fichier contient les noms de tous les réseaux auxquels le réseau se connecte via les routeurs.

Le programme d'installation Oracle Solaris configure la base de données networks initiale. Toutefois, si vous ajoutez un réseau à la topologie réseau existante, vous devez mettre à jour cette base de données.

La page de manuel networks(4) contient la syntaxe complète de /etc/inet/networks. Le format de base est le suivant :

network-name network-number nickname(s) #comment

nom-réseau	Nom officiel du réseau
numéro-réseau	Numéro attribué par le FAI ou l'IR (Internet Registry, registre Internet)
pseudo	Tout autre nom appliqué au réseau
#commentaire	Toute note que vous souhaitez joindre à une entrée du fichier

Il est impératif de mettre à jour le fichier networks. Le programme netstat utilise les informations de cette base de données pour générer les tables d'état.

Un exemple de fichier /etc/networks est fourni ci-dessous.

EXEMPLE 10–9 Fichier /etc/networks

```
#ident    "@(#)networks    1.4    92/07/14 SMI"    /* SVr4.0 1.1    */
#
# The networks file associates Internet Protocol (IP) network
# numbers with network names. The format of this file is:
#
#     network-name              network-number              nicnames . . .

# The loopback network is used only for intra-machine communication
```

EXEMPLE 10–9 Fichier /etc/networks *(Suite)*

```
loopback              127

#
# Internet networks
#
arpanet     10       arpa  # Historical
#
# local networks

eng   192.168.9 #engineering
acc   192.168.5 #accounting
prog  192.168.2 #programming
```

Base de données protocols

La base de données protocols répertorie les protocoles TCP/IP installés sur le système et leurs numéros de protocole. Le programme d'installation Oracle Solaris crée automatiquement la base de données. Ce fichier requiert rarement des tâches d'administration.

La page de manuel protocols(4) décrit la syntaxe de cette base de données. Un exemple de fichier /etc/inet/protocols est fourni ci-dessous.

EXEMPLE 10–10 Fichier /etc/inet/protocols

```
#
# Internet (IP) protocols
#
ip    0   IP    # internet protocol, pseudo protocol number
icmp  1   ICMP  # internet control message protocol
tcp   6   TCP   # transmission control protocol
udp  17   UDP   # user datagram protocol
```

Base de données services

La base de données services répertorie les noms des services TCP et UDP, ainsi que leurs numéros de port connus. Cette base de données est employée par les programmes faisant appel aux services réseau. La base de données services est créée automatiquement lors de l'installation d'Oracle Solaris. En général, cette base de données ne requiert aucune tâche d'administration.

Vous trouverez les informations complètes de syntaxe dans la page de manuel services(4) Un extrait de fichier /etc/inet/services classique est fournit ci-dessous.

EXEMPLE 10–11 Fichier `/etc/inet/services`

```
#
# Network services
#
echo      7/udp
echo      7/tcp
echo      7/sctp6
discard   9/udp     sink null
discard   11/tcp
daytime   13/udp
daytime   13/tcp
netstat   15/tcp
ftp-data  20/tcp
ftp       21/tcp
telnet    23/tcp
time      37/tcp    timeserver
time      37/udp    timeserver
name      42/udp    nameserver
whois     43/tcp    nickname
```

Protocoles de routage dans Oracle Solaris

Cette section décrit les protocoles de routage pris en charge par Oracle Solaris 10 : RIP (Routing Information Protocol, protocole d'informations de routage) et RDISC (ICMP Router Discovery, détection de routeur ICMP). RIP et RDISC constituent des protocoles TCP/IP standard. Pour obtenir la liste complète des protocoles de routage disponibles dans Oracle Solaris, reportez-vous au Tableau 5–1 et au Tableau 5–2.

RIP (Routing Information Protocol)

Le protocole RIP est implémenté par le démon de routage `in.routed` qui démarre à l'initialisation du système. Exécuté sur un routeur avec l'option `s`, le démon `in.routed` renseigne la table de routage du noyau en indiquant une route pour chaque réseau accessible et publie l'accessibilité via toutes les interfaces réseau.

Exécuté sur un hôte avec l'option `q`, le démon `in.routed` extrait les informations de routage mais ne publie pas l'accessibilité. Sur les hôtes, vous pouvez extraire les informations de routage de deux façons :

- Ne spécifiez *pas* l'indicateur `S` (S majuscule : mode d'économie d'espace). `in.routed` construit une table de routage complète exactement de la même manière que sur un routeur.
- Spécifiez l'indicateur `S. in.routed` crée une table de routage minimale pour le noyau, contenant une seule route par défaut pour chaque routeur disponible.

Protocole RDISC (ICMP Router Discovery)

Les hôtes utilisent RDISC pour obtenir les informations de routage des autres routeurs. Par conséquent, lorsque les hôtes exécutent RDISC, les routeurs doivent également exécuter un autre protocole, par exemple RIP, afin d'échanger les informations de routeur.

RDISC est implémenté par le démon `in.routed`, qui doit s'exécuter à la fois sur les routeurs et sur les hôtes. Sur les hôtes, `in.routed` utilise RDISC pour détecter les routes par défaut des routeurs qui se publient eux-mêmes via RDISC. Sur les routeurs, `in.routed` utilise RDISC pour publier les routes par défaut des hôtes sur les réseaux directement connectés. Reportez-vous aux pages de manuel `in.routed(1M)` et `gateways(4)`.

Classes de réseau

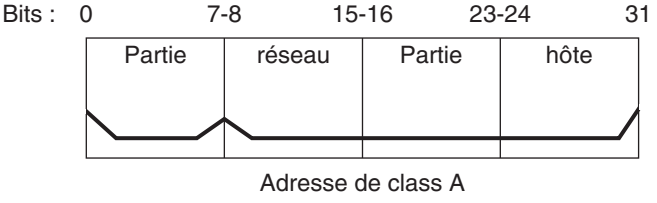
Remarque – Les numéros de réseau basés sur les classes ne sont plus disponibles auprès de l'IANA, mais de nombreux réseaux existants restent basés sur les classes.

Cette section décrit en détail les classes de réseau IPv4. Chaque classe utilise l'espace d'adressage IPv4 32 bits de manière différente, en attribuant un nombre de bits spécifique à la partie réseau de l'adresse. Il existe trois classes : classe A, classe B et classe C.

Numéros de réseau de la classe A

Dans un numéro de réseau de classe A, les 8 premiers bits correspondent à la partie réseau de l'adresse IPv4." Les 24 bits suivants contiennent la partie hôte de l'adresse IPv4, comme illustré sur la figure suivante.

FIGURE 10–3 Allocation des octets dans une adresse de classe A



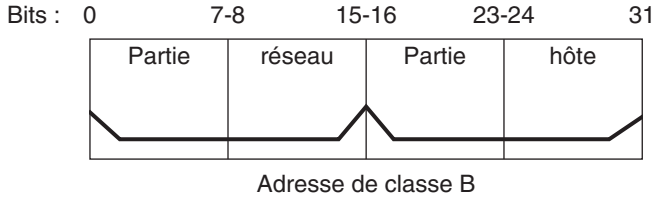
Les valeurs attribuées au premier octet des numéros de réseau de classe A sont définies dans la plage 0–127. Prenons l'exemple de l'adresse IPv4 `75.4.10.4`. La valeur 75 du premier octet

indique que l'hôte se trouve dans un réseau de classe A. Les octets suivants, `4.10.4`, établissent l'adresse de l'hôte. Seul le premier octet d'un numéro de classe A est enregistré auprès de l'IANA. L'utilisation des trois octets suivants est laissée à la discrétion du propriétaire du numéro de réseau. Il existe seulement 127 réseaux de classe A. Chacun de ces numéros peut contenir 16 777 214 hôtes maximum.

Numéros de réseau de la classe B

Dans un numéro de réseau de classe B, les 16 premiers bits correspondent au numéro de réseau et les 16 bits suivants au numéro d'hôte. Le premier octet d'un numéro de réseau de classe B est défini dans la plage 128–191. Dans le numéro `172.16.50.56`, les premiers octets, `172.16`, sont enregistrés auprès de l'IANA et constituent l'adresse réseau. Les deux derniers octets, `50.56`, correspondent à l'adresse hôte. Ils sont attribués à la discrétion du propriétaire du numéro de réseau. La figure suivante illustre une adresse de classe B.

FIGURE 10–4 Allocation des octets dans une adresse de classe B

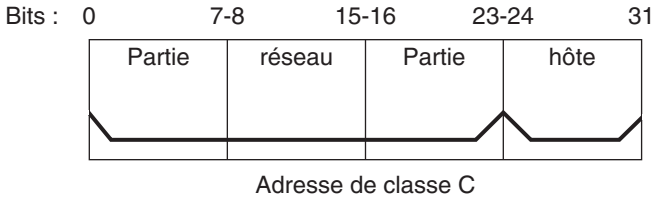


Les adresses de classe B sont souvent attribuées à des organisations dont les réseaux contiennent de nombreux hôtes.

Numéros de réseau de la classe C

Dans un numéro de réseau de classe C, les 24 premiers bits correspondent au numéro de réseau et les 8 bits suivants au numéro d'hôte. Les numéros de réseau de classe C conviennent aux réseaux composés d'un petit nombre d'hôtes n'excédant pas 254. Un numéro de réseau de classe C occupe les trois premiers octets d'une adresse IPv4. Seul le quatrième octet est attribué à la discrétion du propriétaire du réseau. La figure ci-dessous illustre les octets d'une adresse de classe C.

FIGURE 10–5 Allocation des octets dans une adresse de classe C



Le premier octet d'un numéro de réseau de classe C est défini dans la plage 192–223. Les deuxième et troisième octets sont tous les deux compris entre 1 et 255. `192.168.2.5` est un exemple type d'adresse de classe C. Les trois premiers octets, `192.168.2`, constituent le numéro de réseau. Le dernier octet, soit `5` dans cet exemple, correspond au numéro d'hôte.

◆ ◆ ◆ CHAPITRE 11

Présentation détaillée de IPv6 (référence)

Ce chapitre contient des informations de référence concernant l'implémentation du protocole IPv6 sous Oracle Solaris.

Le Chapitre 3, “Présentation d'IPv6” présente IPv6. Les tâches de configuration d'un réseau compatible IPv6 sont décrites au Chapitre 7, “Configuration d'un réseau IPv6 (tâches)”.

Nouveautés du chapitre Présentation détaillée de IPv6

Dans Solaris 10 7/07, le fichier `/etc/inet/ipnodes` devient obsolète. Comme expliqué dans chaque procédure, utilisez le chemin `/etc/inet/ipnodes` uniquement pour les versions précédentes d'Oracle Solaris 10.

Notions approfondies sur les formats d'adressage IPv6

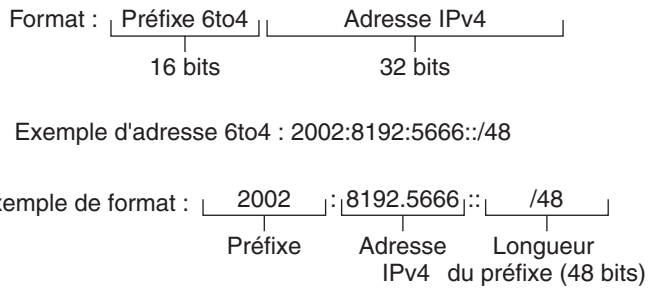
Le Chapitre 3, “Présentation d'IPv6” présente les formats d'adressage IPv6 les plus fréquents : adresse de site unicast et adresse locale de lien. Cette section apporte des informations supplémentaires au Chapitre 3, “Présentation d'IPv6” en décrivant en détail les formats d'adressage suivants :

Adresses 6to4 dérivées

Si vous envisagez de configurer un tunnel 6to4 à partir du point d'extrémité d'un routeur ou d'un hôte, vous devez publier le préfixe du site 6to4 dans le fichier `/etc/inet/ndpd.conf` stocké sur le système du point d'extrémité. Les tâches de configuration des tunnels 6to4 sont présentées à la section “Procédure de configuration d'un tunnel 6to4” à la page 195.

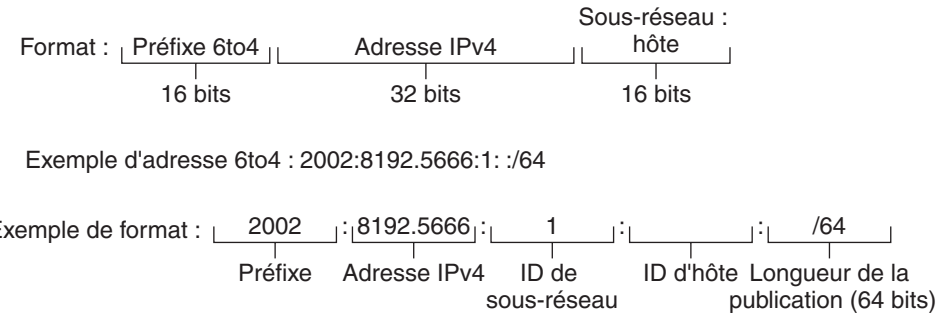
L'illustration suivante présente les éléments d'un préfixe de site 6to4.

FIGURE 11–1 Éléments d'un préfixe de site 6to4



L'illustration suivante présente les éléments d'un préfixe de sous-réseau pour un site 6to4 tel qu'il serait inclus dans le fichier `ndpd.conf`.

FIGURE 11–2 Éléments d'un préfixe de sous-réseau



Le tableau suivant explique les éléments constituant un préfixe de sous-réseau 6to4, les longueurs à respecter et leurs définitions.

Élément	Longueur	Définition
Préfixe	16 bits	Étiquette de préfixe 6to4 2002 (0x2002).
Adresse IPv4	32 bits	Adresse IPv4 unique déjà configurée sur l'interface 6to4. Pour la publication, vous devez spécifier la représentation hexadécimale de l'adresse IPv4 au lieu de celle au format décimal avec points.
ID de sous-réseau	16 bits	ID de sous-réseau unique pour le lien du site 6to4.

Adresses 6to4 dérivées sur un hôte

Lorsqu'un hôte IPv6 reçoit le préfixe 6to4 dérivé par le biais d'une publication de routeur, il reconfigure automatiquement une adresse 6to4 dérivée sur une interface. L'adresse possède le format suivant :

prefix:IPv4-address:subnet-ID:interface-ID/64

La commande `ifconfig -a` sur un hôte avec une interface 6to4 produit la sortie suivante :

```
qfe1:3: flags=2180841<UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6>
 mtu 1500 index 7
        inet6 2002:8192:56bb:9258:a00:20ff:fea9:4521/64
```

Dans cette sortie, l'adresse 6to4 dérivée vient à la suite de `inet6`.

Ce tableau décrit les éléments d'une adresse dérivée d'un préfixe 6to4, les longueurs à respecter et les informations qu'ils contiennent.

Élément de l'adresse	Longueur	Définition
prefix	16 bits	`2002` (préfixe 6to4)
adresse IPv4	32 bits	`8192:56bb` (adresse IPv4 au format hexadécimal pour la pseudointerface 6to4 configurée sur le routeur 6to4)
ID sous-réseau	16 bits	`9258` (adresse du sous-réseau auquel l'hôte appartient)
ID interface	64 bits	`a00:20ff:fea9:4521` (ID de l'interface hôte configurée pour le site 6to4)

Présentation détaillée des adresses IPv6 multicast

L'adresse IPv6 multicast permet de distribuer des informations ou des services identiques à un groupe défini d'interfaces, appelé *groupe multicast*. En règle générale, les interfaces des groupes multicast appartiennent à des nœuds différents. Une interface peut faire partie d'un nombre indéfini de groupes multicast. Les paquets envoyés à l'adresse multicast sont distribués à tous les membres du groupe multicast. Par exemple, l'un des rôles des adresses multicast est de diffuser des informations de façon similaire à l'adresse de diffusion IPv4.

Le tableau suivant décrit le format d'une adresse multicast.

TABLEAU 11–1 Format d'adresse IPv6 multicast

8 bits	4 bits	4 bits	8 bits	8 bits	64 bits	32 bits
`11111111`	*FLGS*	`SCOP`	*Réservé*	*Plen*	*Préfixe réseau*	*ID de groupe*

La liste suivante récapitule le contenu de chaque champ.

- `11111111` – Identifie l'adresse en tant qu'adresse multicast.
- *FLGS* – Jeu des quatre indicateurs 0,0,P,T. Les deux premiers doivent être zéro. Le champ P possède l'une des valeurs suivantes :
  - 0 = adresse multicast qui n'est pas assignée en fonction du préfixe réseau
  - 1 = adresse multicast assignée en fonction du préfixe réseau

  Si P est défini sur 1, T doit être défini sur 1.
- *Réservé* - Valeur nulle réservée.
- *Plen* - Nombre de bits au niveau du préfixe du site qui identifient le sous-réseau, pour une adresse multicast assignée en fonction du préfixe réseau.
- *ID de groupe* - Identificateur du groupe multicast (permanent ou dynamique).

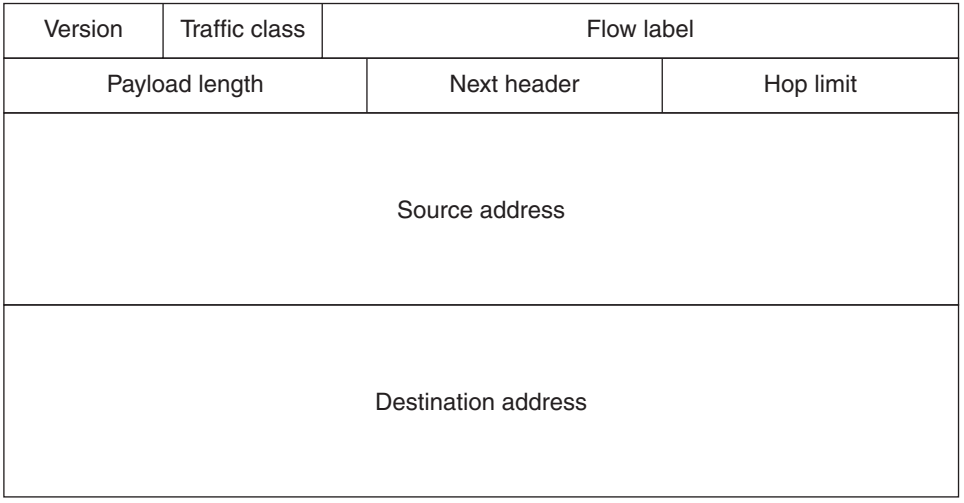
Pour des informations complètes sur le format multicast, reportez-vous au document RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses (`ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt`).

Certaines adresses IPv6 multicast sont assignées de façon permanente par l'IANA (Internet Assigned Numbers Authority). Par exemple, les adresses multicast de tous les nœuds et de tous les routeurs requises par tous les hôtes et routeurs IPv6. Les adresses IPv6 multicast peuvent également être assignées de façon dynamique. Pour plus d'informations sur l'utilisation appropriée des adresses et des groupes multicast, reportez-vous au document RFC 3307, Allocation Guidelines for IPv6 Multicast Addresses.

Format d'en-tête de paquet IPv6

Le protocole IPv6 définit un jeu d'en-têtes comprenant l'en-tête IPv6 de base ainsi que les en-têtes d'extension IPv6. La figure suivante illustre les champs qui s'affichent dans l'en-tête IPv6 et l'ordre dans lequel ils apparaissent.

FIGURE 11–3 Format d'en-tête IPv6 de base



La liste suivante décrit la fonction de chaque champ d'en-tête.

- **Version** – Numéro de version 4 bits du protocole Internet = 6.
- **Traffic class** – Champ de classe de trafic 8 bits.
- **Flow label** – Champ 20 bits.
- **Payload length** – Entier sans signe 16 bits constituant le reste du paquet qui suit l'en-tête IPv6 (en octets).
- **Next header** – Sélecteur 8 bits. Identifie le type d'en-tête qui suit immédiatement l'en-tête IPv6. Utilise la même valeur que le champ du protocole IPv4.

- **Hop limit** – Entier sans signe 8 bits. Décrémentation de 1 par nœud transférant le paquet. Si la valeur du champ est définie sur zéro, le paquet est abandonné.
- **Source address** – 128 bits. L'adresse du premier expéditeur du paquet.
- **Destination address** – 128 bits. L'adresse du destinataire prévu du paquet. Le destinataire prévu n'est pas nécessairement le destinataire s'il existe un en-tête de routage facultatif.

En-têtes d'extension IPv6

Les options IPv6 sont placées dans des en-têtes d'extension distincts situés, dans un paquet, entre l'en-tête IPv6 et l'en-tête de la couche transport. La plupart des en-têtes d'extension IPv6 ne sont vérifiés ou traités par les routeurs qu'au moment où le paquet arrive à sa destination prévue. Cette fonction améliore de façon remarquable les performances du routeur pour les paquets qui contiennent des options. En effet, sous IPv4, toutes les options présentes dans un paquet doivent être vérifiées par le routeur.

À la différence des options IPv4, les en-têtes d'extension IPv6 possèdent une longueur indéfinie. De plus, le nombre d'options pouvant être incluses dans un paquet n'est pas limité à 40 octets. Grâce à cela et à la manière dont les options IPv6 sont généralement traitées, les options IPv6 peuvent servir à des fonctions difficiles d'utilisation dans IPv4.

Pour une meilleure gestion des en-têtes d'option suivants et du protocole de transport qui suit, les options IPv6 sont toujours des entiers avec une longueur multiple de 8 octets. Ce type d'entier permet de conserver l'alignement des en-têtes suivants.

Les en-têtes d'extension IPv6 ci-dessous sont actuellement définis :

- **Routing** – Routage étendu tel que le routage IPv4 à la source lâche
- **Fragmentation** – Fragmentation et réassemblage
- **Authentication** – Intégrité, authentification et sécurité
- **Encapsulating Security Payload** – Confidentialité
- **Hop-by-Hop options** – Options spéciales requérant un traitement saut par saut
- **Destination options** – Informations facultatives devant être vérifiées par le nœud de destination

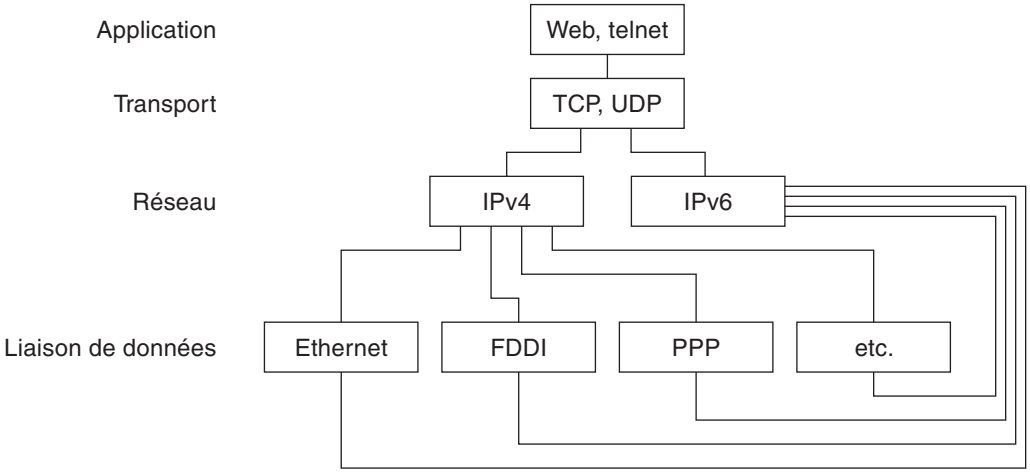
Protocoles doubles piles

Le terme *double pile* désigne la duplication complète de tous les niveaux de la pile de protocole des applications à la couche réseau. Par exemple, un système qui exécute à la fois les protocoles OSI et TCP/IP représente une duplication complète.

Oracle Solaris est de type *double pile*. En d'autres termes, Oracle Solaris implémente les protocoles IPv4 et IPv6. Lorsque vous installez ce système d'exploitation, vous pouvez choisir d'activer les protocoles IPv6 dans la couche IP ou d'utiliser les protocoles IPv4 définis par

défaut. Le reste de la pile TCP/IP est identique. Par conséquent, les mêmes protocoles de transport, TCP UDP et SCTP, peuvent s'exécuter sur les réseaux IPv4 et IPv6. Les mêmes applications peuvent également s'exécuter sur ces réseaux. La Figure 11–4 illustre le fonctionnement des protocoles IPv4 et IPv6 sous forme de protocoles doubles piles à travers les différentes couches de suites de protocoles Internet.

FIGURE 11–4 Architecture du protocole double pile



Dans un environnement à double pile, les sous-jeux des hôtes et des routeurs sont mis à niveau vers IPv4 et IPv6. Cette approche assure l'interopérabilité constante des nœuds mis à niveau avec des nœuds exclusivement IPv4.

Implémentation IPv6 sous Oracle Solaris

Cette section décrit les fichiers, commandes et démons nécessaires au protocole IPv6 sous Oracle Solaris.

Fichiers de configuration IPv6

Cette section décrit les fichiers de configuration faisant partie de l'implémentation IPv6 :

- “Fichier de configuration `ndpd.conf`” à la page 268
- “Fichier de configuration d'interface IPv6” à la page 271
- “Fichier de configuration `/etc/inet/ipaddrsel.conf`” à la page 272

Fichier de configuration `ndpd.conf`

Le fichier de configuration `/etc/inet/ndpd.conf` sert à configurer les options utilisées par le démon Neighbor Discovery `in.ndpd`. Pour un routeur, `ndpd.conf` sert principalement à configurer le préfixe du site à publier vers le lien. Pour un hôte, `ndpd.conf` sert à désactiver la configuration automatique des adresses ou à configurer des adresses temporaires.

Le tableau suivant présente les mots-clés utilisés dans le fichier `ndpd.conf`.

TABLEAU 11–2 Mots-clés de `/etc/inet/ndpd.conf`

Variable	Description
`ifdefault`	Spécifie le comportement du routeur pour toutes les interfaces. Utilisez la syntaxe suivante pour définir les paramètres du routeur et les valeurs correspondantes : `ifdefault [`*valeur variable*`]`
`prefixdefault`	Spécifie le comportement par défaut pour la publication du préfixe. Utilisez la syntaxe suivante pour définir les paramètres du routeur et les valeurs correspondantes : `prefixdefault [`*valeur variable*`]`
`if`	Définit les paramètres de l'interface. Utilisez la syntaxe suivante : `if` *interface* `[`*valeur variable*`]`
`prefix`	Publie les informations du préfixe par interface. Utilisez la syntaxe suivante : `prefix` *préfixe/longueur interface* `[`*valeur variable*`]`

Dans le fichier `ndpd.conf`, vous utilisez des mots-clés du tableau avec jeu de variables de configuration du routeur. Ces variables sont définies en détail dans le document RFC 2461, Neighbor Discovery for IP Version 6 (IPv6) (`http://www.ietf.org/rfc/rfc2461.txt?number=2461`).

Le tableau suivant répertorie les variables de configuration d'une interface et fournit une brève définition de chacune.

TABLEAU 11–3 Variables de configuration d'interface du fichier `/etc/inet/ndpd.conf`

Variable	Par défaut	Définition
`AdvRetransTimer`	0	Spécifie la valeur du champ Retrans Timer pour la publication de messages envoyés par le routeur.
`AdvCurHopLimit`	Diamètre actuel du réseau Internet	Spécifie la valeur à entrer dans le champ Hop Limit pour la publication de messages envoyés par le routeur.
`AdvDefaultLifetime`	3 + `MaxRtrAdvInterval`	Spécifie la durée de vie par défaut des publications du routeur.

TABLEAU 11–3 Variables de configuration d'interface du fichier `/etc/inet/ndpd.conf` *(Suite)*

Variable	Par défaut	Définition
`AdvLinkMTU`	0	Spécifie une valeur d'unité de transmission maximale (MTU) que le routeur doit envoyer. Une valeur nulle indique que ne routeur ne spécifie pas d'options MTU.
`AdvManaged Flag`	False	Spécifie la valeur à entrer dans l'indicateur de configuration de la gestion des adresses pour la publication du routeur.
`AdvOtherConfigFlag`	False	Spécifie la valeur à entrer dans l'indicateur de configuration des autres paquets avec état pour la publication du routeur.
`AdvReachableTime`	0	Spécifie la valeur du champ Reachable Time pour la publication de messages envoyés par le routeur.
`AdvSendAdvertisements`	False	Indique si le nœud doit envoyer des publications et répondre aux requêtes du routeur. Vous devez définir explicitement la variable sur TRUE dans le fichier `ndpd.conf` afin d'activer les fonctions de publication du routeur. Pour plus d'informations, reportez-vous à la section "Procédure de configuration d'un routeur compatible IPv6" à la page 180.
`DupAddrDetect Transmits`	1	Définit le nombre de messages de requête voisine consécutifs que le protocole Neighbor Discovery doit envoyer lors de la détection d'adresses du nœud local dupliquées.
`MaxRtrAdvInterval`	600 secondes	Spécifie le temps d'attente maximal lors de l'envoi de publications de multidiffusion non requises.
`MinRtrAdvInterval`	200 secondes	Spécifie le temps d'attente minimal lors de l'envoi de publications de multidiffusion non requises.
`StatelessAddrConf`	True	Détermine si le nœud configure son adresse IPv6 par le biais de la configuration automatique des adresses sans état. Si la valeur False est déclarée dans le fichier `ndpd.conf`, l'adresse doit être configurée manuellement. Pour plus d'informations, reportez-vous à la section "Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur" à la page 188.
`TmpAddrsEnabled`	False	Indique si une adresse temporaire doit être créée pour toutes les interfaces ou pour une interface particulière d'un nœud. Pour plus d'informations, reportez-vous à la section "Procédure de configuration d'une adresse temporaire" à la page 185.
`TmpMaxDesyncFactor`	600 secondes	Spécifie une valeur aléatoire à soustraire de la variable de durée de vie préférée `TmpPreferredLifetime` au démarrage de la commande `in.ndpd`. L'objectif de la variable `TmpMaxDesyncFactor` est d'éviter que tous les systèmes de votre réseau ne régénèrent leurs adresses temporaires en même temps. `TmpMaxDesyncFactor` permet de remplacer la limite supérieure par cette valeur.

TABLEAU 11–3 Variables de configuration d'interface du fichier `/etc/inet/ndpd.conf` *(Suite)*

Variable	Par défaut	Définition
`TmpPreferredLifetime`	False	Définit la durée de vie préférée d'une adresse temporaire. Pour plus d'informations, reportez-vous à la section "Procédure de configuration d'une adresse temporaire" à la page 185.
`TmpRegenAdvance`	False	Spécifie à l'avance la durée d'obtention d'une désapprobation pour une adresse temporaire. Pour plus d'informations, reportez-vous à la section "Procédure de configuration d'une adresse temporaire" à la page 185.
`TmpValidLifetime`	False	Définit la durée de vie correcte d'une adresse temporaire. Pour plus d'informations, reportez-vous à la section "Procédure de configuration d'une adresse temporaire" à la page 185.

Le tableau suivant répertorie les variables utilisées pour configurer les préfixes IPv6.

TABLEAU 11–4 Variables de configuration de préfixe du fichier `/etc/inet/ndpd.conf`

Variable	Par défaut	Définition
`AdvAutonomousFlag`	True	Spécifie la valeur à entrer dans le champ Autonomous Flag figurant dans les informations sur le préfixe.
`AdvOnLinkFlag`	True	Spécifie la valeur à entrer dans l'indicateur on-link "L-bit" figurant dans les informations sur le préfixe.
`AdvPreferredExpiration`	Non définie	Spécifie la date d'expiration préférée du préfixe.
`AdvPreferredLifetime`	604 800 secondes	Spécifie la valeur à entrer pour la durée de vie préférée dans les informations sur le préfixe.
`AdvValidExpiration`	Non définie	Spécifie la date d'expiration correcte du préfixe.
`AdvValidLifetime`	2 592 000 secondes	Spécifie la durée de vie correcte du préfixe qui est configurée.

EXEMPLE 11–1 Fichier `/etc/inet/ndpd.conf`

L'exemple suivant répertorie les mots-clés et les variables de configuration utilisés dans le fichier `ndpd.conf`. Supprimez le commentaire (#) pour activer la variable.

```
# ifdefault       [variable-value ]*
# prefixdefault [variable-value ]*
# if ifname    [variable-value ]*
# prefix prefix/length  ifname
#
#  Per interface configuration variables
#
#DupAddrDetectTransmits
#AdvSendAdvertisements
#MaxRtrAdvInterval
#MinRtrAdvInterval
```

EXEMPLE 11–1 Fichier `/etc/inet/ndpd.conf` *(Suite)*

```
#AdvManagedFlag
#AdvOtherConfigFlag
#AdvLinkMTU
#AdvReachableTime
#AdvRetransTimer
#AdvCurHopLimit
#AdvDefaultLifetime
#
# Per Prefix:  AdvPrefixList configuration variables
#
#
#AdvValidLifetime
#AdvOnLinkFlag
#AdvPreferredLifetime
#AdvAutonomousFlag
#AdvValidExpiration
#AdvPreferredExpiration

ifdefault AdvReachableTime 30000 AdvRetransTimer 2000
prefixdefault AdvValidLifetime 240m AdvPreferredLifetime 120m

if qe0 AdvSendAdvertisements 1
prefix 2:0:0:56::/64 qe0
prefix fec0:0:0:56::/64 qe0

if qe1 AdvSendAdvertisements 1
prefix 2:0:0:55::/64 qe1
prefix fec0:0:0:56::/64 qe1

if hme1 AdvSendAdvertisements 1
prefix  2002:8192:56bb:1::/64 qfe0

if hme1 AdvSendAdvertisements 1
prefix  2002:8192:56bb:2::/64 hme1
```

Fichier de configuration d'interface IPv6

IPv6 utilise le fichier `/etc/hostname6.`*interface* au démarrage afin de définir automatiquement les interfaces logiques IPv6. Si vous activez le protocole IPv6 lors de l'installation d'Oracle Solaris, le programme d'installation crée un fichier `/etc/hostname6.`*interface* pour l'interface réseau principale en plus du fichier `/etc/hostname.` *interface*.

Si plus d'une interface physique est détectée lors de l'installation, vous êtes invité à configurer ces interfaces. Le programme d'installation crée des fichiers de configuration d'interface IPv4 physique et des fichiers de configuration d'interface IPv6 logique pour toute interface supplémentaire indiquée.

Tout comme les interfaces IPv4, les interfaces IPv6 peuvent être configurées manuellement après l'installation d'Oracle Solaris. Vous pouvez créer un fichier `/etc/hostname6.` *interface* pour toute nouvelle interface. Pour connaître la procédure de configuration manuelle d'une interface, reportez-vous au Chapitre 6, “Administration d'interfaces réseau (tâches)”.

Le nom des nouveaux fichiers de configuration d'interface peut avoir la syntaxe suivante :

```
hostname.interface
hostname6.interface
```

La variable *interface* possède la syntaxe suivante :

dev[.*module*[.*module* ...]]*PPA*

péri Indique un périphérique d'interface réseau. Le périphérique peut être une interface réseau physique, telle que `eri` ou `qfe` ou une interface logique de type tunnel. Pour de plus amples informations, reportez-vous à la section "Fichier de configuration d'interface IPv6" à la page 271.

Module Répertorie un ou plusieurs modules `STREAMS` à empiler sur le périphérique lorsque celui-ci est monté.

PPA Indique le point d'attache physique.

La syntaxe [.[.]] est également acceptée.

EXEMPLE 11–2 Fichiers de configuration d'interface IPv6

Exemples de noms de fichier de configuration IPv6 valides :

```
hostname6.qfe0
hostname.ip.tun0
hostname.ip6.tun0
hostname6.ip6to4tun0
hostname6.ip.tun0
hostname6.ip6.tun0
```

Fichier de configuration `/etc/inet/ipaddrsel.conf`

Le fichier `/etc/inet/ipaddrsel.conf` contient la table des règles de sélection d'adresse IPv6 par défaut. Si vous avez activé le protocole IPv6 lors de l'installation d'Oracle Solaris, ce fichier contient les éléments présentés dans le Tableau 11–5.

Vous pouvez modifier le contenu de `/etc/inet/ipaddrsel.conf`. Toutefois, cette opération n'est pas recommandée. Si cela s'avère nécessaire, reportez-vous à la procédure décrite à la section "Administration de la table des règles de sélection d'adresses IPv6" à la page 230. Pour plus d'informations sur le fichier `ippaddrsel.conf`, reportez-vous à la section "Raisons pour lesquelles le tableau des règles de sélection d'adresses IPv6 doit être modifié" à la page 273 ainsi qu'à la page de manuel `ipaddrsel.conf`(4).

Commandes associées à IPv6

Cette section décrit les commandes ajoutées lors de l'implémentation du protocole IPv6 sous Oracle Solaris. Les commandes existantes qui ont été modifiées pour prendre en charge IPv6 y sont également détaillées.

Commande `ipaddrsel`

La commande `ipaddrsel` permet de modifier le tableau des règles de sélection des adresses IPv6 par défaut.

Le noyau Oracle Solaris utilise la table des règles de sélection des adresses IPv6 par défaut pour le classement des adresses de destination et la sélection des adresses sources pour les en-têtes de paquet IPv6. Le fichier `/etc/inet/ipaddrsel.conf` contient ce tableau de règles.

Le tableau suivant répertorie les formats d'adresse par défaut ainsi que les priorités de chacune telles qu'elles doivent figurer dans le tableau de règles. Vous pouvez rechercher des informations techniques sur la sélection d'adresses IPv6 dans la page de manuel `inet6(7P)`.

TABLEAU 11–5 Tableau des règles de sélection des adresses IPv6 par défaut

Préfixe	Priorité	Définition
`::1/128`	50	Loopback
`::/0`	40	Par défaut
`2002::/16`	30	6to4
`::/96`	20	IPv4 Compatible
`::ffff:0:0/96`	10	IPv4

Dans ce tableau, les préfixes IPv6 (`::1/128` et `::/0`) ont la priorité sur les adresses 6to4 (`2002::/16`) et les adresses IPv4 (`::/96` et `::ffff:0:0/96`). Par conséquent, le noyau choisit par défaut l'adresse IPv6 globale de l'interface pour les paquets envoyés vers une autre destination IPv6. L'adresse IPv4 de l'interface est moins prioritaire, notamment pour les paquets envoyés vers une destination IPv6. Étant donné l'adresse IPv6 source sélectionnée, le noyau utilise également le format IPv6 pour l'adresse de destination.

Raisons pour lesquelles le tableau des règles de sélection d'adresses IPv6 doit être modifié

En règle générale, le tableau des règles de sélection d'adresses IPv6 par défaut n'a pas besoin d'être modifié. En cas de modification nécessaire, exécutez la commande `ipaddrsel`.

Les situations suivantes nécessitent une modification du tableau :

- Si le système possède une interface qui est utilisée pour un tunnel 6to4, vous pouvez définir une priorité plus élevée pour les adresses 6to4.
- Si vous souhaitez qu'une adresse source particulière communique avec une adresse de destination particulière, vous pouvez ajouter ces adresses au tableau de règles. Ensuite, vous pouvez les marquer comme des adresses préférées à l'aide de la commande `ifconfig`.
- Si vous voulez que les adresses IPv4 aient la priorité sur les adresses IPv6, vous pouvez remplacer la priorité de `::ffff:0:0/96` par un chiffre plus élevé.
- Si vous devez assigner une priorité plus élevée à des adresses désapprouvées, vous pouvez ajouter ces adresses au tableau de règles. Prenons l'exemple des adresses de site locales, actuellement désapprouvées sur le réseau IPv6. Ces adresses possèdent le préfixe `fec0::/10` . Vous pouvez modifier le tableau de règles afin de définir une priorité plus élevée pour ces adresses.

Pour de plus amples informations sur la commande `ipaddrsel`, reportez-vous à la page de manuel `ipaddrsel(1M)`.

Commande `6to4relay`

La *création de tunnel 6to4* permet à des sites 6to4 isolés de communiquer. Cependant, pour transférer des paquets vers un site IPv6 natif et non-6to4, le routeur 6to4 doit être relié au routeur relais 6to4 par un tunnel. Le *routeur relais 6to4* transfère ensuite les paquets 6to4 au réseau IPv6 et, finalement, au site IPv6 natif. Si un site 6to4 doit échanger des données avec un site IPv6, vous pouvez créer le tunnel approprié à l'aide de la commande `6to4relay`.

Sous Oracle Solaris, la liaison de tunnels à des routeurs relais est désactivée car l'utilisation des routeurs relais n'est pas sécurisée. Avant de relier un tunnel à un routeur relais 6to4, vous devez être conscient des problèmes qui peuvent survenir avec ce type de scénario. Pour de plus amples informations sur les routeurs relais 6to4, reportez-vous à la section “Informations importantes pour la création de tunnels vers un routeur relais 6to4” à la page 297. Pour activer la prise en charge d'un routeur relais 6to4, vous pouvez suivre la procédure indiquée à la section “Procédure de configuration d'un tunnel 6to4” à la page 195.

Syntaxe de la commande 6to4relay

La commande `6to4relay` possède la syntaxe suivante :

```
6to4relay -e [-a IPv4-address] -d -h
```

`-e` Assure la prise en charge de tunnels entre le routeur 6to4 et un routeur relais 6to4 anycast. Ainsi, l'adresse du point d'extrémité du tunnel est définie sur `192.88.99.1` , soit l'adresse du groupe anycast de routeurs relais 6to4.

`-a` *adresse IPv4* Assure la prise en charge de tunnels entre le routeur 6to4 et un routeur relais 6to4 possédant l'*adresse IPv4* spécifiée.

`-d`	Désactive la prise en charge de tunnels vers un routeur relais 6to4 (paramètre par défaut d'Oracle Solaris).
`-h`	Affiche l'aide concernant la commande `6to4relay`.

Pour plus d'informations, reportez-vous à la page de manuel `6to4relay`(1M).

EXEMPLE 11–3 Affichage par défaut du statut de la prise en charge de routeurs relais 6to4

La commande `6to4relay`, sans argument, affiche le statut actuel de la prise en charge des routeurs relais 6to4. Cet exemple indique la sortie par défaut de l'implémentation du protocole IPv6 sous Oracle Solaris.

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is disabled
```

EXEMPLE 11–4 Affichage du statut avec prise en charge des routeurs relais 6to4 activée

Lorsque la prise ne charge des routeurs relais est activée, la commande `6to4relay` affiche la sortie suivante :

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is enabled
IPv4 destination address of Relay Router=192.88.99.1
```

EXEMPLE 11–5 Affichage du statut avec un routeur relais 6to4 spécifié

Si vous spécifiez l'option `-a` et une adresse IPv4 dans la commande `6to4relay`, l'adresse IPv4 fournie avec l'option `- a` remplace l'adresse `192.88.99.1`.

La commande `6to4relay` ne signale pas l'exécution des options `-d`, `-e` et `-a` *adresse IPv4*. Cependant, elle n'affiche aucun message d'erreur lié à l'exécution de ces options.

Extensions de commande `ifconfig` pour la prise en charge IPv6

La commande `ifconfig` permet de monter les interfaces IPv6 et le module de mise sous tunnel. `ifconfig` utilise un jeu étendu de ioctls pour configurer à la fois les interfaces réseau IPv4 et IPv6. Les options `ifconfig` qui prennent en charge les opérations IPv6 sont répertoriées ci-dessous. Pour connaître les différentes tâches IPv4 et IPv6 qui impliquent l'exécution de la commande `ifconfig`, reportez-vous à la section “Contrôle de la configuration de l'interface avec la commande `ifconfig`” à la page 209.

`index`	Définit l'index de l'interface.
`tsrc/tdst`	Définit la source ou la destination du tunnel.
`addif`	Crée l'interface logique suivante.
`removeif`	Supprime une interface logique possédant une adresse IP spécifique.

`destination`	Définit l'adresse de destination point à point pour une interface.
`set`	Définit une adresse et/ou un masque de réseau pour une interface.
`subnet`	Définit l'adresse de sous-réseau d'une interface.
`xmit/-xmit`	Active ou désactive la transmission de paquets sur une interface.

Le Chapitre 7, “Configuration d'un réseau IPv6 (tâches)” fournit les procédures de configuration des réseaux IPv6.

EXEMPLE 11–6 Ajout d'une interface IPv6 logique avec l'option `-addif` de la commande `ifconfig`

La commande `ifconfig` suivante crée une interface logique `hme0:3` :

```
# ifconfig hme0 inet6 addif up
Created new logical interface hme0:3
```

Cette forme de `ifconfig` vérifie la création de l'interface :

```
# ifconfig hme0:3 inet6
hme0:3: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        inet6  inet6 fe80::203:baff:fe11:b321/10
```

EXEMPLE 11–7 Suppression d'une interface IPv6 logique avec l'option `-removeif` de la commande `ifconfig`

La commande `ifconfig` suivante supprime une interface logique `hme0:3` :

```
# ifconfig hme0:3 inet6 down

# ifconfig hme0 inet6 removeif 1234::5678
```

EXEMPLE 11–8 Configuration de la source d'un tunnel IPv6 à l'aide de la commande `ifconfig`

```
# ifconfig ip.tun0 inet6 plumb index 13
```

Ouvre le tunnel à associer au nom de l'interface physique.

```
# ifconfig ip.tun0 inet6
ip.tun0: flags=2200850<POINTOPOINT,RUNNING,MULTICAST,NONUD,
#IPv6> mtu 1480 index 13
        inet tunnel src 0.0.0.0
        inet6 fe80::/10 --> ::
```

Configure les flux nécessaires au protocole TCP/IP pour utiliser le périphérique du tunnel et signaler son statut.

```
# ifconfig ip.tun0 inet6 tsrc 120.46.86.158 tdst 120.46.86.122
```

Configure l'adresse source et l'adresse cible du tunnel.

EXEMPLE 11–8 Configuration de la source d'un tunnel IPv6 à l'aide de la commande `ifconfig` *(Suite)*

```
# ifconfig ip.tun0 inet6
ip.tun0: flags=2200850<POINTOPOINT,RUNNING,MULTICAST,NONUD,
IPv6> mtu 1480 index 13
        inet tunnel src 120.46.86.158  tunnel dst 120.46.86.122
        inet6 fe80::8192:569e/10 --> fe80::8192:567a
```

Indique le nouveau statut du périphérique après la configuration.

EXEMPLE 11–9 Configuration d'un tunnel 6to4 à l'aide de `ifconfig` (forme longue)

Dans l'exemple suivant, une configuration de pseudointerface 6to4 utilise l'ID de sous-réseau 1 et spécifie l'ID hôte sous forme hexadécimale.

```
# ifconfig ip.6to4tun0 inet6 plumb
# ifconfig ip.6to4tun0 inet tsrc 129.146.86.187 \
2002:8192:56bb:1::8192:56bb/64 up

# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NONUD,IPv6>mtu 1480 index 11
        inet tunnel src 129.146.86.187
        tunnel hop limit 60
        inet6 2002:8192:56bb:1::8192:56bb/64
```

EXEMPLE 11–10 Configuration d'un tunnel 6to4 à l'aide de `ifconfig` (forme courte)

Voici une forme courte de la commande permettant de configurer un tunnel 6to4.

```
# ifconfig ip.6to4tun0 inet6 plumb
# ifconfig ip.6to4tun0 inet tsrc 129.146.86.187 up

# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NONUD,IPv6>mtu 1480 index 11
        inet tunnel src 129.146.86.187
        tunnel hop limit 60
        inet6 2002:8192:56bb::1/64
```

Modification de la commande `netstat` en vue de la prise en charge IPv6

La commande `netstat` affiche le statut des réseaux IPv4 et IPv6. Vous pouvez choisir les informations de protocole à afficher en définissant la valeur de `DEFAULT_IP` dans le fichier `/etc/default/inet_type` ou en utilisant l'option `-f` dans la ligne de commande. Avec une valeur de `DEFAULT_IP` permanente, vous vous assurez que la commande `netstat` affiche uniquement les informations IPv4. Vous pouvez ignorer ce paramètre et utiliser l'option `-f`. Pour plus d'informations sur le fichier `inet_type` , reportez-vous à la page de manuel `inet_type(4)`.

L'option `-p` de la commande `netstat` affiche la table des connexions réseau-média, c'est-à-dire la table des protocoles de résolution d'adresse pour l'IPv4 et le cache voisin pour l'IPv6. Pour de

plus amples informations, reportez-vous à la page de manuel `netstat`(1M) La section "Affichage du statut des sockets" à la page 216 décrit les procédures impliquant l'exécution de cette commande.

Modification de la commande `snoop` en vue de la prise en charge IPv6

La commande `snoop` permet de capturer des paquets IPv4 et IPv6. Cette commande peut s'afficher avec des en-têtes IPv6, des en-têtes d'extension IPv6, des en-têtes ICMPv6 et des données de protocole Neighbor Discovery. Par défaut, la commande `snoop` affiche les deux types de paquet (IPv4 et IPv6). Pour afficher soit l'un, soit l'autre, spécifiez le mot-clé de protocole `ip` ou `ip6` avec la commande `snoop`. L'option de filtrage IPv6 vous permet de filtrer tous les paquets IPv4 et IPv6 et d'afficher uniquement les paquets IPv6. Pour plus d'informations, reportez-vous à la page de manuel `snoop`(1M) La section "Contrôle du trafic réseau IPv6" à la page 229 décrit les procédures implicant l'exécution de la commande `snoop`.

Modification de la commande `route` en vue de la prise en charge IPv6

La commande `route` fonctionne sur les routes IPv4 (par défaut) et IPv6. Pour réaliser des opérations sur les routes IPv6, tapez l'option `-inet6` immédiatement à la suite de la commande `route` dans la ligne de commande. Pour plus d'informations, reportez-vous à la page de manuel `route`(1M).

Modification de la commande `ping` en vue de la prise en charge IPv6

La commande `ping` se sert des protocoles IPv4 et IPv6 pour sonder les hôtes cibles. Le choix du protocole dépend des adresses renvoyées par le serveur de noms pour l'hôte cible spécifique. Par défaut, si ce serveur renvoie une adresse IPv6 pour l'hôte cible, la commande `ping` utilise le protocole IPv6. S'il renvoie une adresse IPv4, la commande `ping` utilise le protocole IPv4. Pour ignorer cette action, vous pouvez taper l'option `-A` dans la ligne de commande et spécifier le protocole à utiliser.

Pour de plus amples informations, reportez-vous à la page de manuel `ping`(1M) La section "Test des hôtes distants à l'aide de la commande `ping`" à la page 220 décrit les procédures implicant l'exécution de la commande `ping` .

Modification de la commande `traceroute` en vue de la prise en charge IPv6

Vous pouvez exécuter la commande `traceroute` pour tracer les routes IPv4 et IPv6 vers un hôte spécifique. Du point de vue du protocole, `traceroute` utilise le même algorithme que la commande `ping`. Pour ignorer ce choix, tapez l'option `-A` dans la ligne de commande. Vous pouvez tracer chaque route vers chaque adresse d'un hôte multiréseau en tapant l'option `-a` dans la ligne de commande.

Pour de plus amples informations, reportez-vous à la page de manuel `traceroute`(1M) La section “Affichage des informations de routage à l'aide de la commande `traceroute`” à la page 224 décrit les procédures qui impliquent l'exécution de la commande `traceroute`.

Démons liés à IPv6

Cette section présente les démons liés à IPv6.

Démon `in.ndpd` pour Neighbor Discovery

Le démon `in.ndpd` implémente le protocole IPv6 Neighbor Discovery ainsi que celui de découverte de routeur. Il implémente également la configuration automatique d'adresse IPv6. Les options suivantes sont prises en charge par `in.ndpd`.

`-d` Active le débogage.

`-D` Active le débogage dans le cadre d'événements spécifiques.

`-f` Spécifie un fichier de données de configuration spécifique au lieu du fichier `/etc/inet/ndpd.conf`.

`-I` Imprime les informations associées à chaque interface.

`-n` Ne met pas en boucle les publications du routeur.

`-r` Ignore la réception de paquets.

`-v` Spécifie le mode détaillé en faisant état de plusieurs types de message de diagnostic.

`-t` Active le suivi des paquets.

Le démon `in.ndpd` est contrôlé par les paramètres définis dans le fichier de configuration `/etc/inet/ndpd.conf` et par ceux du fichier de démarrage `/var/inet/ndpd_state.` *interface* qui s'appliquent.

Lorsque le fichier `/etc/inet/ndpd.conf` existe, il est analysé et utilisé pour configurer un nœud en tant que routeur. Le Tableau 11–2 répertorie les mots-clés corrects susceptibles de figurer dans ce fichier. Lors de l'initialisation d'un hôte, les routeurs risquent de ne pas être disponibles immédiatement. Les paquets publiés par le routeur risquent d'être abandonnés. En outre, les paquets risquent de ne pas atteindre l'hôte.

Le fichier `/var/inet/ndpd_state.`*interface* est un fichier d'état. Ce fichier est régulièrement mis à jour par chaque nœud. En cas de défaillance et de redémarrage du nœud, ce dernier peut configurer ses interfaces en l'absence de routeurs. Ce fichier contient l'adresse de l'interface, l'heure de la dernière mise à jour du fichier et la durée de validité du fichier. Il contient également d'autres paramètres “hérités” de précédentes publications de routeur.

Remarque – Il est inutile de modifier le contenu des fichiers d'état. Le démon `in.ndpd` assure la maintenance automatique des fichiers d'état.

Consultez les pages de manuel `in.ndpd(1M)` et `ndpd.conf(4)` pour obtenir des listes des variables de configuration et des valeurs acceptables.

Démon `in.ripngd`, pour routage IPv6

Le démon `in.ripngd` implémente les informations de RIPng (Routing Information Protocol next-generation, protocole d'informations de routage nouvelle génération) pour les routeurs IPv6. Le RIPng définit l'équivalent IPv6 de RIP (Routing Information Protocol, protocole d'informations de routage). Lorsque vous configurez un routeur IPv6 avec la commande `routeadm` et activez le routage IPv6, le démon `in.ripngd` implémente RIPng sur le routeur.

Vous trouverez ci-dessous les options RIPng prises en charge.

`-p` *n* — *n* spécifie le numéro de port alternatif utilisé pour l'envoi ou la réception de paquets RIPnG.

`-q` — Supprime les informations de routage.

`-s` — Force le routage d'informations même si le démon fait office de routeur.

`-P` — Supprime l'utilisation du poison reverse.

`-S` — Si `in.ripngd` n'agit pas en tant que routeur, le démon saisit uniquement une route par défaut pour chaque routeur.

Démon `inetd` et services IPv6

Une application de serveur compatible IPv6 peut gérer les requêtes IPv4 et IPv6, ou les requêtes IPv6 uniquement. Le serveur gère toujours les requêtes par le biais d'un socket IPv6. En outre, le serveur utilise le même protocole qu'utilise le client correspondant. Pour ajouter ou modifier un service pour IPv6, utilisez les commandes disponibles à partir du service SMF (Service Management Facility, utilitaire de gestion des services).

- Pour plus d'informations sur les commandes SMF, reportez-vous aux "Utilitaires d'administration en ligne de commande SMF" du *Guide d'administration système : administration de base*.
- Pour obtenir une tâche d'exemple utilisant le service SMF pour configurer un manifeste de service IPv4 s'exécutant sur SCTP, reportez-vous à la section "Ajout de services utilisant le protocole SCTP" à la page 141.

Pour configurer un service IPv6, vous devez vous assurer que la valeur du champ `proto` dans le profil `inetadm` pour ce service répertorie la valeur adéquate :

- Pour un service assurant la gestion de requêtes IPv4 et IPv6, sélectionnez `tcp6`, `udp6` ou `sctp`. Une valeur `proto` de `tcp6`, `udp6` ou `sctp6` a pour conséquence de faire passer `inetd` sur un socket IPv6 vers le serveur. Le serveur contient une adresse mappée IPv4 au cas où un client IPv4 recevrait une requête.
- Pour un service qui gère uniquement les requêtes IPv6, sélectionnez `tcp6only` ou `udp6only`. Si `proto` a l'une de ces valeurs, `inetd` passe le serveur à un socket IPv6.

Si vous remplacez une command'Oracle Solaris par une autre implémentation, vous devez vous assurer que l'implémentation de ce service prend en charge le protocole IPv6. Si l'implémentation ne prend pas IPv6 en charge, vous devez spécifier la valeur `proto` en tant que `tcp`, `udp` ou `sctp`.

Voici un profil qui résulte de l'exécution de `inetadm` pour un manifeste de service `echo` prenant IPv4 et IPv6 en charge, et s'exécute sur 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
```

La syntaxe suivante permet de modifier la valeur du champ `proto` :

```
# inetadm -m FMRI proto="transport-protocols"
```

Tous les serveurs fournis avec le logiciel Oracle Solaris ne nécessitent qu'une entrée de profil spécifiant `proto` en tant que `tcp6`, `udp6` ou `sctp6`. Cependant, le serveur shell distant (`shell`) et le serveur d'exécution distant (`exec`) sont à présent composés d'une instance de service unique, nécessitant une valeur `proto` contenant les valeurs `tcp` et `tcp6only`. Par exemple, pour définir la valeur `proto` pour `shell`, émettez la commande suivante :

```
# inetadm -m network/shell:default proto="tcp,tcp6only"
```

Consultez les extensions IPv6 de l'API Socket dans la section *Programming Interfaces Guide* pour obtenir des informations supplémentaires sur l'écriture de serveurs compatibles IPv6 qui utilisent des sockets.

Informations importantes relatives à la configuration d'un service pour IPv6

Gardez les éléments suivants à l'esprit lorsque vous ajoutez ou modifiez un service pour IPv6 :

- Vous devez spécifier la valeur `proto` en tant que `tcp6`, `sctp6` ou `udp6` afin d'activer les connexions IPv4 ou IPv6. Si vous spécifiez la valeur pour `proto` en tant que `tcp`, `sctp` ou `udp`, le service n'utilise qu'IPv4.
- Bien qu'il soit possible d'ajouter une instance de service utilisant des sockets SCTP de style un à plusieurs à `inetd`, il est déconseillé de le faire. `inetd` ne fonctionne pas avec les sockets SCTP de style un à plusieurs.
- Si un service nécessite deux entrées en raison de propriétés `wait-status` ou `exec` différentes, vous devez créer deux instances/services à partir du service d'origine.

Protocole ND IPv6

IPv6 présente le protocole Neighbor Discovery, comme décrit dans le document RFC 2461, Neighbor Discovery for IP Version 6 (IPv6) (`http://www.ietf.org/rfc/rfc2461.txt?number=2461`). Pour obtenir une présentation des principales fonctionnalités de la détection des voisins, reportez-vous à la section “Présentation du protocole de détection de voisins IPv6” à la page 83.

Cette section décrit les fonctionnalités suivantes du protocole ND :

Messages ICMP de la détection des voisins

La détection de voisins définit cinq nouveaux messages ICMP (Internet Control Message Protocol, protocole de messages de contrôle Internet). Les messages remplissent les fonctions suivantes :

- **Sollicitation de routeur** – Lorsqu'une interface est activée, les hôtes peuvent demander des messages de sollicitation de routeur. Les sollicitations demandent aux routeurs de générer immédiatement des publications de routeurs, plutôt qu'à la prochaine heure prévue.
- **Publication de routeur** – Les routeurs publient leur présence, divers liens de paramètres et divers liens de paramètres Internet. Les routeurs effectuent des publications régulières ou en réponse à un message de sollicitation de routeur. Les publications de routeur contiennent

des préfixes utilisés pour la détermination sur lien ou la configuration d'adresse, une valeur de limite de saut recommandée, et ainsi de suite.

- **Sollicitation de voisin** – Les nœuds envoient des messages de sollicitation de voisins afin de déterminer l'adresse de couche liaison du voisin. Les messages de sollicitation de voisin sont également envoyés afin de vérifier qu'un voisin est toujours accessible par une adresse de couche liaison mise en cache. Les sollicitations s'utilisent également pour la détection d'adresses dupliquées.
- **Publication de voisins** – Un nœud envoie des messages de publication de voisinage en réponse à un message de sollicitation de voisinage Le nœud peut également envoyer des publications de voisinage non sollicitées pour signaler une modification de l'adresse de couche liaison.
- **Redirection** – Les routeurs utilisent les messages de redirection afin d'informer les hôtes de l'existence d'un meilleur saut pour une destination ou que la destination se trouve sur la même liaison.

Processus de configuration automatique

Cette section comprend une présentation des étapes typiques effectuées par une interface lors d'une configuration automatique. La configuration automatique s'effectue uniquement sur des liaisons compatibles multicast.

1. Une interface compatible multicast est activée, par exemple, lors du démarrage système d'un nœud.
2. Le nœud démarre le processus de configuration automatique en générant une adresse lien-local pour l'interface.

   L'adresse lien-local est formée à partir de l'adresse MAC (Media Access Control) de l'interface.
3. Le nœud envoie un message de sollicitation de voisin contenant l'adresse lien-local provisoire en guise de cible.

   Le message a pour objectif de vérifier que l'adresse possible n'est pas déjà utilisée par un autre nœud sur la liaison. Une fois la vérification effectuée, l'adresse lien-local peut être assignée à l'interface.

   a. Si un autre nœud utilise déjà l'adresse proposée, celui-ci renvoie une publication de voisin indiquant que l'adresse est déjà en cours d'utilisation.

   b. Si un autre nœud tente également d'utiliser la même adresse, le nœud envoie également une sollicitation de voisinage pour la cible.

      Le nombre de transmissions ou de retransmissions de sollicitation de voisins, ainsi que le temps d'attente entre sollicitations, sont spécifiques aux liaisons. Au besoin, vous pouvez définir ces paramètres.

4. Si un nœud détermine que son adresse lien-local possible n'est pas unique, la configuration automatique est interrompue. Dans ce cas, vous devrez configurer manuellement l'adresse lien-local de l'interface.

   Pour simplifier la récupération, vous pouvez fournir un autre ID d'interface qui remplace l'identifiant par défaut. Ensuite, le mécanisme de configuration automatique peut reprendre, en utilisant le nouvel ID d'interface, qui est à priori unique.

5. Lorsqu'un nœud détermine l'unicité de sa future adresse lien-local, il assigne celle-ci à l'interface.

   Le nœud dispose alors d'une connectivité de niveau IP avec les nœuds voisins. Les étapes restantes de la configuration automatique sont effectuées exclusivement par les hôtes.

Obtention d'une publication de routeur

La phase suivante de la configuration automatique consiste à obtenir une publication de routeur ou à déterminer une absence totale de routeurs. Si les routeurs sont présents, ils envoient des publications de routeur qui spécifient le type de configuration automatique que doit effectuer un hôte.

Les routers envoient des publications de routeur à intervalles réguliers. Cependant, le temps d'attente entre publications successives est en règle générale plus long que le temps d'attente possible d'un hôte effectuant la configuration automatique. Afin d'obtenir une publication dans les plus brefs délais, un hôte envoie une ou plusieurs sollicitations de routeur au groupe multicast tous routeurs.

Variables de préfixes de configuration

La publication de routeur contient également des variables de préfixe avec des informations utilisées par la configuration automatique d'adresse sans état pour la génération de préfixes. Le champ de configuration automatique d'adresse sans état dans les publications de routeur sont traitées indépendamment. Un champ d'option contenant les informations de préfixe, l'indicateur de configuration automatique d'adresse, indique si l'option s'applique également à la configuration automatique sans état. Si le champ d'option s'y applique, des champs d'option supplémentaires contiennent un préfixe de sous-réseau avec des valeurs de durée de vie. Ces valeurs indiquent la durée de validité et de préférence des adresses créées à partir du préfixe.

Dans la mesure où les routeurs génèrent régulièrement des publications de routeur, les hôtes reçoivent de nouvelles publications en continu. Les hôtes compatibles IPv6 traitent les informations contenues dans chaque publication. Les hôtes ajoutent des informations. Ils actualisent également les informations reçues dans les publications précédentes.

Unicité des adresses

Pour des raisons de sécurité, l'unicité de toutes les adresses doit être vérifiée, préalablement à leur assignation à une interface. La situation est différente pour les adresses créées par configuration automatique sans état. L'unicité d'une adresse est déterminée principalement par la partie de l'adresse formée à partir d'un ID d'interface. Par conséquent, si un nœud a déjà vérifié l'unicité d'une adresse lien-local, il est inutile de tester les adresses supplémentaires individuellement. Les adresses doivent être créées à partir du même ID d'interface. Toutes les adresses obtenues manuellement doivent par contre être testées individuellement pour leur unicité. Les administrateurs système de certains sites pensent que les bénéfices de la détection d'adresses dupliquées ne vaut pas le temps système qu'elle utilise. Pour ces sites, l'utilisation de la détection des adresses dupliquées peut être désactivée en définissant un indicateur de configuration par interface.

Pour accélérer le processus de configuration automatique, un hôte peut générer son adresse lien-local et vérifier son unicité, pendant que l'hôte attend une publication de routeur. Un routeur peut retarder une réponse à une sollicitation de routeur de quelques secondes. Par conséquent, le temps total nécessaire à la configuration automatique peut être bien plus long si les deux étapes sont effectuées en série.

Sollicitation de voisin et inaccessibilité

La détection de voisins utilise les messages de *sollicitation de voisin* pour déterminer si plusieurs nœuds sont assignés à la même adresse unicast. *La détection d'inaccessibilité de voisin* détecte la défaillance d'un voisin ou du chemin de transfert du voisin. Cette détection nécessite une confirmation de la réception des paquets par le voisin. La détection d'inaccessibilité de voisins détermine également que les paquets sont traités correctement par la couche IP du nœud.

La détection d'inaccessibilité de voisin utilise les confirmations en provenance de deux sources : les protocoles de couche supérieure et les messages de sollicitation de voisin. Lorsque c'est possible, les protocoles de couche supérieure fournissent une confirmation positive de la *progression* d'une connexion. Par exemple, à la réception d'accusés de réception TCP, il est confirmé que les données précédemment envoyées ont été livrées correctement.

Lorsqu'un nœud n'obtient pas de confirmation en provenance des protocoles de couche supérieure, le nœud envoie des messages de sollicitation de voisins. Ces messages sollicitent des publications de voisinage en tant que confirmation d'accessibilité à partir du prochain saut. Pour réduire le trafic réseau inutile, les messages de sonde sont envoyés uniquement au nœud envoyant des paquets activement.

Algorithme de détection d'adresse dupliquée

Pour garantir que toutes les adresses configurées sont susceptibles d'être uniques sur un lien donné, les nœuds exécutent un algorithme de *détection d'adresse dupliquée* sur les adresses. Les nœuds doivent exécuter l'algorithme avant d'assigner les adresses à une interface. L'algorithme de détection d'adresses dupliquées est exécuté sur toutes les adresses.

Le processus de configuration automatique décrit dans cette section s'applique uniquement aux hôtes et non aux routeurs. Dans la mesure où la configuration automatique utilise des informations publiées par les routeurs, ces derniers doivent être configurés différemment. Cependant, les routeurs génèrent des adresses lien-local à l'aide du mécanisme décrit dans ce chapitre. En outre, les routeurs doivent réussir l'algorithme de détection d'adresses dupliquées sur toutes les adresses préalablement à l'assignation d'une adresse à une interface.

Publications de proxy

Un routeur qui accepte les paquets à la place d'une adresse cible peut émettre des publications de voisin impossibles à ignorer. Le routeur peut accepter des paquets pour une adresse cible incapable de répondre aux sollicitations de voisins. L'utilisation de proxy n'est actuellement pas spécifiée. Cependant, la publication de proxy pourrait être utilisée pour la gestion de cas comme ceux de nœuds mobiles qui ont été déplacés hors liaison. Notez que l'utilisation de proxy n'est pas destinée à l'être en tant que mécanisme général de gestion des nœuds qui n'implémentent pas ce protocole.

Équilibrage de charge entrante

Les nœuds avec interfaces répliquées peuvent avoir besoin d'équilibrer la charge de la réception de paquets entrants sur plusieurs interfaces réseau situées sur la même liaison. Ces nœuds possèdent plusieurs adresses lien-local assignées à la même interface. Par exemple, un pilote de réseau unique peut représenter plusieurs cartes d'interface réseau en tant qu'interface logique unique possédant plusieurs adresses lien-local.

La gestion de l'équilibrage de charge s'effectue en autorisant les routeurs à omettre l'adresse lien-local source des paquets de publication de routeur. Par conséquent, les voisins doivent utiliser les messages de sollicitation de voisin afin de connaître les adresses lien-local des routeurs. Les messages renvoyés de publication des voisins peuvent contenir des adresses lien-local différentes, selon l'adresse qui a envoyé la demande.

Modification d'adresse lien-local

Un nœud qui sait que son adresse lien-local a été modifiée peut envoyer des paquets de publication de voisins multicast non sollicités. Le nœud peut envoyer des paquets multicast à tous les nœuds pour une mise à jour des adresses lien-local mises en cache qui ne sont plus valides. L'envoi de publications non sollicitées constitue uniquement une amélioration des performances. L'algorithme de détection d'inaccessibilité des voisins assure la fiabilité de la détection de la nouvelle adresse par le nœud, bien que le temps d'attente risque d'être légèrement plus long.

Comparaison du protocole ND et du protocole ARP et autres protocoles IPv4

La fonctionnalité du protocole ND (Neighbor Discovery, détection des voisins) IPv6 correspond à une combinaison des protocoles IPv4 : ARP (Address Resolution Protocol, protocole de résolution d'adresse), détection de routeur ICMP (Internet Control Message Protocol, protocole de messages de contrôle Internet) et redirection ICMP. IPv4 ne possède pas de protocole ou de mécanisme accepté par tous pour la détection d'inaccessibilité. Cependant, les exigences de l'hôte spécifient les algorithmes possibles pour la détection de passerelles bloquées. La détection de passerelles bloquées est un sous-ensemble des problèmes résolus par la détection d'inaccessibilité de voisins.

La liste suivante compare le protocole de détection de voisins à la suite de protocoles IPv4 associés.

- La détection de routeur fait partie du jeu de protocoles IPv6 de base. Les hôtes IPv6 n'ont pas besoin d'émettre la commande `snoop` aux protocoles de routage pour rechercher un routeur. IPv4 utilise le protocole ARP, la détection de routeur ICMP et la redirection ICMP pour la détection de routeur.
- Les publications de routeur IPv6 gèrent les adresses lien-local. Aucun échange de paquet supplémentaire n'est nécessaire pour la résolution de l'adresse lien-local du routeur.
- Les publications de routeur gèrent les préfixes de site pour une liaison. Aucun mécanisme séparé n'est nécessaire pour la configuration du masque de réseau, contrairement à IPv4.
- Les publications de routeur sont compatibles avec la configuration automatique d'adresse. La configuration automatique n'est pas implémentée dans IPv4.
- La détection de voisins permet aux routeurs IPv6 de publier la MTU utilisable pour les hôtes sur la liaison. Par conséquent, tous les nœuds utilisent la même valeur de MTU sur des liaisons ne disposant pas d'une MTU correctement définie. Les hôtes IPv4 sur un même réseau peuvent avoir des MTU différentes.

- Contrairement aux adresses de diffusion IPv4, la multidiffusion de résolution d'adresse IPv6 est répartie sur 4 milliards (2^32) d'adresses multicast, ce qui réduit de façon significative les interruptions relatives à la résolution d'adresses sur des nœuds autres que la cible. En outre, les ordinateurs non IPv6 ne doivent pas être éteints.
- Les redirections IPv6 contiennent l'adresse lien-local du premier nouveau saut. La résolution d'adresse séparée n'est pas nécessaire lors de la réception d'une redirection.
- Il est possible d'associer plusieurs préfixes de site au même réseau IPv6. Par défaut, les hôtes sont informés de tous les préfixes de site locaux par les publications de routeur. Cependant, les routeurs peuvent être configurés afin d'omettre certains ou tous les préfixes des publications de routeur. Dans de tels cas, les hôtes partent du principe que les destinations se trouvent sur des réseaux distants. Par conséquent, les hôtes envoient le trafic aux routeurs. Un routeur peut alors émettre des redirections le cas échéant.
- Contrairement à IPv4, le destinataire d'un message IPv6 redirigé part du principe que le nouveau saut suivant se trouve sur le réseau local. Dans IPv4, un hôte ignore les messages de redirection qui spécifient un saut suivant qui ne se trouve pas sur le réseau local, selon le masque de réseau. Le mécanisme de redirection IPv6 est similiaire à l'utilitaire XRedirect d'IPv4. Le mécanisme de redirection est utile sur des liens de non diffusion ou de médias partagés. Sur ces réseaux, les nœuds ne doivent pas effectuer de vérification sur tous les préfixes pour les destinations de liaison locale.
- La détection d'inaccessibilité de voisin IPv6 améliore la livraison de paquets en la présence de routeurs défaillants. Cette capacité améliore la livraison de paquets sur des liaisons partiellement défaillantes ou partitionnées. Cette capacité améliore également la livraison de paquet sur des nœuds qui modifient leurs adresses lien-local. Par exemple, les nœuds mobiles peuvent se déplacer hors du réseau local sans aucune perte de connectivité en raison d'anciens caches ARP. IPv4 ne possède pas de méthode correspondante de détection d'inaccessibilité de voisins.
- Contrairement au protocole ARP, la détection de voisins détecte les défaillances de demi liaison à l'aide de la détection d'inaccessibilité de voisins. La détection de voisins évite d'envoyer du trafic aux voisins en l'absence de connectivité bidirectionnelle.
- En utilisant les adresses lien-local pour identifier les routeurs de façon unique, les hôtes IPv6 peuvent conserver les associations de routeur. La capacité d'identification de routeurs est requise pour les publications de routeur et pour les messages de redirection. Les hôtes doivent conserver les associations de routeur si le site utilise de nouveaux préfixes globaux. IPv4 ne possède pas de méthode comparable d'identification des routeurs.
- Dans la mesure où les messages de détection de voisins ont une limite de saut de 255 après réception, le protocole n'est pas affecté par les attaques de mystification en provenance de nœuds hors liaison. Les nœuds IPv4 hors liaison sont eux capables d'envoyer des messages de redirection ICMP. Les nœuds IPv4 hors liaison peuvent également envoyer des messages de publication de routeur.

- En plaçant la résolution d'adresse à la couche ICMP, la détection de voisins est moins dépendante de médias que le protocole ARP. Par conséquent, les mécanismes standard d'authentification IP et de sécurité peuvent être utilisés.

Routage IPv6

Le routage IPv6 est quasiment identique au routage IPv4 sous CIDR (Classless Inter-Domain Routing, routage inter-domaine sans classe). La seule différence est la taille des adresses qui sont de 128 bits dans IPv6 au lieu de 32 bits dans IPv4. Avec des extensions simples, il est possible d'utiliser la totalité des algorithmes de routage d'IPv4 comme OSPF, RIP, IDRP et IS-IS.

IPv6 comprend également des extensions de routage simples qui prennent en charge de nouvelles capacités de routage puissantes. La liste suivante décrit les nouvelles capacités de routage :

- sélection de fournisseur en fonction de la stratégie, des performances, des coûts, etc ;
- hébergement de mobilité, routage vers emplacement actuel ;
- réadressage automatique, routage vers nouvelle adresse.

Les nouvelles capacités de routage s'obtiennent par la création de séquences d'adresses IPv6 utilisant l'option de routage IPv6. Une source IPv6 utilise l'option de routage afin de répertorier un ou plusieurs nœuds intermédiaires, ou groupes topologiques, à visiter en cours d'acheminement vers la destination du paquet. Cette fonction possède énormément de similitudes avec l'option IPv4 de source lâche et de route d'enregistrement.

Pour que les séquences d'adresses soient une fonction générale, les hôtes IPv6 doivent, dans la plupart des cas, inverser les routes d'un paquet reçu par un hôte. Le paquet doit être authentifié à l'aide de l'utilisation de l'en-tête d'authentification IPv6. Le paquet doit contenir des séquences d'adresse afin d'être renvoyé à son point d'origine. Cette technique force les implémentations d'hôtes IPv6 pour la prise en charge de la gestion et de l'inversion des routes source. La gestion et l'inversion des routes source est la clé permettant aux fournisseurs de travailler avec les hôtes qui implémentent les nouvelles capacités IPv6 comme la sélection de fournisseur et les adresses étendues.

Publication de routeur

Sur des liens compatibles multicast et des liens point à point, chaque routeur envoie régulièrement un paquet de publication de routeur au groupe multicast pour lui annoncer sa disponibilité. Un hôte reçoit des publications de routeur de la totalité des routeurs, constituant une liste des routeurs par défaut. Les routeurs génèrent des publications de routeur de façon suffisamment fréquente pour permettre aux hôtes d'être avertis de leur présence en quelques minutes. Cependant, les routeurs n'effectuent pas de publications à une fréquence suffisante

pour se fier à une absence de publication permettant de détecter une défaillance de routeur. Un algorithme de détection séparé qui détermine l'inaccessibilité de voisin fournit la détection de défaillance.

Préfixes de publication de routeurs

Les publications de routeur contiennent une liste de préfixes de sous-réseau utilisés pour déterminer si un hôte se trouve sur le même lien que le routeur. La liste de préfixes est également utilisée pour la configuration d'adresses autonomes. Les indicateurs associés aux préfixes spécifient les utilisations spécifiques d'un préfixe particulier. Les hôtes utilisent les préfixes sur liaison publiés afin de constituer et de maintenir une liste utilisée pour décider lorsque la destination d'un paquet se trouve sur la liaison ou au-delà d'un routeur. Une destination peut se trouver sur une liaison même si celle-ci n'est couverte par aucun préfixe sur liaison publié. Dans de tels cas, un routeur peut envoyer une redirection. La redirection informe l'expéditeur que la destination est un voisin.

Les publications de routeur et les indicateurs par préfixe permettent aux routeurs d'informer des hôtes de la méthode qu'ils doivent utiliser pour effectuer une configuration automatique d'adresse sans état.

Messages de publication de routeurs

Les messages de publication de routeur contiennent également des paramètres Internet, comme la limite de saut, que les hôtes devraient utiliser dans des paquets entrants. Les messages de publication de routeur peuvent également (facultativement) contenir des paramètres de liens, comme le lien MTU. Cette fonctionnalité permet l'administration centralisée des paramètres critiques. Les paramètres peuvent être définis sur des routeurs et propagés automatiquement à tous les hôtes qui y sont connectés.

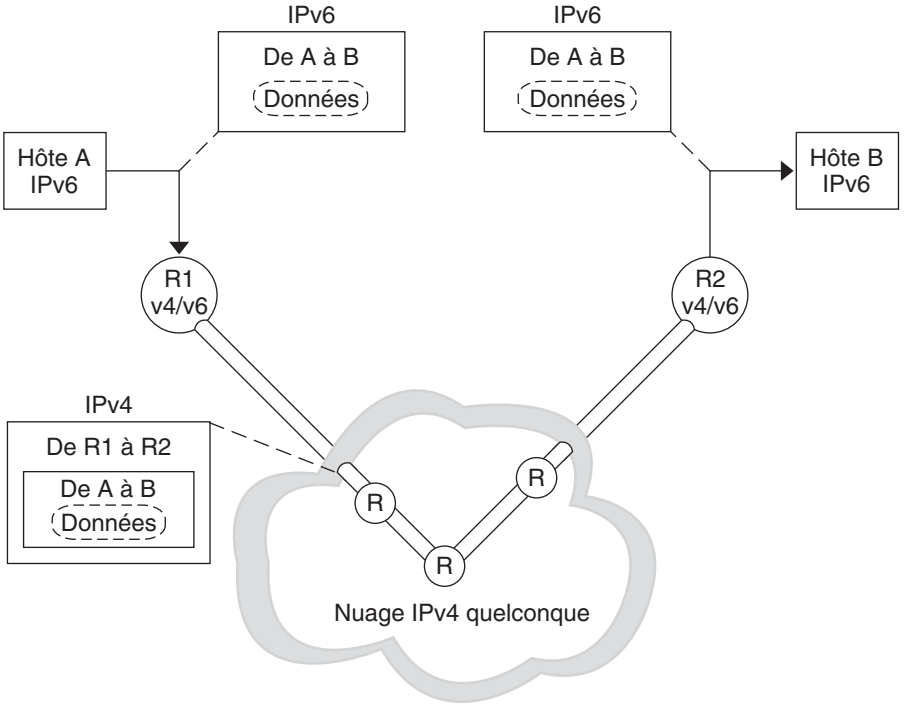
Les nœuds effectuent la résolution d'adresses par l'envoi de sollicitation de voisin à un groupe multicast, demandant au nœud cible de retourner son adresse de couche liaison. Les messages de sollicitation de voisin multicast sont envoyés à l'adresse de nœud multicast demandée de l'adresse cible. La cible retourne son adresse de couche liaison dans un message de publication d'un voisin unicast. Une paire de paquets de requête-réponse unique est suffisante pour permettre à l'initiateur et à la cible de résoudre les adresses de couche liaison de l'un et de l'autre. L'initiateur inclut son adresse de couche liaison dans la sollicitation de voisin.

Tunnels IPv6

Pour réduire toute dépendance possible d'un site IPv4/IPv6 double pile, il n'est pas nécessaire que tous les routeurs situés dans le chemin entre deux nœuds IPv6 soient compatibles avec IPv6. Le mécanisme prenant une telle configuration de réseau en charge s'appelle *mise en tunnel*. Les paquets IPv6 sont placés dans des paquets IPv4, qui sont ensuite acheminés via les

routeurs IPv4. L'illustration suivante représente le mécanisme de mise en tunnel via des routeurs IPv4. Ces routeurs sont signalés sur l'illustration par un R.

FIGURE 11–5 Mécanisme de mise en tunnel IPv6



L'implémentation du protocole IPv6 sous Oracle Solaris comprend deux types de mécanismes de mise en tunnel :

- tunnels configurés entre deux routeurs, comme sur la Figure 11–5 ;
- tunnels automatiques se terminant aux hôtes de points d'extrémité.

Un tunnel configuré est actuellement utilisé sur Internet à d'autres fins, par exemple, sur le MBONE, la dorsale multidiffusion IPv4. Fonctionnellement, le tunnel se compose de deux routeurs configurés de sorte à disposer d'une liaison virtuelle point à point entre les deux routeurs sur le réseau IPv4. Ce type de tunnel est susceptible d'être utilisé à l'avenir sur certaines parties d'Internet.

Les tunnels automatiques doivent disposer d'adresses compatibles avec IPv4. Les tunnels automatiques permettent de connecter des nœuds IPv6 en cas d'indisponibilité des routeurs IPv6. Ces tunnels peuvent provenir d'un hôte double pile ou d'un routeur double pile, grâce à la configuration d'une interface réseau de mise en tunnel automatique. Ces tunnels se terminent

toujours sur l'hôte double pile. Ils déterminent de façon dynamique l'adresse IPv4 de destination, qui correspond au point d'extrémité du tunnel, en extrayant l'adresse à partir de l'adresse de destination compatible IPv4.

Tunnels configurés

Le format des interfaces de création de tunnel est le suivant :

`ip.tun` *ppa*

ppa correspond au point de connexion physique.

Lors du démarrage du système, le module de création de tunnel (`tun`) se place, via la commande `ifconfig`, sur l'IP afin de créer une interface virtuelle. Pour effectuer ce déplacement, vous devez créer le fichier `hostname6.*` adéquat.

Par exemple, pour créer un tunnel afin d'encapsuler les paquets IPv6 sur un réseau IPv4, IPv6 sur IPv4, créez le fichier suivant :

`/etc/hostname6.ip.tun0`

Le contenu de ce fichier est transféré à `ifconfig` une fois le montage des interfaces terminé. Le contenu correspond aux paramètres nécessaires pour configurer un tunnel point à point.

EXEMPLE 11–11 Fichier `hostname6.ip.tun0` pour un tunnel IPv6 sur IPv4

Vous trouverez ci-dessous un exemple d'entrées dans le fichier `hostname6.ip.tun0` :

```
tsrc 10.10.10.23 tdst 172.16.7.19 up
addif 2001:db8:3b4c:1:5678:5678::2 up
```

Dans cet exemple, la source IPv4 et les adresses de destination sont utilisées comme des jetons afin de configurer automatiquement des adresses IPv6 lien-local. Ces adresses correspondent à la source et à la destination de l'interface `ip.tun0`. Deux interfaces sont configurées. L'interface `ip.tun0` est configurée. Une interface logique, `ip.tun0:1`, est également configurée. Les adresses source et de destination IPv6 de l'interface logique sont spécifiées à l'aide de la commande `addif`.

Le contenu de ces fichiers de configuration est passé à `ifconfig` sans aucune modification lors du démarrage système en mode multiutilisateur. Les entrées de l'Exemple 11–11 sont équivalentes à ce qui suit :

```
# ifconfig ip.tun0 inet6 plumb
# ifconfig ip.tun0 inet6 tsrc 10.0.0.23 tdst 172.16.7.19 up
# ifconfig ip.tun0 inet6 addif 2001:db8:3b4c:1:5678:5678::2 up
```

Vous trouverez ci-dessous la sortie de `ifconfig -a` pour ce tunnel.

```
ip.tun0: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,
  NONUD,IPv6> mtu 1480 index 6
        inet tunnel src 10.0.0.23  tunnel dst 172.16.7.19
        inet6 fe80::c0a8:6417/10 --> fe80::c0a8:713
ip.tun0:1: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,NONUD,IPv6> mtu 1480
  index 5
        inet6 2001:db8:3b4c:1:5678:5678::2
```

Vous pouvez configurer d'autres interfaces logiques en ajoutant des lignes au fichier de configuration à l'aide de la syntaxe suivante :

```
addif IPv6-source IPv6-destination up
```

Remarque – Lorsque l'une des extrémités du tunnel correspond à un routeur IPv6 qui publie un ou plusieurs préfixes sur le tunnel, il n'est pas nécessaire de disposer des commandes `addif` dans les fichiers de configuration de tunnel. Seul `tsrc` et `tdst` pourraient être nécessaires, car toutes les autres adresses sont configurées automatiquement.

Dans certains cas, les adresses lien-local source et de destination doivent être configurées manuellement pour un tunnel particulier. Modifiez la première ligne du fichier de configuration afin d'inclure ces adresses lien-local. La ligne suivante est un exemple :

```
tsrc 10.0.0.23 tdst 172.16.7.19 fe80::1/10 fe80::2 up
```

Notez que l'adresse lien-local source dispose d'une longueur de préfixe de 10. Dans cet exemple, l'interface `ip.tun0` ressemble à ce qui suit :

```
ip.tun0: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,NONUD,IPv6> mtu 1480
index 6
        inet tunnel src 10.0.0.23  tunnel dst 172.16.7.19
        inet6 fe80::1/10 --> fe80::2
```

Pour créer un tunnel afin d'encapsuler les paquets IPv6 sur un réseau IPv6, IPv6 sur IPv6, créez le fichier suivant :

```
/etc/hostname6.ip6.tun0
```

EXEMPLE 11–12 Fichier `hostname6.ip6.tun0` pour un tunnel IPv6 sur IPv6

L'exemple suivant correspond à des entrées du fichier `hostname6.ip6.tun0` pour une encapsulation IPv6 sur un réseau IPv6 :

```
tsrc 2001:db8:3b4c:114:a00:20ff:fe72:668c
        tdst 2001:db8:15fa:25:a00:20ff:fe9b:a1c3
fe80::4 fe80::61 up
```

Pour créer un tunnel afin d'encapsuler les paquets IPv4 sur un réseau IPv6, IPv4 sur IPv6, créez le fichier suivant :

```
/etc/hostname.ip6.tun0
```

EXEMPLE 11–13 Fichier `hostname.ip6.tun0` pour un tunnel IPv4 sur IPv6

L'exemple suivant correspond à des entrées du fichier `hostname.ip6.tun0` pour une encapsulation IPv4 sur un réseau IPv6 :

```
tsrc 2001:db8:3b4c:114:a00:20ff:fe72:668c
         tdst 2001:db8:15fa:25:a00:20ff:fe9b:a1c3
10.0.0.4 10.0.0.61 up
```

Pour créer un tunnel afin d'encapsuler les paquets IPv4 sur un réseau IPv4, IPv4 sur IPv4, créez le nom de fichier suivant :

```
/etc/hostname.ip.tun0
```

EXEMPLE 11–14 Fichier `hostname.ip.tun0` pour un tunnel IPv4 sur IPv4

L'exemple suivant correspond à des entrées du fichier `hostname.ip.tun0` pour une encapsulation IPv4 sur un réseau IPv4 :

```
tsrc 172.16.86.158 tdst 192.168.86.122
10.0.0.4 10.0.0.61 up
```

Pour obtenir des informations spécifiques sur `tun`, reportez-vous à la page de manuel `tun(7M)`. Pour obtenir une description générale des concepts de création de tunnel lors de la transition vers le protocole IPv6, reportez-vous à la section “Présentation des tunnels IPv6” à la page 85. Pour obtenir une description des procédures de configuration de tunnels, reportez-vous à la section “Tâches de configuration de tunnels pour la prise en charge d'IPv6 (liste des tâches)” à la page 191.

Tunnels automatiques 6to4

Dans Oracle Solaris, la création de tunnels 6to4 constitue la méthode temporaire recommandée pour effectuer la transition entre les adressages IPv4 et IPv6. Les tunnels 6to4 permettent aux sites IPv6 isolés de communiquer, par le biais d'un tunnel automatique, avec un réseau IPv4 ne prenant pas en charge le protocole IPv6. Pour utiliser des tunnels 6to4, vous devez configurer un routeur de bordure sur le réseau IPv6 en tant que point d'extrémité du tunnel 6to4 automatique. Par la suite, le routeur 6to4 peut participer à un tunnel vers un autre site 6to4 ou vers un site IPv6 natif et non-6to4, le cas échéant.

Cette section fournit des références sur les rubriques concernant les tunnels 6to4 :

- Topologie d'un tunnel 6to4
- Adressage 6to4 (et format de publication)
- Description du flux de paquets dans un tunnel 6to4
- Topologie d'un tunnel reliant un routeur 6to4 et un routeur relais 6to4
- Informations importantes pour la configuration de la prise en charge d'un routeur relais 6to4

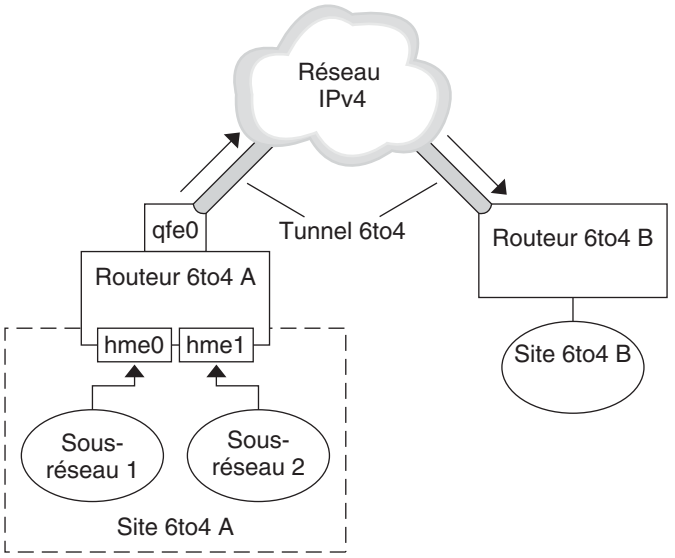
Le tableau suivant décrit les autres tâches permettant de configurer des tunnels 6to4 et les ressources permettant obtenir d'autres informations utiles.

Tâche ou détail	Référence
Configuration d'un tunnel 6to4	“Procédure de configuration d'un tunnel 6to4” à la page 195
RFC lié aux 6to4	RFC 3056, "Connection of IPv6 Domains via IPv4 Clouds" (`http://www.ietf.org/rfc/rfc3056.txt`)
Informations détaillées sur la commande `6to4relay` (prise en charge des tunnels vers un routeur relais 6to4)	`6to4relay`(1M)
Problèmes de sécurité avec 6to4	Security Considerations for 6to4 (`http://www.ietf.org/rfc/rfc3964.txt`)

Topologie d'un tunnel 6to4

Un tunnel 6to4 offre la connexion IPv6 à tous les sites 6to4, quel que soit leur emplacement. De même, le tunnel offre un lien à l'ensemble des sites IPv6, notamment l'Internet IPv6 natif, à condition d'être configuré pour la transmission vers un routeur relais. La figure suivante illustre un tunnel 6to4 connectant des sites 6to4.

FIGURE 11–6 Tunnel entre deux sites 6to4



La figure illustre deux réseaux 6to4 isolés (Site A et Site B). Chaque site possède un routeur configuré avec une connexion externe à un réseau IPv4. Un tunnel 6to4 à l'échelle du réseau IPv4 offre une connexion entre sites 6to4.

Pour convertir un site IPv6 en site 6to4, vous devez configurer au moins une interface de routeur prenant en charge 6to4. Cette interface doit assurer la connexion externe au réseau IPv4. L'adresse que vous configurez sur `qfe0` doit être globale et unique. Sur cette figure, l'interface du routeur A (`qfe0`) connecte le site A au réseau IPv4. L'interface `qfe0` doit déjà être configurée avec une adresse IPv4 pour que vous puissiez définir `qfe0` en tant que pseudointerface 6to4.

Dans cet exemple, le site A 6to4 se compose de deux sous-réseaux connectés aux interfaces `hme0` et `hme1` du routeur A. Dès que les hôtes IPv6 des sous-réseaux du site A reçoivent la publication du routeur A, ils sont automatiquement reconfigurés sur les adresses 6to4 dérivées.

Le site B est un autre site 6to4 isolé. Pour recevoir correctement le trafic du site A, un routeur de bordure sur le site B doit être configuré pour prendre en charge 6to4. Dans le cas contraire, le routeur ne reconnaît pas les paquets reçus du site A et les abandonne.

Description du flux de paquets dans un tunnel 6to4

Cette section décrit le flux de paquets allant d'un hôte sur un site 6to4 à un autre hôte sur un site 6to4 distant. Ce scénario nécessite la topologie illustrée sur la Figure 11–6. Cela suppose également de configurer au préalable les routeurs et les hôtes 6to4.

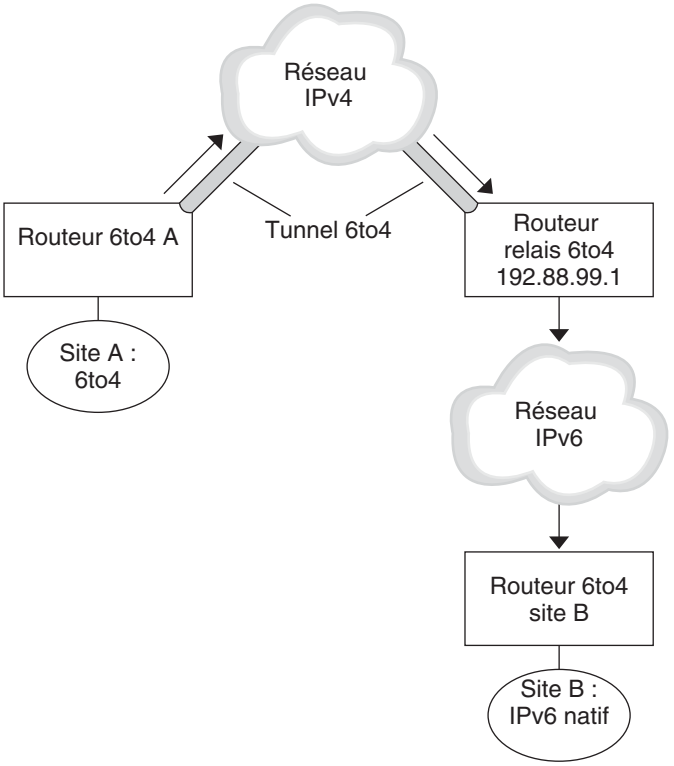
1. Un hôte du sous-réseau 1 appartenant au site 6to4 A envoie une transmission à un hôte du site 6to4 B. Chaque en-tête de paquet possède des adresses 6to4 dérivées source et cible.

2. Le routeur du site A encapsule chaque paquet 6to4 dans un en-tête IPv4. Dans ce processus, le routeur définit l'adresse cible IPv4 de l'en-tête d'encapsulation sur l'adresse du routeur du site B. L'adresse cible IPv6 de chaque paquet IPv6 transmis via l'interface du tunnel contient également l'adresse cible IPv4. Ainsi, le routeur est en mesure de déterminer l'adresse cible IPv4 définie sur l'en-tête d'encapsulation. Ensuite, il utilise la procédure de routage IPv4 standard pour transmettre le paquet sur le réseau IPv4.
3. Tout routeur IPv4 rencontré par les paquets utilise l'adresse IPv4 cible de ces derniers pour la transmission. Cette adresse constitue l'adresse IPv4 globale et unique de l'interface du routeur B, qui sert également de pseudointerface 6to4.
4. Les paquets du site A arrivent sur le routeur B qui les décapsule en paquets IPv6 à partir de l'en-tête IPv4.
5. Le routeur B se sert alors de l'adresse cible des paquets IPv6 pour transmettre ces derniers à l'hôte destinataire sur le site B.

Informations importantes pour la création de tunnels vers un routeur relais 6to4

Les routeurs relais 6to4 fonctionnent en tant que points d'extrémité des tunnels reliant des routeurs 6to4 à des réseaux IPv6 natifs, non 6to4. Les routeurs relais constituent essentiellement des ponts entre le site 6to4 et les sites IPv6 natifs. Ce type de routeur risque de ne pas garantir la sécurité du réseau ; c'est pourquoi il n'est pas pris en charge par Oracle Solaris. Cependant, si votre site nécessite un tel tunnel, vous pouvez exécuter la commande `6to4relay` pour créer le type de tunnel suivant.

FIGURE 11–7 Tunnel entre un site 6to4 et un routeur relais 6to4



Sur la Figure 11–7, le site A (6to4) doit communiquer avec un nœud du site B (IPv6 natif). L'illustration indique la trajectoire du trafic entre le site A et le site B à travers un tunnel 6to4 créé sur le réseau IPv4. Le tunnel dispose d'un routeur A 6to4 et d'un routeur relais 6to4 à chaque extrémité. Au-delà du routeur 6to4 se trouve le réseau IPv6 auquel le site B IPv6 est connecté.

Flux de paquets entre un site 6to4 et un site IPv6 natif

Cette section décrit le flux de paquets se déplaçant d'un site 6to4 vers un site IPv6 natif. Ce scénario nécessite la topologie illustrée sur la Figure 11–7.

1. Un hôte résidant sur le site A (6to4) envoie une transmission à un hôte de destination appartenant au site B (IPv6 natif). Chaque en-tête de paquet possède une adresse 6to4 dérivée en tant qu'adresse source. L'adresse de destination correspond à une adresse IPv6 standard.

2. Le routeur 6to4 du site A encapsule chaque paquet dans un en-tête IPv4, dont la destination correspond à l'adresse IPv4 du routeur relais 6to4. Ensuite, il utilise la procédure de routage IPv4 standard pour transmettre le paquet sur le réseau IPv4. Tout routeur IPv4 rencontré par les paquets envoie ceux-ci vers le routeur relais 6to4.
3. Le routeur relais 6to4 anycast le plus proche (physiquement) du site A récupère les paquets destinés au groupe anycast `192.88.99.1`.

Remarque – Les routeurs relais 6to4 faisant partie du groupe anycast de routeurs relais 6to4 possèdent l'adresse IP `192.88.99.1`. Cette adresse anycast constitue l'adresse par défaut des routeurs relais 6to4. Si vous avez besoin d'un routeur relais 6to4 spécifique, vous pouvez supprimer celui par défaut et spécifier l'adresse IPv4 du routeur en question.

---

4. Ce routeur relais décapsule ensuite l'en-tête IPv4 des paquets 6to4, dévoilant l'adresse de destination sur le réseau IPv6.
5. Finalement, il envoie ces paquets IPv6 sur le réseau IPv6, où un routeur du site B les récupère et les envoie au noeud IPv6 de destination.

Extensions IPv6 de services d'assignation de noms Oracle Solaris

Cette section décrit les modifications en matière d'attribution de noms introduites par l'implémentation d'IPv6. Vous pouvez stocker les adresses IPv6 dans les fichiers de services d'assignation de noms, NIS, LDAP, DNS ou ou tout autre fichier Oracle Solaris de votre choix. Vous pouvez également utiliser le protocole NIS à travers les transports RPC IPv6 pour la récupération de données NIS.

Extensions DNS pour IPv6

Un enregistrement de ressources spécifique IPv6, l'enregistrement de ressource AAAA, a été spécifié dans le document RFC 1886 *DNS Extensions to Support IP Version 6*. Cet enregistrement AAAA mappe un nom d'hôte en une adresse IPv6 de 128 bits. L'enregistrement PTR est toujours utilisé avec IPv6 pour mapper les adresses IP en noms d'hôtes. Les 32 quartets de d'adresse 128 bits sont inversés pour une adresse IPv6. Chaque quartet est converti dans sa valeur hexadécimale ASCII correspondante. Ensuite, `ip6.int` est joint.

Modifications apportées au fichier `nsswitch.conf`

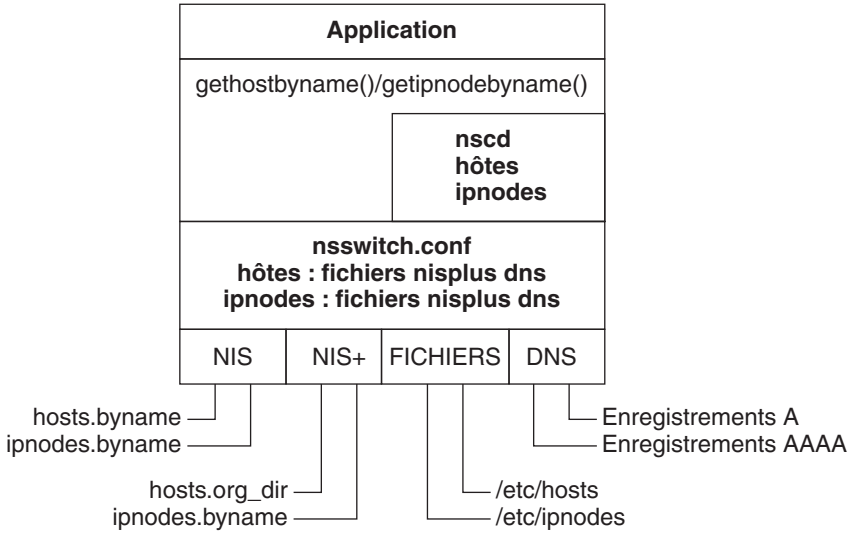
Pour Solaris 10 11/06 et versions antérieures, en plus de la capacité de recherche d'adresses IPv6 via `/etc/inet/ipnodes` , la prise en charge IPv6 a été ajoutée aux services d'attribution de noms NIS, LDAP et DNS. Par conséquent, le fichier `nsswitch.conf` a été modifié afin de prendre les recherches IPv6 en charge.

```
hosts:  files dns nisplus [NOTFOUND=return]
ipnodes: files dns nisplus [NOTFOUND=return]
```

Remarque – Avant de modifier le fichier `/etc/nsswitch.conf` pour rechercher `ipnodes` dans plusieurs services d'attribution de noms, renseignez ces bases de données `ipnodes` avec des adresses IPv4 et IPv6. Autrement, des retards inutiles peuvent entraîner une résolution des adresses hôtes, notamment des retards de durée d'initialisation.

Le diagramme suivant illustre la nouvelle relation entre le fichier `nsswitch.conf` et les nouvelles bases de données de services d'attribution de noms utilisant les commandes `gethostbyname` et `getipnodebyname`. Les nouveaux éléments sont en italique. La commande `gethostbyname` vérifie uniquement les adresses IPv4 stockées dans `/etc/inet/hosts`. Dans Solaris 10 11/06 et versions antérieures, la commande `getipnodebyname` consulte la base de données spécifiée dans l'entrée `ipnodes` du fichier `nsswitch.conf`. En cas d'échec de la recherche, la commande vérifie la base de données spécifiée dans l'entrée `hosts` du fichier `nsswitch.conf`.

FIGURE 11–8 Relation entre `nsswitch.conf` et les services d'attribution de noms



Pour plus d'informations sur les services de noms, reportez-vous au document *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Modifications apportées aux commandes de services d'attribution de noms

Pour la prise en charge d'IPv6, vous pouvez rechercher les adresses IPv6 avec les commandes existantes des services d'attribution de noms. Par exemple, la commande `ypmatch` fonctionne avec les nouveaux mappages NIS. La commande `nslookup` peut rechercher les nouveaux enregistrements AAAA dans DNS.

Prise en charge IPv6 de NFS et RPC

Les logiciels NFS et RPC (Remote Procedure Call, appel de procédure distant) prennent IPv6 en charge de façon totalement fluide. Les commandes existantes relatives aux services NFS restent inchangées. Il est également possible d'exécuter la plupart des applications RPC sur IPv6 sans aucune modification. Certaines applications RPC avancées de reconnaissance d'acheminement peuvent nécessiter une mise à jour.

Prise en charge d'IPv6 sur ATM

Oracle Solaris prend en charge le protocole IPv6 sur des ATM, des PVC (Permanent Virtual Circuits, circuits virtuels permanents) et des SVC (Switched Virtual Circuits, circuits virtuels à commutation) statiques.

PARTIE III

DHCP

Cette partie traite des concepts propres au protocole DHCP (Dynamic Host Configuration Protocol) et décrit les tâches nécessaires à la planification, à la configuration, à l'administration et au dépannage du service DHCP.

◆ ◆ ◆ CHAPITRE 12

À propos de DHCP (présentation)

Ce chapitre vous propose de découvrir le protocole DHCP (Dynamic Host Configuration Protocol) et les concepts à la base de ce protocole. Il décrit également les avantages que présente le protocole DHCP pour votre réseau.

Le présent chapitre contient les informations suivantes :

À propos du protocole DHCP

Le protocole DHCP permet de procéder automatiquement à la configuration des systèmes hôtes d'un réseau TCP/IP au moment de leur initialisation. Le protocole DHCP utilise un mécanisme client/serveur. Les serveurs stockent et gèrent les informations de configuration des clients et les fournissent à leur demande. Ces informations comprennent l'adresse IP du client ainsi que des données sur les services réseau accessibles au client.

DHCP est l'évolution d'un protocole précédent, BOOTP, conçu pour l'initialisation des systèmes sur un réseau TCP/IP. Il utilise le même format que le protocole BOOTP pour les messages échangés entre le client et le serveur. À la différence des messages BOOTP, les messages DHCP peuvent contenir des données de configuration du réseau pour le client.

L'un des avantages majeurs du protocole DHCP est sa capacité à gérer les affectations d'adresses IP au moyen de baux. L'intérêt des *baux* est de pouvoir récupérer les adresses IP lorsqu'elles ne sont plus utilisées afin de les attribuer à d'autres clients. Cela permet à un site DHCP d'utiliser un pool d'adresses IP plus petit que celui qui serait nécessaire si tous les clients possédaient une adresse IP permanente.

Intérêt du protocole DHCP

Le service DHCP vous fait gagner un temps précieux en prenant à sa charge un certain nombre de tâches liées à la configuration d'un réseau TCP/IP et à l'administration quotidienne de ce réseau. Notez que dans l'implémentation Oracle Solaris, DHCP fonctionne uniquement avec IPv4.

DHCP offre les avantages suivants :

- **Gestion des adresses IP** – L'un des principaux atouts de DHCP est effectivement de faciliter l'administration des adresses IP. Dans un réseau sans protocole DHCP, vous devez allouer manuellement les adresses IP. Il faut attribuer des adresses IP uniques à chaque client et configurer chacun d'eux individuellement. Si un client est transféré sur un autre réseau, il faut alors effectuer manuellement les modifications se rapportant à ce client. Par contre, si vous activez le protocole DHCP, le serveur DHCP gère et assigne lui-même les adresses IP sans que l'administrateur ait à intervenir. Les clients peuvent être placés sur d'autres sous-réseaux sans nécessiter de reconfiguration manuelle, car ils sont capables d'obtenir d'un serveur DHCP les informations client correspondant au nouveau réseau.
- **Configuration centralisée des clients du réseau** – Vous pouvez créer une configuration sur mesure pour certains clients ou pour certains types de client. Les données de configuration sont stockées au même endroit : à l'intérieur du magasin de données DHCP. Vous n'avez pas besoin de vous connecter à un client pour changer sa configuration. Il est possible de modifier plusieurs clients à la fois en changeant simplement les informations dans le magasin de données.
- **Prise en charge des clients BOOTP** – Les serveurs BOOTP et les serveurs DHCP se chargent d'écouter et de répondre aux messages diffusés par les clients. Le serveur DHCP peut répondre aussi bien aux requêtes des clients BOOTP qu'à celles des clients DHCP. Les clients BOOTP reçoivent une adresse IP et les informations nécessaires au démarrage à partir d'un serveur.
- **Prise en charge des clients locaux et distants** – Le protocole BOOTP permet de relayer les messages d'un réseau à un autre. Le protocole DHCP utilise cette fonctionnalité BOOTP de différentes manières. La plupart des routeurs de réseau peuvent être configurés comme des agents de relais BOOTP dans le but de transmettre des requêtes BOOTP à des serveurs ne figurant pas sur le réseau du client. Les requêtes DHCP peuvent être relayées de la même manière, dans la mesure où le routeur ne fait aucune distinction entre les requêtes DHCP et les requêtes BOOTP. Il est également possible de configurer le serveur DHCP de sorte qu'il se comporte comme un agent de relais BOOTP, lorsqu'un routeur compatible avec la fonctionnalité de relais BOOTP n'est pas disponible.
- **Initialisation à partir du réseau** – Les clients peuvent utiliser le protocole DHCP pour obtenir les informations nécessaires à un démarrage à partir d'un serveur du réseau, au lieu de faire appel au protocole RARP (Reverse Address Resolution Protocol) et au fichier `bootparams`. Le serveur DHCP peut donner au client tous les renseignements dont il a besoin pour fonctionner : adresse IP, serveur d'initialisation et données de configuration du réseau. Comme les requêtes DHCP peuvent être relayées d'un sous-réseau à un autre, vous

pouvez vous contenter de déployer un nombre moins important de serveurs d'initialisation sur votre réseau lorsque vous avez recours au service d'initialisation de réseau DHCP. L'initialisation RARP exige un serveur d'initialisation par sous-réseau.

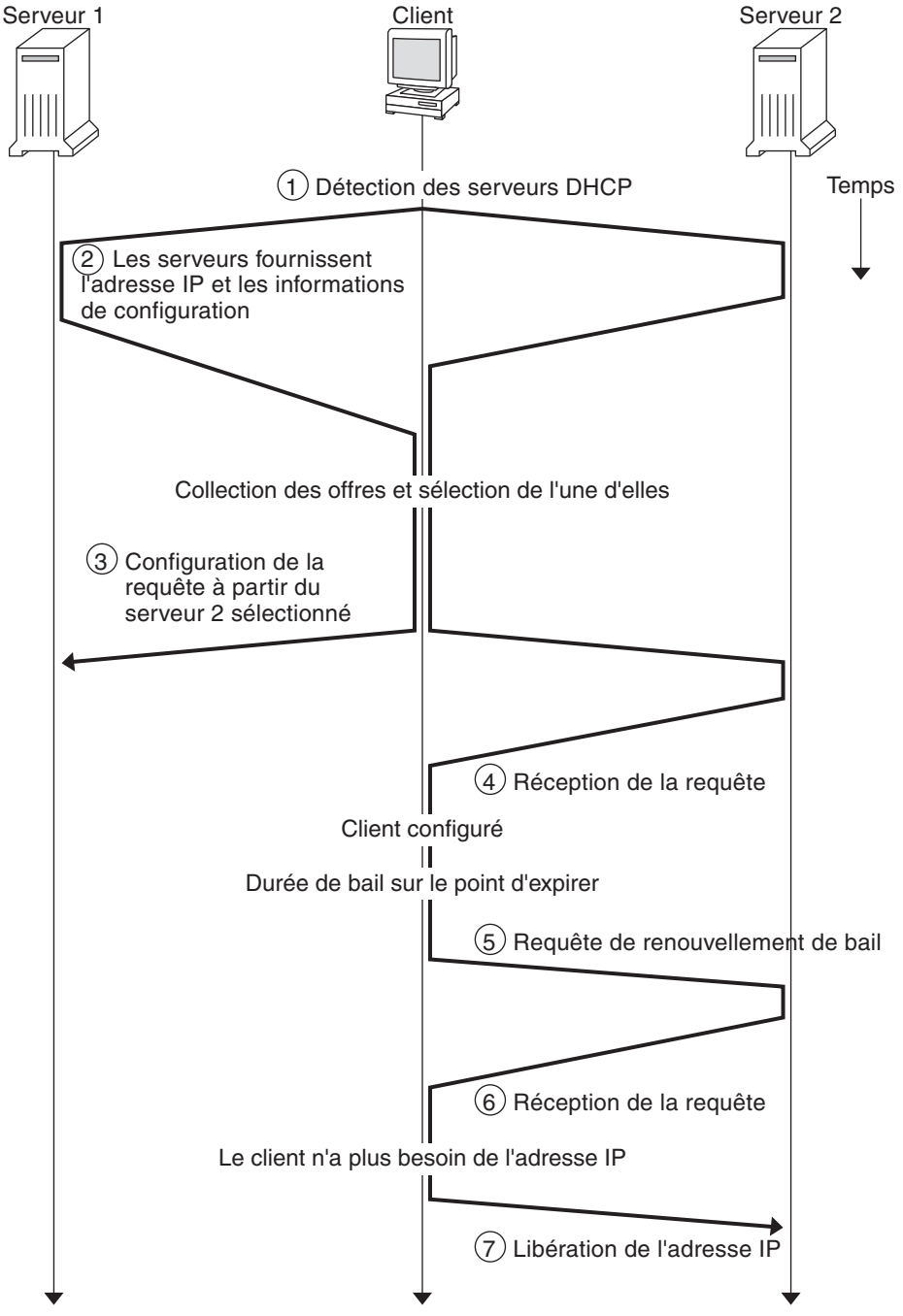
- **Gestion de réseaux de grande taille** – DHCP peut être exploité par des réseaux comptant des millions de clients DHCP. Le serveur DHCP utilise la technique de multithreading pour traiter plusieurs requêtes client à la fois. Il gère également les magasins de données, c'est-à-dire des espaces de stockage optimisés pour traiter de grandes quantités de données. L'accès aux magasins de données est contrôlé par des modules de traitement indépendants. Grâce aux magasins de données, vous êtes libre de travailler avec toutes les bases de données qui vous intéressent.

Mode de fonctionnement du protocole DHCP

Vous devez commencer par installer et configurer le serveur DHCP. Lors de la phase de configuration, il est nécessaire de fournir un certain nombre d'informations au sujet du réseau avec lequel les clients vont communiquer. Une fois ces précisions apportées, les clients auront la possibilité de demander et de recevoir des informations spécifiques au réseau.

Le schéma ci-après montre comment s'enchaînent les différents événements liés au service DHCP. Les nombres figurant dans les cercles correspondent aux étapes numérotées de la description suivant le schéma.

FIGURE 12–1 Séquence des événements pour le service DHCP



Le schéma précédent présente les étapes suivantes :

1. Le client identifie un serveur DHCP en diffusant un *message de détection* à l'adresse de diffusion limitée (`255.255.255.255`) sur le sous-réseau local. Si un routeur est présent et configuré pour agir comme un agent de relais BOOTP, la requête est transmise à d'autres serveurs DHCP sur d'autres sous-réseaux. Le *message de diffusion* du client comprend son identifiant unique (ID) lequel, dans le cadre de l'implémentation DHCP dans Oracle Solaris, est dérivé de l'adresse MAC (Media Access Control) du client. Sur un réseau Ethernet, l'adresse MAC est identique à l'adresse Ethernet.

   Les serveurs DHCP qui reçoivent le message de détection sont capables d'identifier le réseau du client en effectuant l'analyse suivante :

   - Sur quelle interface réseau la requête est-elle parvenue ? Le serveur peut en déduire que le client appartient au réseau auquel l'interface est connectée ou que le client utilise un agent de relais BOOTP relié à ce réseau.
   - La requête contient-elle l'adresse IP d'un agent de relais BOOTP ? Lorsqu'une requête transite par un agent de relais, celui-ci insère son adresse dans l'en-tête de la requête. Lorsque le serveur détecte une *adresse d'un agent de relais*, il sait que la portion réseau de l'adresse désigne l'adresse réseau du client dans la mesure où l'agent de relais doit obligatoirement être connecté au réseau du client.
   - Le réseau du client comporte-t-il des sous-réseaux ? Le serveur consulte la table `netmasks` pour identifier le masque de sous-réseau utilisé sur le réseau désigné par l'adresse de l'agent de relais ou par l'adresse de l'interface réseau ayant reçu la requête. Dès que le serveur connaît cette information, il peut déterminer la portion de l'adresse réseau correspondant à la portion de l'hôte, puis sélectionner une adresse IP qui convient pour le client. Pour plus d'informations au sujet des `netmasks`, reportez-vous à la page de manuel `netmasks(4)`.
2. Une fois que les serveurs DHCP ont réussi à identifier le réseau du client, ils sélectionnent une adresse IP appropriée et s'assurent qu'elle est libre. Ils répondent ensuite au client en diffusant un *message d'offre*. Ce message contient l'adresse IP sélectionnée et des informations au sujet des services pouvant être configurés pour le client. Chaque serveur réserve provisoirement l'adresse IP proposée jusqu'à ce que le client choisisse ou non d'accepter l'adresse IP en question.
3. Le client sélectionne la meilleure offre en fonction du nombre et du type de services proposés. Il diffuse alors une requête indiquant l'adresse IP du serveur ayant fait la meilleure offre. Tous les serveurs DHCP ayant répondu savent ainsi que le client a fait son choix. Les serveurs non sélectionnés peuvent dès lors annuler la réservation des adresses IP proposées.
4. Le serveur sélectionné alloue l'adresse IP au client et stocke cette information dans le magasin de données DHCP. Il adresse également un accusé de réception (message ACK) au client. L'*accusé de réception* contient les paramètres de configuration du réseau pour le client. Le client se sert de l'utilitaire `ping` pour tester l'adresse IP et s'assurer qu'elle n'est utilisée par aucun autre système. Il continue ensuite la procédure d'initialisation afin de se connecter au réseau.

5. Le client contrôle la durée du bail. Au bout d'un certain temps, il envoie un nouveau message au serveur sélectionné pour lui demander d'augmenter la durée du bail.
6. Le serveur DHCP recevant la requête prolonge le bail à condition que le bail soit conforme à la stratégie de location définie par l'administrateur. Si le serveur ne répond pas dans les 20 secondes, le client diffuse une requête de sorte que l'un des autres serveurs DHCP prolonge son bail.
7. Lorsque le client n'a plus besoin de l'adresse IP, il prévient le serveur que l'adresse IP a été libérée. Cette notification peut survenir lors d'un arrêt méthodique ou être effectuée de façon manuelle.

Le serveur DHCP

Le serveur DHCP s'exécute comme un démon d'Oracle Solaris sur un système hôte. Il remplit deux fonctions de base :

- **Gérer les adresses IP** – Le serveur DHCP gère une plage d'adresses IP et les alloue aux clients de façon permanente ou temporaire. Il utilise le mécanisme de bail pour déterminer la durée d'utilisation permise d'une adresse non permanente. Lorsque l'adresse n'est plus utilisée, elle reprend sa place dans le pool d'adresses sous le contrôle du serveur et peut être réallouée à un autre client. Le serveur tient à jour les informations relatives à l'allocation des adresses IP aux clients dans ses tables de réseau DHCP, afin d'éviter tout conflit d'utilisation des adresses.
- **Fournir des données de configuration du réseau aux clients** – Le serveur ne se contente pas d'attribuer des adresses IP. Il fournit également diverses informations relatives à la configuration du réseau (nom d'hôte, adresse de diffusion, masque de sous-réseau, passerelle par défaut, service de noms et bien plus encore). Ces informations proviennent directement de la base de données `dhcptab` du serveur.

Le serveur DHCP peut également être configuré pour jouer les rôles supplémentaires suivants :

- **Répondre aux requêtes de clients BOOTP** – Le serveur écoute les diffusions des clients BOOTP lorsqu'ils découvrent un serveur BOOTP et leur fournit une adresse IP ainsi que des paramètres d'initialisation. Ces informations doivent être configurées de façon statique par un administrateur. Le serveur DHCP peut faire office à la fois de serveur BOOTP et de serveur DHCP.
- **Relayer des requêtes** – Le serveur renvoie les requêtes BOOTP et DHCP vers les serveurs appropriés sur d'autres sous-réseaux. Il lui est impossible d'assurer un service DHCP ou BOOTP lorsqu'il est configuré comme agent de relais BOOTP.
- **Permettre l'initialisation des clients DHCP sur le réseau** – Le serveur est en mesure de donner aux clients DHCP les informations dont ils besoin pour démarrer sur le réseau : adresse IP, paramètres d'initialisation et données de configuration du réseau. Il peut également leur fournir les renseignements nécessaires en vue de leur initialisation et de leur installation sur un réseau de grande taille (WAN).

- **Mettre à jour les tables DNS pour les clients fournissant un nom d'hôte** – Si la demande de service DHCP des clients comporte une option et une valeur `Hostname` , le serveur peut essayer de mettre à jour le service DNS à leur place.

Administration du serveur DHCP

En tant que superutilisateur, vous avez la possibilité de démarrer, arrêter et configurer le serveur DHCP à l'aide du gestionnaire DHCP ou des utilitaires de ligne de commande décrits à la section “Utilitaires de ligne de commande DHCP” à la page 314. En règle générale, le serveur DHCP est configuré pour démarrer automatiquement lors de l'initialisation du système et pour s'interrompre lors de l'arrêt du système. Il n'est pas utile de démarrer et d'arrêter le serveur de façon manuelle dans des conditions normales d'utilisation.

Magasin de données DHCP

Toutes les données utilisées par le serveur DHCP sont conservées dans un magasin de données. Le magasin de données peut être constitué indifféremment de fichiers de texte brut, de tables NIS+ ou de fichiers au format binaire. Lors de la configuration du service DHCP, vous êtes invité à choisir le type de magasin de données à utiliser. La section “Sélection du magasin de données DHCP” à la page 327 décrit les différences entre chaque type de magasin de données. Il est possible de convertir un magasin de données et de passer ainsi d'un format à un autre au moyen du gestionnaire DHCP ou de la commande `dhcpconfig`.

Vous pouvez également transférer le contenu du magasin de données d'un serveur DHCP vers un autre magasin de données. Il existe des utilitaires d'importation et d'exportation qui fonctionnent parfaitement avec les magasins de données, même lorsque les serveurs utilisent des formats différents. Le gestionnaire DHCP ou la commande `dhcpconfig` permettent d'exporter et d'importer l'intégralité d'un magasin de données ou uniquement les données qui vous intéressent.

Remarque – Vous êtes libre de stocker les données DHCP dans la base de données ou le format de fichier de votre choix à condition de développer votre propre module de code pour fournir une interface entre DHCP (serveur et outils de gestion) et la base de données. Pour plus d'informations, reportez-vous au *Solaris DHCP Service Developer's Guide* (en anglais).

Un magasin de données DHCP contient deux types de table. Vous pouvez consulter et gérer le contenu de ces tables à l'aide du gestionnaire DHCP ou des utilitaires de ligne de commande. Il s'agit des types suivants :

- Table `dhcptab` – Table contenant les données de configuration susceptibles d'être transmises aux clients.
- **Tables de réseau DHCP** – Tables contenant des informations au sujet des clients DHCP et BOOTP résidant sur le réseau indiqué dans le nom de la table. Le nom de la table correspondant au réseau `192.168.32.0` se compose, par exemple, de `192_168_32_0`.

Table `dhcptab`

La table `dhcptab` contient toutes les informations que les clients peuvent recueillir à partir du serveur DHCP. Le serveur DHCP analyse le contenu de la table `dhcptab` à chaque démarrage. Le nom de fichier de la table `dhcptab` varie en fonction du magasin de données utilisé. La table `dhcptab` créée par le magasin de données NIS+ `SUNWnisplus` est appelée, par exemple, `SUNWnisplus1_dhcptab`.

Le protocole DHCP définit les informations standard qu'il est possible de communiquer aux clients. Il s'agit en l'occurrence des paramètres, des symboles ou des options. Les options sont représentées dans le protocole DHCP par des codes numériques et des libellés de texte, mais sans valeurs. Le tableau suivant présente les options standard les plus fréquemment employées.

TABLEAU 12–1 Exemples d'options standard DHCP

Code	Libellé	Description
1	`Subnet`	Adresse IP du masque de sous-réseau
3	`Router`	Adresse IP du routeur
6	`DNSserv`	Adresse IP du serveur DNS
12	`Hostname`	Chaîne de texte correspondant au nom d'hôte client
15	`DNSdmain`	Nom du domaine DNS

Des valeurs sont automatiquement attribuées à certaines options lorsque vous fournissez les informations demandées lors de la configuration du serveur. Rien ne vous empêche par la suite d'assigner, de façon explicite, les valeurs voulues à d'autres options. Les options et leurs valeurs sont transmises au client à titre de données de configuration. Par exemple, le couple option/valeur `DNSdmain=Georgia.Peach.COM` définit le nom de domaine DNS du client comme suit : `Georgia.Peach.COM`.

Les options peuvent être regroupées avec d'autres options au sein de conteneurs appelés *macros* de manière à communiquer plus facilement les informations au client. Certaines macros sont

générées automatiquement lors de la phase de configuration du serveur et contiennent des options associées à des valeurs. Il est possible, en outre, d'imbriquer des macros dans d'autres macros.

Le format de la table `dhcptab` est décrit dans la page de manuel `dhcptab(4)` Dans le gestionnaire DHCP, toutes les informations présentées dans les onglets Options et Macros proviennent de la table `dhcptab`. Pour plus d'informations à propos des options, reportez-vous à la section "À propos des options DHCP" à la page 317 Pour plus d'informations au sujet des macros, reportez-vous à la section "À propos des macros DHCP" à la page 318.

N'oubliez pas que la table `dhcptab` ne peut, en aucun cas, être éditée manuellement. Vous devez vous servir de la commande `dhtadm` ou du gestionnaire DHCP pour créer, supprimer ou modifier des options et des macros.

Tables de réseau DHCP

Une table de réseau DHCP permet de faire la correspondance entre les identificateurs de clients, les adresses IP et les paramètres de configuration associés à chaque adresse. Le format des tables de réseau est décrit dans la page de manuel `dhcp_network(4)` Dans le gestionnaire DHCP, toutes les informations présentées dans l'onglet relatif aux adresses proviennent des tables de réseau.

Gestionnaire DHCP

Le gestionnaire DHCP est un outil basé sur une interface graphique (IG) prévu pour réaliser toutes les tâches administratives relatives au service DHCP. Il sert aussi bien à gérer le serveur que les données exploitées par le serveur. Vous devez être superutilisateur pour exécuter le gestionnaire DHCP.

Le gestionnaire DHCP offre les possibilités suivantes :

- Configurer et annuler la configuration du serveur DHCP
- Démarrer, arrêter et redémarrer le serveur DHCP
- Activer et désactiver le service DHCP
- Personnaliser les paramètres du serveur DHCP

Le gestionnaire DHCP permet de gérer les adresses IP, les macros de configuration du réseau et les options de configuration du réseau des façons suivantes :

- En ajoutant et supprimant des réseaux placés sous le contrôle DHCP
- En affichant, ajoutant, modifiant, effaçant et libérant des adresses IP placées sous le contrôle DHCP
- En affichant, ajoutant, modifiant et supprimant des macros de configuration du réseau
- En affichant, ajoutant, modifiant et supprimant des options de configuration du réseau non standard

Le gestionnaire DHCP permet de gérer les magasins de données DHCP des façons suivantes :

- En convertissant les données sous un nouveau format de magasin de données
- En déplaçant les données DHCP d'un serveur DHCP à un autre (il convient pour ce faire d'exporter les données du premier serveur et de les importer sur le deuxième serveur)

Le gestionnaire DHCP propose une aide en ligne complète pour toutes les procédures réalisables avec cet outil. Pour plus d'informations, reportez-vous à la section “À propos du gestionnaire DHCP” à la page 352.

Utilitaires de ligne de commande DHCP

Toutes les opérations de gestion DHCP peuvent être effectuées à l'aide des utilitaires de ligne de commande. Pour exécuter ces utilitaires, vous devez vous connecter en tant que superutilisateur ou en tant qu'utilisateur doté du profil de gestion DHCP. Voir la section “Configuration de l'accès utilisateur aux commandes DHCP” à la page 355.

Le tableau suivant présente les différents utilitaires disponibles et l'intérêt de chacun d'entre-eux.

TABLEAU 12–2 Utilitaires de ligne de commande DHCP

Commande	Description et intérêt	Liens aux pages de manuel
`in.dhcpd`	Démon du service DHCP. Les arguments de la ligne de commande permettent de configurer plusieurs options d'exécution.	`in.dhcpd`(1M)
`dhcpconfig`	Sert à configurer et à annuler la configuration d'un serveur DHCP. Cet utilitaire permet de réaliser la plupart des fonctions du gestionnaire DHCP à partir de la ligne de commande. Il est particulièrement utile pour créer des scripts destinés aux sites souhaitant automatiser certaines fonctions de configuration. `dhcpconfig` collecte des informations à partir des fichiers de topologie de réseau du système serveur dans le but de réunir les données qui conviennent pour la configuration initiale.	`dhcpconfig`(1M)
`dhtadm`	Sert à ajouter, supprimer et modifier des options et des macros de configuration pour les clients DHCP. Cet utilitaire permet d'éditer la table `dhcptab` de façon indirecte pour s'assurer que le format est correct. Vous ne devez, en aucun cas, éditer directement le contenu de la table `dhcptab`.	`dhtadm`(1M)

TABLEAU 12–2 Utilitaires de ligne de commande DHCP *(Suite)*

Commande	Description et intérêt	Liens aux pages de manuel
`pntadm`	Sert à gérer les tables de réseau DHCP. Cet utilitaire est idéal pour : ■ Ajouter et supprimer des adresses IP et des réseaux sous le contrôle DHCP ■ Modifier la configuration du réseau pour les adresses IP spécifiées ■ Afficher des informations au sujet des adresses IP et des réseaux sous le contrôle DHCP	`pntadm(1M)`

Contrôle d'accès des commandes DHCP basé sur les rôles

Le niveau de sécurité des commandes `dhcpconfig`, `dhtadm` et `pntadm` est défini par les paramètres de contrôle d'accès basé sur les rôles (paramètres RBAC). Par défaut, seul un superutilisateur est habilité à exécuter les commandes. Si vous avez l'intention d'exécuter les commandes sous un autre nom d'utilisateur, vous devez allouer le nom d'utilisateur au profil de gestion DHCP comme indiqué à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Configuration du serveur DHCP

Il est nécessaire de configurer le serveur DHCP la première fois que vous lancez le gestionnaire DHCP sur le système destiné au serveur DHCP.

Les boîtes de dialogue de configuration du serveur du gestionnaire DHCP vous invitent à spécifier toutes les informations nécessaires pour activer et exécuter le serveur DHCP sur un réseau. Certaines valeurs par défaut sont obtenues à partir des fichiers système existants. Si vous n'avez pas configuré le système pour le réseau, aucune valeur par défaut n'est définie. Le gestionnaire DHCP vous demande de préciser les informations suivantes :

- Rôle du serveur (fait-il office de serveur DHCP ou d'agent de relais BOOTP ?)
- Type de magasin de données (fichiers texte, fichiers binaires, NIS+ ou autres bases de données ou fichiers spécifiques à votre site)
- Paramètres de configuration du type de magasin de données sélectionné
- Service de noms à utiliser pour mettre à jour les enregistrements de l'hôte, le cas échéant (`/etc/hosts` , NIS+ ou DNS)
- Durée du bail et possibilité ou non pour les clients de renouveler un bail

- Nom du domaine DNS et adresses IP des serveurs DNS
- Adresse réseau et masque de sous-réseau pour le premier réseau à configurer pour le service DHCP
- Type de réseau (local ou point à point)
- Activation ou non de la détection de l'adresse IP d'un routeur
- Nom du domaine NIS et adresses IP des serveurs NIS
- Nom du domaine NIS+ et adresses IP des serveurs NIS+

Vous pouvez également configurer le serveur DHCP à l'aide de la commande `dhcpconfig.` Cet utilitaire rassemble automatiquement les informations nécessaires à partir des fichiers système existants en guise de configuration initiale. Il faut donc s'assurer que les fichiers en question sont à jour avant d'exécuter la commande `dhcpconfig`. Pour plus d'informations au sujet des fichiers utilisés par `dhcpconfig` pour obtenir les données de configuration, reportez-vous à la page de manuel `dhcpconfig(1M)`.

Allocation des adresses IP

Le serveur DHCP accepte les modes d'allocation d'adresses IP suivants :

- **Allocation manuelle** – Le serveur propose une adresse IP spécifique que vous pouvez attribuer à un client DHCP. Il est impossible de récupérer l'adresse ou de l'assigner à un autre client.
- **Allocation automatique ou permanente** – Le serveur propose une adresse IP spécifique non limitée dans le temps. Cette adresse est ainsi associée de façon permanente au client jusqu'à ce que vous changiez l'affectation ou que le client libère l'adresse.
- **Allocation dynamique** – Le serveur propose une adresse IP au client demandeur pendant une durée précise. À l'expiration du bail prévu pour l'adresse, celle-ci est récupérée par le serveur qui se réserve le droit de l'allouer à un autre client. La période limite d'utilisation de l'adresse dépend de la durée du bail configurée pour le serveur.

Données de configuration du réseau

C'est vous qui déterminez la nature des informations communiquées aux clients DHCP. Lors de la configuration du serveur DHCP, vous fournissez des renseignements essentiels au sujet du réseau. Rien ne vous empêche par la suite d'ajouter toute autre information que vous jugez utile de transmettre aux clients.

Le serveur DHCP stocke les données de configuration du réseau dans la table `dhcptab` , par couple option/valeur et sous forme de macros. Les options constituent des mots-clés pour les informations de réseau que vous désirez fournir aux clients. Les valeurs attribuées aux options sont transmises aux clients dans des messages DHCP. L'adresse du serveur NIS est

communiquée, par exemple, au moyen d'une option appelée `NISservs`. L'option `NISservs` possède une valeur équivalente à une liste d'adresses IP, allouée par le serveur DHCP. Les macros sont un moyen pratique de regrouper toutes les options que vous avez l'intention de fournir aux clients en une seule opération. Vous pouvez faire appel au gestionnaire DHCP pour créer des macros et assigner des valeurs aux options. Si vous préférez effectuer ces opérations à partir de la ligne de commande, exécutez l'utilitaire de gestion des tables de configuration DHCP (`dhtadm`).

À propos des options DHCP

Dans DHCP, une *option* désigne un élément d'information du réseau à transmettre à un client. Dans le jargon DHCP, les *symboles* ou les *balises* sont également appelés des options. Une option est définie par un code numérique et un libellé de texte. Elle reçoit une valeur en cas d'utilisation dans le service DHCP.

Le protocole DHCP définit un grand nombre d'options standard pour les données de réseau fréquemment utilisées : `Subnet`, `Router`, `Broadcst`, `NIS+dom`, `Hostname` et `LeaseTim` pour n'en citer que quelques-unes. Vous trouverez la liste complète des options standard sur la page de manuel `dhcp_inittab(4)`. Vous ne pouvez, en aucun cas, modifier les mots-clés des options standard. Il est possible, en revanche, d'attribuer des valeurs aux options se rapportant à votre réseau lorsque vous décidez de les inclure dans des macros.

Vous avez le droit, en outre, de définir de nouvelles options pour les données non représentées par les options standard. Les options que vous créez doivent être classées dans l'une des trois catégories suivantes :

- **Extended** – Catégorie réservée aux options devenues des options DHCP standard, mais pas encore prises en compte dans l'implémentation du serveur DHCP. Optez pour cette catégorie si vous connaissez l'option standard qui vous intéresse, mais ne souhaitez pas mettre à niveau votre serveur DHCP.
- **Site** – Catégorie réservée aux options spécifiques à votre site. C'est à vous qu'il appartient de créer ces options.
- **Vendor** – Catégorie réservée aux options devant s'appliquer uniquement aux clients d'une classe particulière, une plate-forme matérielle ou fournisseur, par exemple. L'implémentation DHCP intègre un certain nombre d'options fournisseur pour les clients Oracle Solaris. Ainsi, l'option `SrootIP4` sert à spécifier l'adresse IP d'un serveur qu'un client s'initialisant à partir du réseau est censé utiliser pour son système de fichiers root (/).

Le Chapitre 15, “Administration de DHCP (tâches)” fournit les procédures de création, de modification et de suppression d'options DHCP.

À propos des macros DHCP

Dans le cadre du service DHCP, une *macro* représente un ensemble d'options de configuration du réseau auxquelles vous avez attribué des valeurs. L'intérêt des macros est de regrouper les options à transmettre à des clients spécifiques ou à certains types de client. Une macro destinée à tous les clients d'un sous-réseau donné pourrait contenir, par exemple, les couples option/valeur correspondant au masque de sous-réseau, à l'adresse IP du routeur, à l'adresse de diffusion, au domaine NIS+ et à la durée du bail.

Traitement des macros par le serveur DHCP

Lorsque le serveur DHCP traite une macro, il place les options et les valeurs de réseau définies dans la macro à l'intérieur d'un message DHCP adressé au client. Le serveur exécute automatiquement certaines macros pour les clients d'un certain type.

Pour pouvoir être traitée automatiquement, la macro doit respecter les conventions de dénomination propres aux catégories présentées dans le tableau suivant.

TABLEAU 12–3 Catégories de macros DHCP autorisant un traitement automatique

Catégorie de macros	Description
Classe de client	Le nom de la macro correspond à une classe de client désignée par le type de machine client et/ou le système d'exploitation. Si un serveur dispose, par exemple, d'une macro appelée `SUNW.Sun-Blade-100`, tout client dont l'implémentation matérielle est `SUNW,Sun-Blade-100` reçoit automatiquement les valeurs figurant dans la macro `SUNW.Sun-Blade-100`.
Adresse réseau	Le nom de la macro correspond à une adresse IP de réseau gérée par DHCP. Si un serveur dispose, par exemple, d'une macro appelée `10.53.224.0`, tout client connecté au réseau `10.53.224.0` reçoit automatiquement les valeurs figurant dans la macro `10.53.224.0`.
ID client	Le nom de la macro correspond à un identificateur unique pour le client. Il est généralement dérivé d'une adresse Ethernet ou MAC. Si un serveur dispose, par exemple, d'une macro appelée `08002011DF32`, le client possédant l'ID de client `08002011DF32` (dérivé de l'adresse Ethernet `8:0:20:11:DF:32`) reçoit automatiquement les valeurs figurant dans la macro nommée `08002011DF32` .

Une macro portant un nom n'appartenant à aucune des catégories indiquées dans le Tableau 12–3 peut être traitée uniquement si l'une des conditions suivantes est vérifiée :

- La macro est mappée à une adresse IP.
- La macro est imbriquée dans une autre macro traitée automatiquement.
- La macro est imbriquée dans une autre macro mappée à une adresse IP.

Remarque – Lorsque vous configurez un serveur, une macro dont le nom correspond au nom du serveur est créée par défaut. Cette macro de serveur ne s'exécute *pas* automatiquement, quel que soit le client auquel elle s'applique, dans la mesure où elle ne possède aucun des types de nom autorisant un traitement automatique. Lorsque vous définissez par la suite de nouvelles adresses IP sur le serveur, celles-ci sont mappées dans le but d'utiliser la macro de serveur par défaut.

Ordre de traitement des macros

Lorsqu'un client DHCP demande des services DHCP, le serveur DHCP identifie les macros répondant à la requête du client. Il traite les macros, en se servant des catégories de macros pour déterminer leur ordre d'exécution. Il s'occupe d'abord de la catégorie la plus générale et traite la catégorie la plus spécifique en dernier. Les macros sont traitées dans l'ordre suivant :

1. Macros de la classe de client – Catégorie la plus générale
2. Macros d'adresse réseau – Plus spécifiques que les macros de la classe de client
3. Macros mappées aux adresses IP – Plus spécifiques que les macros d'adresse réseau
4. Macros d'ID de client – Catégorie la plus spécifique, se rapportant à un seul client

Une macro imbriquée dans une autre macro est traitée pendant l'exécution de cette dernière.

Si la même option figure dans plusieurs macros, la valeur de cette option dans la macro correspondant à la catégorie la plus spécifique est prise en compte, car c'est elle qui est traitée en dernier. Si une macro d'adresse réseau contient, par exemple, la valeur 24 heures pour l'option de durée de bail et qu'une macro d'ID de client indique une durée de bail équivalente à 8 heures, le client reçoit la valeur 8 heures.

Limite de taille pour les macros DHCP

La somme totale des valeurs attribuées à l'ensemble des options dans une macro ne doit pas dépasser 255 octets, y compris les codes d'option et les informations de longueur. Cette limite est dictée par le protocole DHCP.

Les macros qui sont les plus concernées par cette limite sont celles utilisées pour transmettre des chemins aux fichiers des serveurs d'installation Oracle Solaris. En règle générale, vous devez fournir le minimum d'informations nécessaires concernant le fournisseur. Pour les options nécessitant des chemins d'accès, vous devez utiliser des noms courts. Si vous créez des liens symboliques vers des chemins d'accès longs, vous pouvez communiquer les noms de liens les plus courts.

Le client DHCP

Le terme « client » est parfois employé pour faire référence à une machine physique jouant le rôle de client sur le réseau. Or, le client DHCP décrit dans ce document est une entité logicielle. Le client DHCP est un démon (`dhcpagent`) s'exécutant dans Oracle Solaris, sur un système configuré pour recevoir sa configuration réseau d'un serveur DHCP. Les clients DHCP d'autres fournisseurs peuvent également utiliser les services du serveur DHCP Ce document traite uniquement du client DHCP

Pour plus d'informations sur le client DHCP, reportez-vous au Chapitre 16, “Configuration et administration du client DHCP”.

◆ ◆ ◆ CHAPITRE 13

Planification pour le service DHCP (liste des tâches)

Vous pouvez utiliser le service DHCP au sein d'un réseau que vous créez ou qui existe déjà. Si vous avez l'intention de mettre en place un nouveau réseau, reportez-vous au Chapitre 2, “Planification de votre réseau TCP/IP (tâches)” avant d'essayer de configurer le service DHCP. Si le réseau existe déjà, suivez les consignes et instructions proposées ci-après.

Le présent chapitre décrit les procédures préalables à la configuration du service DHCP sur votre réseau. Ces informations concernent le gestionnaire DHCP, mais rien ne vous empêche de configurer le service DHCP à l'aide de l'utilitaire de ligne de commande `dhcpconfig`.

Le présent chapitre contient les informations suivantes :

Préparation du réseau pour le service DHCP (liste des tâches)

Avant de configurer votre réseau en vue d'utiliser le protocole DHCP, vous devez réunir un certain nombre d'informations afin de décider s'il est préférable de configurer un ou plusieurs serveurs. Utilisez la liste des tâches du tableau suivant pour indiquer les tâches de préparation de votre réseau pour le service DHCP. Le tableau suivant répertorie les tâches, les descriptions des fonctions que chaque tâche effectue et les sections expliquant en détails les étapes à suivre pour effectuer chaque tâche.

Tâche	Description	Voir
Établir un inventaire de la topologie de réseau.	Déterminez et localisez les services disponibles sur le réseau.	"Inventaire de la topologie du réseau" à la page 322
Évaluer le nombre de serveurs DHCP nécessaires.	Utilisez le nombre prévu de clients DHCP pour vous aider à déterminer la quantité de serveurs DHCP dont vous avez besoin.	"Évaluation du nombre de serveurs DHCP nécessaires" à la page 323
Mettre à jour les fichiers système et la table `netmasks`.	Reflétez la topologie du réseau avec précision.	"Mises à jour des fichiers système et des tables de masques de réseau" à la page 324

Inventaire de la topologie du réseau

Si vous ne l'avez pas déjà fait, faites un inventaire des éléments physiques de votre réseau. Indiquez la position des routeurs et des clients et l'emplacement des serveurs assurant des services au réseau. Grâce à cet inventaire de la topologie du réseau, vous serez plus à même de déterminer le serveur à privilégier pour le service DHCP. Cela vous aidera également à identifier les données de configuration que le serveur DHCP est susceptible de fournir aux clients.

Pour plus d'informations sur la planification de votre réseau, reportez-vous au Chapitre 2, "Planification de votre réseau TCP/IP (tâches)".

La procédure de configuration DHCP permet de rassembler certaines informations relatives au réseau à partir des fichiers système et réseau du serveur. La section "Mises à jour des fichiers système et des tables de masques de réseau" à la page 324 explique l'intérêt de ces fichiers. Vous souhaiterez éventuellement proposer aux clients d'autres informations de service. Dans ce cas, vous devrez les intégrer aux macros du serveur. Lors de l'examen de la topologie du réseau, pensez à noter les adresses IP des serveurs pouvant présenter un intérêt pour vos clients. Les serveurs suivants peuvent, par exemple, fournir des services sur votre réseau. Or, la configuration DHCP ne permet pas de les détecter.

- Serveur de temps
- Serveur de journalisation
- Serveur d'impression
- Serveur d'installation
- Serveur d'initialisation
- Serveur proxy Web
- Serveur de swap
- Serveur de polices X Window
- Serveur TFTP (Trivial File Transfer Protocol)

Topologie de réseau à éviter

Dans certains environnements de réseau IP, les médias physiques sont mis en commun entre plusieurs réseaux locaux (LAN). Les réseaux peuvent utiliser diverses interfaces réseau matérielles ou diverses interfaces logiques. Le protocole DHCP ne fonctionne pas très bien dans ce type de réseau de médias partagés. Lorsque plusieurs réseaux locaux sont répartis sur le même réseau physique, la requête d'un client DHCP est acheminée vers toutes les interfaces matérielles du réseau. Cela donne l'impression que le client est connecté à tous les réseaux IP à la fois.

Or, DHCP doit être en mesure de déterminer l'adresse du réseau d'un client afin d'attribuer l'adresse IP qui convient à ce dernier. Si plusieurs réseaux sont présents sur le média physique, le serveur n'est pas capable d'identifier le réseau du client. Il lui est impossible d'assigner une adresse IP s'il ne connaît pas le numéro du réseau.

Vous ne pouvez utiliser DHCP que sur un seul réseau. Si un des réseaux ne permet pas de répondre aux besoins du protocole DHCP, vous devez alors reconfigurer les réseaux. Voici quelques considérations importantes à prendre en compte :

- Utilisez un masque de sous-réseau à longueur variable (VLSM) sur vos sous-réseaux pour profiter au mieux de l'espace d'adressage IP dont vous disposez. Vous n'aurez peut-être pas besoin d'exécuter plusieurs réseaux sur le même réseau physique. Pour savoir comment mettre en place un masque de sous-réseau à longueur variable, reportez-vous à la page de manuel `netmasks(4)` Pour plus d'informations sur le CIDR (Classless Inter-Domain Routing, routage inter-domaine sans classe) et le VLSM (Variable-Length Subnet Mask, masque de sous-réseau à longueur variable), consultez `http://www.ietf.org/rfc/rfc1519.txt`.
- Configurez les ports de vos commutateurs afin d'affecter les périphériques à différents réseaux locaux (LAN) physiques. Cette technique permet de préserver le mappage réseau local-réseau IP, exigé par DHCP. Pour plus d'informations sur la configuration des ports, consultez la documentation de référence du commutateur.

Évaluation du nombre de serveurs DHCP nécessaires

Le type de magasin de données que vous choisissez a une incidence directe sur le nombre de serveurs qu'il est nécesssaire de prévoir pour gérer tous vos clients DHCP. Le tableau suivant indique le nombre maximum de clients DHCP et BOOTP pouvant être pris en charge par un serveur DHCP pour chaque magasin de données.

TABLEAU 13–1 Estimation du nombre maximum de clients gérés par un serveur DHCP

Type de magasin de données	Nombre maximum de clients gérés
Fichiers texte	10 000
NIS+	40 000

TABLEAU 13–1 Estimation du nombre maximum de clients gérés par un serveur DHCP *(Suite)*

Type de magasin de données	Nombre maximum de clients gérés
Fichiers binaires	100 000

Ce nombre maximum est une indication générale et non une valeur absolue. La capacité d'un client d'un serveur DHCP dépend avant tout du nombre de transactions que le serveur doit traiter par seconde. La durée des baux et les habitudes d'utilisation ont un impact non négligeable sur la vitesse de transaction. Supposons, par exemple, que les baux sont prévus pour une durée de 12 heures et que les utilisateurs éteignent leurs systèmes pendant la nuit. Si un grand nombre d'utilisateurs allument au même moment leur système le matin, le pic de transactions gérées par le serveur sera à son maximum dans la mesure où les demandes de baux parviendront simultanément au serveur. Dans un environnement de ce type, le nombre de clients pris en charge par le serveur DHCP sera forcément inférieur. Le serveur DHCP est capable, à l'inverse, de gérer un plus grand nombre de clients dans un environnement mettant en jeu des baux de plus longue durée, ou dans un environnement où les périphériques sont connectés en permanence (comme dans le cas des modems câble).

La section "Sélection du magasin de données DHCP" à la page 327 propose une comparaison des types de magasins de données.

Mises à jour des fichiers système et des tables de masques de réseau

Lors de la phase de configuration DHCP, les outils DHCP analysent divers fichiers système sur votre serveur afin de rechercher les informations dont ils ont besoin pour configurer le serveur.

Avant de lancer le gestionnaire DHCP ou d'exécuter l'utilitaire `dhcpconfig`, il est donc important de s'assurer que ces informations sont à jour. Si vous constatez des erreurs après avoir configuré le serveur, servez-vous du gestionnaire DHCP ou de `dhtadm` pour modifier les macros sur le serveur.

Le tableau suivant présente une partie des informations collectées lors de la configuration du serveur DHCP et les sources utilisées. Veillez à ce que ces informations soient définies correctement sur le serveur avant de commencer à configurer DHCP sur le serveur. Si vous apportez des modifications aux fichiers système une fois le serveur configuré, vous devez reconfigurer le service pour refléter les changements en question.

TABLEAU 13–2 Informations utilisées pour la configuration DHCP

Informations	Source	Commentaires
Fuseau horaire	Date système, paramètres de fuseau horaire	La date et le fuseau horaire sont initialement définis lors de l'installation d'Oracle Solaris. Vous pouvez changer la date à l'aide de la commande `date`. Pour changer le fuseau horaire, il convient d'éditer le fichier `/etc/default/init` afin de définir la variable d'environnement `TZ`. Pour plus d'informations, reportez-vous à la page de manuel `TIMEZONE(4)`.
Paramètres DNS	`/etc/resolv.conf`	Le serveur DHCP recherche les paramètres DNS (tels que le nom de domaine DNS et les adresses de serveur DNS) dans le fichier `/etc/resolv.conf`. Reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)* (en anglais) ou à la page de manuel `resolv.conf(4)` pour plus d'informations sur `resolv.conf`.
Paramètres NIS ou NIS+	Nom du domaine système, `nsswitch.conf`, NIS ou NIS+	Le serveur DHCP a recours à la commande `domainname` pour obtenir le nom de domaine du système serveur. Le fichier `nsswitch.conf` indique au serveur l'emplacement des informations basées sur le domaine. Si le système serveur est un client NIS ou NIS+, le serveur DHCP exécute une requête pour connaître les adresses IP du serveur NIS ou NIS+. Pour plus d'informations, reportez-vous à la page de manuel `nsswitch.conf(4)`.
Routeur par défaut	Tables de routage système, invite d'utilisateur	Le serveur DHCP effectue une recherche dans les tables de routage du réseau afin d'identifier le routeur par défaut des clients reliés au réseau local. Si les clients ne figurent pas sur le même réseau, le serveur DHCP vous demande de lui donner cette information.

TABLEAU 13–2 Informations utilisées pour la configuration DHCP *(Suite)*

Informations	Source	Commentaires
Masque de sous-réseau	Interface réseau, table `netmasks`	Le serveur DHCP analyse ses propres interfaces réseau pour déterminer le masque de sous-réseau et l'adresse de diffusion pour les clients locaux. Si la requête provient d'un agent de relais, le serveur obtient le masque de sous-réseau à partir de la table `netmasks` du réseau de l'agent de relais.
Adresse de diffusion	Interface réseau, table `netmasks`	Dans le cas d'un réseau local, le serveur DHCP obtient l'adresse de diffusion en envoyant une requête à l'interface réseau. Dans le cas d'un réseau distant, le serveur utilise l'adresse IP des agents de relais BOOTP et le masque de sous-réseau du réseau distant pour calculer l'adresse de diffusion pour le réseau.

Décisions relatives à la configuration de votre serveur DHCP (liste des tâches)

Cette section traite des décisions qu'il est nécessaire de prendre avant de configurer le premier serveur DHCP sur votre réseau. Le tableau suivant vous guide dans la configuration du service DHCP de votre réseau et lie chaque tâche à la section décrivant les étapes à suivre pour effectuer chaque tâche.

Tâche	Description	Voir
Sélectionner un serveur pour le service DHCP.	Vérifiez si le serveur remplit les conditions nécessaires pour exécuter le service DHCP.	“Sélection de l'hôte réservé au service DHCP” à la page 327
Choisir un magasin de données.	Comparez les types de magasin de données pour déterminer celui qui convient le mieux à votre site.	“Sélection du magasin de données DHCP” à la page 327
Définir une stratégie de location.	Intéressez-vous de près à la location d'adresses IP afin d'élaborer la meilleure stratégie de location possible pour votre site.	“Stratégie de location” à la page 328
Spécifier l'adresse d'un routeur ou envisager la détection du routeur.	Déterminez si les clients DHCP utilisent un routeur particulier ou procèdent à la détection du routeur.	“Identification des routeurs pour les clients DHCP” à la page 329

Sélection de l'hôte réservé au service DHCP

En gardant la topologie de votre réseau à l'esprit, prenez en considération les spécifications système suivantes pour choisir l'hôte qui hébergera le serveur DHCP.

L'hôte doit satisfaire aux exigences suivantes :

- Il doit exécuter Solaris 2.6 ou une version ultérieure. Si vous avez l'intention de gérer un grand nombre de clients, installez Solaris 8 7/01 ou une version ultérieure.
- Il doit être accessible par tous les réseaux dont certains clients prévoient d'utiliser DHCP, soit directement sur le réseau ou par l'intermédiaire d'un agent de relais BOOTP.
- Il doit être configuré de façon à utiliser le routage.
- Il doit disposer d'une table `netmasks` configurée correctement afin de refléter la topologie du réseau.

Sélection du magasin de données DHCP

Vous pouvez décider de stocker les données DHCP dans des fichiers texte, dans des fichiers binaires ou dans le service d'annuaire NIS+. Le tableau suivant récapitule les fonctions de chaque type de magasin de données et indique l'environnement de prédilection pour chacun d'eux.

TABLEAU 13–3 Comparaison des magasins de données DHCP

Type de magasin de données	Performances	Maintenance	Partage	Environnement
Fichiers binaires	Hautes performances, capacité supérieure	Maintenance limitée, aucun serveur de base de données nécessaire. Le contenu doit être examiné avec le gestionnaire DHCP ou `dhtadm` et `pntadm`. Des sauvegardes régulières des fichiers sont conseillées.	Les magasins de données ne peuvent pas être partagés entre les serveurs DHCP.	Environnements de moyenne à grande taille comptant de nombreux réseaux avec des milliers de clients par réseau. Convient à des FAI de petite taille ou de taille moyenne.
NIS+	Performances et capacités modérées, liées aux performances et capacités du service NIS+	Le système serveur DHCP doit être configuré en tant que client NIS+. Nécessite une maintenance de service NIS+. Le contenu doit être examiné avec le gestionnaire DHCP ou `dhtadm` et `pntadm`. Une sauvegarde régulière avec `nisbackup` est conseillée.	Les données DHCP sont distribuées dans NIS+, et plusieurs serveurs peuvent accéder aux mêmes conteneurs.	Environnements de petite à moyenne taille comptant jusqu'à 5 000 clients par réseau.

TABLEAU 13–3 Comparaison des magasins de données DHCP *(Suite)*

Type de magasin de données	Performances	Maintenance	Partage	Environnement
Fichiers texte	Performances modérées, faible capacité	Maintenance limitée, aucun serveur de base de données nécessaire. Possible de lire le format ASCII sans le gestionnaire DHCP, `dhtadm` ou `pntadm`. Des sauvegardes régulières des fichiers sont conseillées.	Le magasin de données peut être partagé entre plusieurs serveurs DHCP à condition de stocker les données DHCP sur un système de fichiers exporté via un point de montage NFS.	Environnements de petite taille comptant moins de 10 000 clients, à raison de moins d'un millier de clients par réseau.

Le système d'information réseau (NIS) traditionnel n'est pas proposé comme magasin de données dans la mesure où il ne gère pas les mises à jour incrémentielles accélérées. Si votre réseau utilise le système NIS, prévoyez des fichiers texte ou des fichiers binaires pour votre magasin de données.

Stratégie de location

Un *bail* représente la durée d'utilisation d'une adresse IP accordée par le serveur DHCP à un client DHCP. Lors de la phase de configuration initiale du serveur, vous êtes tenu de définir une stratégie de location à l'échelle du site. La *stratégie de location* permet d'une part, de fixer la durée des baux, et d'autre part d'autoriser ou non les clients à renouveler leur bail. Le serveur se sert des informations fournies pour définir les valeurs des options dans les macros par défaut qu'il génère en cours de configuration. Vous pouvez mettre en place différentes stratégies en fonction de clients spécifiques ou des types de client, en définissant les options des macros de configuration que vous créez.

La *durée du bail* représente le nombre d'heures, de jours ou de semaines de validité du bail. Lorsqu'un client se voit attribuer une adresse IP ou renégocie le bail d'une adresse IP, l'heure et la date d'expiration du bail sont automatiquement calculées. Le nombre d'heures correspondant est ajouté aux données d'horodatage indiquées sur l'accusé de réception DHCP du client. Supposons, par exemple, que l'accusé de réception DHCP soit daté du 16 septembre 2005 à 9 h 15 et que la durée du bail soit de 24 heures. Dans ce cas, le bail expirera le 17 septembre 2005 à 9 h 15. Le délai d'expiration du bail est stocké dans l'enregistrement réseau DHCP du client, qui est visible depuis le gestionnaire DHCP ou à l'aide de l'utilitaire `pntadm` .

Il est recommandé de choisir une durée de bail relativement courte de façon à pouvoir récupérer rapidement les adresses laissées libres. Mais il faut également prévoir une durée de bail suffisamment longue pour parer aux interruptions de service DHCP. Les clients doivent, en effet, être capables de fonctionner pendant la réparation du système sur lequel le service DHCP

s'exécute. La règle d'or est de fixer un bail d'une durée équivalente à deux fois la durée d'indisponibilité prévue d'un système. Si vous avez besoin, par exemple, de quatre heures pour vous procurer et remplacer une pièce défectueuse et réinitialiser le système, envisagez un bail de huit heures.

L'option de négociation précise si le client est en droit de renégocier son bail auprès du serveur avant qu'il expire. Si la négociation est autorisée, le client contrôle le temps restant avant l'expiration du bail. Dès que la moitié de la durée du bail s'est écoulée, le client demande au serveur DHCP de prolonger son bail afin de revenir à la durée d'origine. Il est recommandé de désactiver l'option de négociation des baux dans les environnements comptant plus de systèmes que d'adresses IP. L'utilisation des adresses IP sera dès lors limitée dans le temps. Si le nombre d'adresses IP est suffisant, il est préférable, au contraire, d'activer l'option de négociation des baux pour éviter que les clients arrêtent leurs interfaces réseau dès l'expiration de leur bail. Si vous autorisez les clients à renouveler leur bail, il est possible que les connexions TCP des clients (sessions NFS et Telnet, par exemple) s'interrompent. Vous pouvez activer l'option de négociation des baux pour l'ensemble des clients lors de la configuration du serveur. En utilisant l'option `LeaseNeg` dans les macros de configuration, il est possible d'activer cette option pour certains clients en particulier ou pour certains types de client.

Remarque – Les systèmes offrant des services sur le réseau doivent impérativement conserver leurs adresses IP. Les baux à court terme sont donc à proscrire pour ce type de système. Vous pouvez utiliser le service DHCP avec ces systèmes à condition de leur assigner des adresses IP manuelles réservées, au lieu de leur attribuer des adresses IP bénéficiant de baux permanents. Il suffit ensuite de détecter à quel moment l'adresse IP du système n'est plus utilisée.

Identification des routeurs pour les clients DHCP

Les systèmes hôtes font appel à des routeurs pour les communications qui sortent du cadre de leur réseau local. Les hôtes doivent connaître les adresses IP de ces routeurs.

Lorsque vous configurez un serveur DHCP, il y a deux façons de communiquer les adresses des routeurs aux clients DHCP. Le premier moyen est de fournir des adresses IP spécifiques pour les routeurs. Cependant, la méthode préférée consiste à demander aux clients de trouver eux-mêmes les routeurs grâce au protocole de détection des routeurs.

Si des clients de votre réseau sont en mesure de détecter des routeurs de cette manière, vous devez recourir au protocole de détection des routeurs, même s'il n'y a qu'un seul routeur. Cette technique permet au client de s'adapter facilement aux changements de routeur dans le réseau. Supposons, par exemple, qu'un routeur tombe en panne et soit remplacé par un routeur avec une nouvelle adresse. Les clients pourront détecter automatiquement cette adresse sans avoir à obtenir une nouvelle configuration de réseau pour connaître la nouvelle adresse du routeur.

Décisions relatives à la gestion des adresses IP (liste des tâches)

Lors de la configuration du service DHCP, vous définissez les aspects des adresses IP que le serveur doit gérer. Si votre réseau a besoin de plusieurs serveurs DHCP, vous pouvez confier la responsabilité d'une partie des adresses IP à chaque serveur. Il faut donc choisir la façon dont vous souhaitez répartir ces responsabilités. Le tableau suivant représente la liste des tâches à effectuer pour gérer les adresses IP lorsque vous utilisez un service DHCP sur le réseau. Le tableau contient également des liens vers les sections correspondantes expliquant en détails comment effectuer chaque tâche.

Tâche	Description	Référence
Décider quelles adresses le serveur doit gérer.	Déterminez le nombre et la nature des adresses que vous souhaitez placer sous la responsabilité du serveur DHCP.	"Définition du nombre et des plages d'adresses IP" à la page 330
Décider si le serveur doit générer ou non automatiquement les noms d'hôtes pour les clients.	Renseignez-vous sur les méthodes de génération des noms d'hôtes clients pour trouver la meilleure solution.	"Génération des noms d'hôtes clients" à la page 331
Déterminer la macro de configuration à attribuer aux clients.	Renseignez-vous sur les macros de configuration des clients pour sélectionner la macro la plus appropriée.	"Macros de configuration client par défaut" à la page 331
Déterminer les types de bail à privilégier.	Étudiez les différents types de bail existants afin de choisir celui qui convient le mieux pour vos clients DHCP.	"Choix entre un bail dynamique ou permanent" à la page 332

Définition du nombre et des plages d'adresses IP

Lors de la phase de configuration initiale du serveur, le gestionnaire DHCP permet de placer un bloc (ou plage) d'adresses IP sous le contrôle du service DHCP en indiquant simplement le nombre total d'adresses et la première adresse du bloc. Le gestionnaire DHCP ajoute une liste d'adresses contiguës à partir de ces informations. Si vous avez plusieurs blocs d'adresses non contiguës, vous pouvez ajouter d'autres blocs contigus en exécutant à nouveau l'assistant d'ajout d'adresses du gestionnaire DHCP, à l'issue de la configuration initiale.

Avant de configurer vos adresses IP, vous devez savoir combien le bloc initial compte d'adresses et connaître l'adresse IP de la première adresse du bloc.

Génération des noms d'hôtes clients

Étant donné que DHCP est un service dynamique, l'adresse IP n'est pas associée de façon définitive au nom d'hôte du système qui l'utilise. Les outils de gestion DHCP offrent une option permettant de générer un nom de client à associer à chaque adresse IP. Les noms des clients se composent d'un préfixe, ou nom root, d'un tiret et d'un numéro attribué par le serveur. Si le nom root est `charlie`, par exemple, les noms des clients sont `charlie-1`, `charlie-2`, `charlie-3`, et ainsi de suite.

Par défaut, les noms de clients générés commencent par le nom du serveur DHCP chargé de leur administration. Cette technique est pratique dans les environnements disposant de plusieurs serveurs DHCP, car vous pouvez identifier rapidement dans les tables de réseau DHCP les clients gérés par chaque serveur DHCP. Il est possible, cependant, de remplacer le nom root par un nom de votre choix.

Avant de configurer vos adresses IP, décidez si vous voulez ou non que les outils de gestion DHCP génèrent les noms des clients et, le cas échéant, choisissez le nom root à utiliser à cet effet.

Vous pouvez faire correspondre les noms des clients générés à des adresses IP dans `/etc/inet/hosts` , DNS ou NIS+ si vous optez pour l'enregistrement des noms d'hôtes lors de la configuration du service DHCP. Pour plus d'informations, reportez-vous à la section "Enregistrement des noms d'hôtes clients" à la page 368.

Macros de configuration client par défaut

Dans DHCP, une *macro* est une collection d'options de configuration réseau définies par des valeurs. Le serveur DHCP utilise les macros pour déterminer les données de configuration du réseau à envoyer à un client DHCP.

Lorsque vous configurez le serveur DHCP, les outils de gestion rassemblent les informations nécessaires à partir des fichiers système et en s'adressant directement à vous par le biais des invites ou des options de ligne de commande que vous spécifiez. Ils produisent ensuite les macros suivantes :

- **Macro d'adresse réseau** : cette macro prend le nom de l'adresse IP du réseau client. Si le réseau s'appelle par exemple `192.68.0.0`, la macro d'adresse réseau s'appelle également `192.68.0.0`. Elle contient les informations nécessaires à tout client faisant partie du réseau : masque de sous-réseau, adresse de diffusion du réseau, routeur par défaut ou jeton de détection du routeur, mais aussi le domaine NIS/NIS+ et le serveur si celui-ci utilise un service NIS/NIS+. Elle peut également comprendre des options applicables à votre réseau. La macro d'adresse réseau est automatiquement traitée pour tous les clients situés sur ce réseau, comme cela est indiqué à la section "Ordre de traitement des macros" à la page 319.
- **Macro de localisation** : cette macro est appelée `Locale`. Elle contient le décalage (en secondes) par rapport au format UTC (temps universel), ce qui permet de calculer le fuseau horaire. Cette macro n'est pas traitée automatiquement, mais elle est incluse dans la macro de serveur.
- **Macro de serveur** : elle prend le nom d'hôte du serveur. Si le serveur s'appelle par exemple `pineola`, la macro de serveur s'appelle également `pineola`. Elle contient toutes les informations relatives à la stratégie de location, au serveur de temps, au domaine DNS et au serveur DNS, et éventuellement les autres données que le programme de configuration a pu recueillir à partir des fichiers système. Comme la macro de localisation est imbriquée à la macro de serveur, le serveur DHCP la traite en même temps que cette dernière.

  Lorsque vous configurez des adresses IP pour le premier réseau, vous devez choisir la macro de configuration client à appliquer à tous les clients DHCP utilisant les adresses en question. Un mappage (correspondance) est alors établi entre la macro que vous sélectionnez et les adresses IP. La macro sélectionnée par défaut est la macro du serveur, car c'est elle qui contient les informations requises par tous les clients exploitant ce serveur.

Les clients reçoivent les options contenues dans la macro d'adresse réseau avant les options de la macro mappée aux adresses IP. Cet ordre de traitement explique pourquoi les options de la macro du serveur sont prioritaires sur toute autre option conflictuelle dans la macro d'adresse réseau. Pour plus d'informations à ce sujet, reportez-vous à la section "Ordre de traitement des macros" à la page 319.

Choix entre un bail dynamique ou permanent

Le *type de bail* indique si la stratégie de location s'applique aux adresses IP que vous configurez. Lors de la phase de configuration initiale du serveur, pendant l'ajout des adresses, le gestionnaire DHCP vous donne le choix entre un bail dynamique ou permanent. Si vous configurez le serveur DHCP à l'aide de la commande `dhcpconfig`, les baux sont considérés comme dynamiques.

Lorsqu'une adresse IP bénéficie d'un *bail dynamique*, le serveur DHCP a le pouvoir de gérer cette adresse. Il peut allouer l'adresse IP à un client, prolonger son bail, détecter à quel moment elle n'est plus utilisée et récupérer l'adresse. Lorsqu'une adresse IP bénéficie d'un *bail permanent*, le serveur DHCP est simplement capable d'allouer l'adresse. Le client devient ensuite propriétaire de l'adresse jusqu'à ce qu'il soit tenu explicitement de la libérer. Dès que l'adresse est libre, le serveur a le droit de l'attribuer à un autre client. L'adresse n'est pas soumise à la stratégie de location tant qu'elle est associée à un type de bail permanent.

Lorsque vous configurez une plage d'adresses IP, le type de bail que vous choisissez s'applique à toutes les adresses de la plage. Pour tirer le meilleur parti possible du service DHCP, il est conseillé d'utiliser des baux dynamiques pour la plupart des adresses. Rien ne vous empêche ensuite de modifier les adresses de votre choix pour les louer de façon permanente. Il faut veiller, cependant, à limiter le nombre total de baux permanents.

Adresses IP réservées selon le type de bail

Il est possible de réserver des adresses IP en les attribuant manuellement à des clients spécifiques. Vous pouvez aussi bien associer un bail permanent qu'un bail dynamique à une adresse réservée. Si vous optez pour un bail permanent, les conditions suivantes s'appliquent :

- L'adresse peut uniquement être allouée au client qui lui est associé.
- Le serveur DHCP ne sera pas en mesure d'attribuer l'adresse à un autre client.
- L'adresse ne peut pas être récupérée par le serveur DHCP.

Si vous optez pour un bail dynamique, l'adresse réservée ne peut être allouée qu'au client qui lui est associé. Le client doit, toutefois, contrôler la durée du bail et négocier un prolongement comme si l'adresse n'était pas réellement réservée. Cette technique permet de savoir à quel moment le client utilise l'adresse en analysant le contenu de la table réseau.

Vous ne pouvez pas envisager des adresses réservées pour l'ensemble des adresses IP lors de la phase de configuration initiale. Les adresses réservées doivent être employées dans certains cas de figure uniquement.

Planification pour plusieurs serveurs DHCP

Si vous souhaitez configurer plusieurs serveurs DHCP pour gérer vos adresses IP, tenez compte des consignes suivantes :

- Divisez le pool d'adresses IP de façon à confier à chaque serveur la gestion d'une plage d'adresses précise en évitant tout conflit.
- Choisissez le service NIS+ en guise de magasin de données, s'il est disponible. Sinon, sélectionnez des fichiers texte et spécifiez un répertoire partagé comme chemin d'accès absolu au magasin de données. Le magasin de données des fichiers binaires n'est pas partageable.
- Configurez chaque serveur séparément pour octroyer correctement la propriété des adresses et permettre la création automatique des macros basées sur le serveur.
- Configurez les serveurs de façon à ce qu'ils puissent analyser les options et les macros dans la table `dhcptab` aux intervalles prévus et bénéficier ainsi des dernières informations disponibles. Vous pouvez vous servir du gestionnaire DHCP pour programmer la lecture automatique de la table `dhcptab` comme indiqué à la section "Personnalisation des options de performance pour le serveur DHCP" à la page 369.
- Assurez-vous que tous les clients sont en mesure d'accéder à l'ensemble des serveurs DHCP pour permettre à ces derniers de se substituer les uns aux autres en cas de besoin. Un client détenteur d'un bail valide pour une adresse peut essayer de valider sa configuration ou de prolonger son bail s'il ne parvient pas à joindre le serveur auquel appartient l'adresse du client. Un autre serveur peut répondre au client lorsque celui-ci n'a pas réussi à contacter le serveur principal au bout de 20 secondes. Si un client demande une adresse IP particulière et que le serveur ayant la propriété de l'adresse n'est pas disponible, un des autres serveurs traite la requête. Dans ce cas, le client ne reçoit pas l'adresse demandée. Il obtient l'adresse IP appartenant au serveur DHCP qui s'est chargé de lui répondre.

Planification de la configuration DHCP de vos réseaux distants

Après la phase de configuration DHCP initiale, vous avez la possibilité de placer des adresses IP sous le contrôle DHCP sur des réseaux distants. Cependant, comme les fichiers système ne sont pas disponibles localement, le gestionnaire DHCP et l'utilitaire `dhcpconfig` ne peuvent pas y rechercher les informations nécessaires et proposer des valeurs par défaut. C'est à vous alors de fournir ces informations. Avant de commencer à configurer un réseau distant, vous devez avoir connaissance des informations suivantes :

- Adresse IP du réseau distant.
- Masque de sous-réseau du réseau distant. Cette information peut être obtenue à partir de la table `netmasks` du service de noms. Si le réseau utilise des fichiers locaux, recherchez cette information dans `/etc/netmasks` sur un système du réseau. Si le réseau a recours au service NIS+, servez-vous de la commande `niscat netmasks.org_dir`. Si le réseau a recours au service NIS, exécutez la commande `ypcat -k netmasks.byaddr`. Vérifiez si la table `netmasks` contient bien toutes les données de topologie pour l'ensemble des sous-réseaux à gérer.
- Type de réseau. Les clients communiquent avec le réseau par l'intermédiaire d'une connexion locale (LAN) ou grâce au protocole point à point (PPP).
- Informations de routage. Les clients sont-ils capables de procéder à la détection du routeur ? Si ce n'est pas le cas, vous devez déterminer l'adresse IP d'un routeur qu'ils sont susceptibles d'exploiter.
- Domaine NIS et serveurs NIS, le cas échéant.
- Domaine NIS+ et serveurs NIS+, le cas échéant.

Pour savoir comment ajouter des réseaux, reportez-vous à la section "Ajout de réseaux DHCP" à la page 374.

Choix de l'outil de configuration du serveur DHCP

Après avoir réuni toutes les informations nécessaires et planifié le service DHCP, vous êtes prêt à configurer un serveur DHCP. Pour ce faire, vous pouvez faire appel au gestionnaire DHCP ou à l'utilitaire de ligne de commande `dhcpconfig`. Le gestionnaire DHCP permet de sélectionner des options et de spécifier les données qui serviront à créer la table `dhcptab` et les tables de réseau utilisées par le serveur DHCP. L'utilitaire `dhcpconfig` vous demande de spécifier les données à l'aide des options de ligne de commande.

Fonctionnalités du gestionnaire DHCP

Le gestionnaire DHCP, outil graphique basé sur la technologie Java™, offre un assistant de configuration DHCP. Cet assistant démarre automatiquement la première fois que vous exécutez le gestionnaire DHCP sur un système non configuré comme serveur DHCP. L'assistant de configuration DHCP affiche une série de boîtes de dialogue demandant des informations essentielles pour configurer un serveur : format du magasin de données, stratégie de location, serveurs et domaines DNS/NIS/NIS+ et adresses des routeurs. L'assistant est capable de collecter directement certaines informations à partir des fichiers système. Il vous suffit de confirmer que les informations sont correctes ou de les corriger, si nécessaire.

Le démon du serveur DHCP démarre sur le système serveur dès que vous aurez passé en revue toutes les boîtes de dialogue et validé les informations demandées. Vous êtes alors invité à lancer l'assistant d'ajout d'adresses pour configurer les adresses IP pour le réseau. Seul le réseau du serveur est configuré pour DHCP au départ. Les autres options de serveur prennent des valeurs par défaut. Une fois la configuration initiale terminée, exécutez à nouveau le gestionnaire DHCP pour ajouter des réseaux et modifier les autres options de serveur.

Pour plus d'informations au sujet de l'assistant de configuration DHCP, reportez-vous à la section "Configuration et annulation de la configuration d'un serveur DHCP avec le gestionnaire DHCP" à la page 339 Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "À propos du gestionnaire DHCP" à la page 352.

Fonctionnalités de l'utilitaire `dhcpconfig`

L'utilitaire `dhcpconfig` prend en charge les options servant à configurer et à annuler la configuration d'un serveur DHCP et permet de convertir les données du magasin de données sous un nouveau format ou bien d'importer/exporter des données depuis/vers d'autres serveurs DHCP. Lorsque vous configurez un serveur DHCP au moyen de l'utilitaire `dhcpconfig`, celui-ci recherche les informations appropriées dans les fichiers système indiqués à la section "Mises à jour des fichiers système et des tables de masques de réseau" à la page 324. Il n'est pas possible de visualiser et de confirmer les informations obtenues à partir des fichiers système, comme vous pourriez le faire avec le gestionnaire DHCP. Il est donc important de s'assurer que les fichiers sont à jour avant d'exécuter `dhcpconfig`. Vous pouvez également vous servir des options de la ligne de commande pour remplacer les valeurs que l'utilitaire `dhcpconfig` obtient par défaut des fichiers système. La commande `dhcpconfig` peut être utilisée au sein de scripts. Pour plus d'informations, reportez-vous à la page de manuel `dhcpconfig(1M)`.

Comparaison entre le gestionnaire DHCP et `dhcpconfig`

Le tableau suivant récapitule les différences entre les deux outils de configuration du serveur.

TABLEAU 13–4 Comparaison entre le gestionnaire DHCP et la commande `dhcpconfig`

Fonctionnalité	Gestionnaire DHCP	`dhcpconfig` avec options
Informations réseau collectées à partir du système.	Permet d'afficher les informations recueillies à partir des fichiers système et d'y apporter des modifications, si nécessaire.	Vous pouvez spécifier les informations du réseau à l'aide des options de ligne de commande.
Vitesse de configuration.	Accélère la procédure de configuration en omettant d'afficher les invites pour les options de serveur non primordiales et en utilisant à la place des valeurs par défaut. Vous pouvez changer les options qui ne sont pas essentielles après la phase de configuration initiale.	La procédure de configuration est plus rapide, mais il faudra éventuellement spécifier les valeurs de nombreuses options.

Le Chapitre 14, “Configuration du service DHCP (tâches)” indique les procédures à suivre pour configurer votre serveur avec le gestionnaire DHCP ou l'utilitaire `dhcpconfig`.

◆ ◆ ◆ CHAPITRE 14

Configuration du service DHCP (tâches)

En configurant le service DHCP sur votre réseau, vous configurez et démarrez le premier serveur DHCP. Vous pourrez par la suite ajouter d'autres serveurs DHCP en leur donnant accès aux mêmes données depuis un emplacement partagé, à condition que le magasin de données gère les données partagées. Ce chapitre décrit les différentes tâches qu'il est nécessaire d'effectuer pour configurer le serveur DHCP et placer les réseaux et les adresses IP associées sous le contrôle de DHCP. Il explique également comment annuler la configuration d'un serveur DHCP.

Chaque tâche inclut une procédure vous aidant à réaliser l'opération dans le gestionnaire DHCP ainsi qu'une procédure détaillant la tâche équivalente avec l'utilitaire de ligne de commande `dhcpconfig`. Le présent chapitre contient les informations suivantes :

Si vous avez des difficultés à configurer le service DHCP, reportez-vous au Chapitre 17, "Résolution des problèmes DHCP (référence)".

Après avoir configuré le service DHCP, reportez-vous au Chapitre 15, "Administration de DHCP (tâches)" pour plus d'informations sur la gestion du service DHCP.

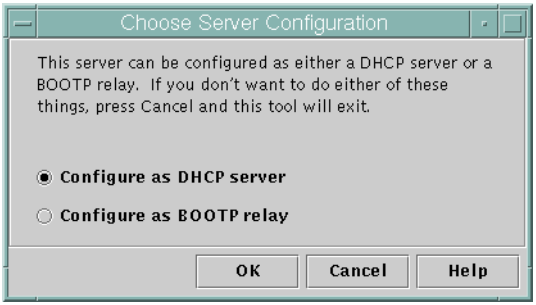
Configuration et annulation de la configuration d'un serveur DHCP avec le gestionnaire DHCP

Cette section présente les procédures permettant de configurer et d'annuler la configuration d'un serveur DHCP à l'aide du gestionnaire DHCP. Pour accéder au gestionnaire DHCP, il est indispensable d'exécuter un système X Window tel que le CDE ou GNOME.

Il est possible d'exécuter le gestionnaire DHCP en tant que superutilisateur grâce à la commande `/usr/sadm/admin/bin/dhcpmgr` . Pour obtenir des informations générales au sujet de cet utilitaire, reportez-vous à la section "À propos du gestionnaire DHCP" à la page 352 Pour obtenir des instructions détaillées sur l'exécution du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du service DHCP (gestionnaire DHCP)" à la page 357.

Lorsque vous exécutez le gestionnaire DHCP sur un serveur non configuré pour DHCP, l'écran suivant s'affiche. Vous pouvez choisir de configurer un serveur DHCP ou un agent de relais BOOTP.

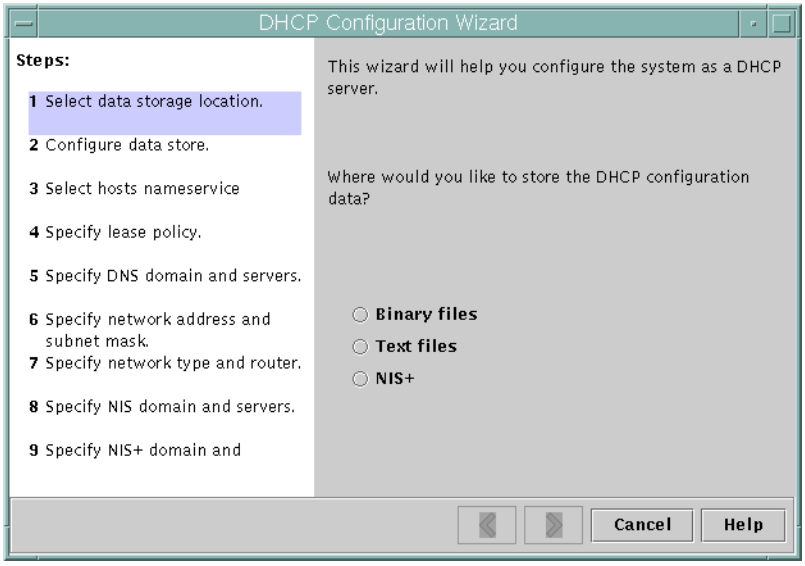
FIGURE 14–1 Boîte de dialogue de sélection de la configuration du serveur dans le gestionnaire DHCP



Configuration de serveurs DHCP

Lorsque vous configurez un serveur DHCP, le gestionnaire DHCP vous invite à spécifier les informations nécessaires par le biais de l'assistant de configuration DHCP. L'écran initial de l'assistant est semblable à celui de la figure suivante.

FIGURE 14–2 Écran initial de l'assistant de configuration DHCP



Dès que vous avez terminé de répondre aux invites de l'assistant, le gestionnaire DHCP crée les éléments présentés dans le tableau qui suit.

TABLEAU 14–1 Éléments créés lors de la configuration du serveur DHCP

Élément	Description	Contenu
Fichier de configuration du service, `/etc/inet/dhcpsvc.conf`	Stocke les mots-clés et les valeurs des options de configuration du serveur.	Type et emplacement du magasin de données et options utilisées avec `in.dhcpd` pour lancer le démon DHCP au démarrage du système. Ce fichier ne doit pas être édité manuellement. Pour modifier les données de configuration DHCP, utilisez impérativement `dhcpmgr` ou `dhcpconfig`.
Table `dhcptab`	Le gestionnaire DHCP crée la table `dhcptab` si celle-ci n'existe pas déjà.	Macros et options avec les valeurs qui leur sont assignées.
Macro de localisation (facultative), appelée aussi `Locale`	Indique le décalage horaire en secondes par rapport au temps universel (UTC).	Option `UTCoffst` avec le nombre de secondes assigné.

TABLEAU 14–1 Éléments créés lors de la configuration du serveur DHCP *(Suite)*

Élément	Description	Contenu
Macro de serveur dont le nom correspond au nom du noeud du serveur.	Contient les options pour lesquelles les valeurs sont déterminées par les entrées de l'administrateur ayant configuré le serveur DHCP. Les options s'appliquent à tous les clients exploitant les adresses appartenant au serveur.	Macro `locale`, plus les options suivantes : ■ `Timeserv`, configurée pour pointer vers l'adresse IP principale du serveur. ■ `LeaseTim`, configurée pour correspondre à la durée en secondes des baux. ■ `LeaseNeg`, si vous avez choisi des baux négociables. ■ `DNSdmain` et `DNSserv`, si le service DNS est configuré. ■ `Hostname`, option à laquelle *aucune* valeur ne doit être assignée. La présence de cette option indique que le nom d'hôte doit être obtenu à partir du service de noms.
Macro d'adresse réseau portant le même nom que l'adresse réseau du réseau du client.	Contient les options pour lesquelles les valeurs sont déterminées par les entrées de l'administrateur ayant configuré le serveur DHCP. Les options s'appliquent à tous les clients résidant sur le réseau spécifié par le nom de la macro.	Options suivantes : ■ `Subnet`, configurée pour correspondre au masque de sous-réseau du sous-réseau local ■ `Router`, configurée pour correspondre à l'adresse IP d'un routeur, ou `RDiscvyF` pour demander au client de procéder à la détection du routeur. ■ `Broadcst`, configurée pour correspondre à l'adresse IP de diffusion. Cette option est présente à condition qu'il ne s'agisse pas d'un réseau point à point. ■ `MTU`, pour l'unité de transmission maximale ■ `NISdmain` et `NISservs`, si le service NIS est configuré. ■ `NIS+dom` et `NIS+serv`, si le service NIS+ est configuré.
Table de réseau	La table reste vide tant que vous ne créez pas d'adresses IP pour le réseau.	Aucun contenu tant qu'aucune adresse IP n'est ajoutée.

▼ Configuration d'un serveur DHCP (gestionnaire DHCP)

Avant de commencer

Veuillez lire le Chapitre 13, “Planification pour le service DHCP (liste des tâches)” avant de configurer votre serveur DHCP. Conformez-vous notamment aux instructions de la section “Décisions relatives à la configuration de votre serveur DHCP (liste des tâches)” à la page 326 afin de réaliser les tâches suivantes :

- Sélectionner le système qui fera office de serveur DHCP ;
- Définir votre magasin de données, la stratégie de location et les informations du routeur.

1. **Connectez-vous au système serveur en tant que superutilisateur.**

2. **Lancez le gestionnaire DHCP.**

   ```
   #/usr/sadm/admin/bin/dhcpmgr &
   ```

3. **Choisissez l'option de configuration en tant que serveur DHCP.**

   Cela a pour effet de lancer l'assistant de configuration DHCP.

4. **Sélectionnez les options correspondantes ou saisissez les informations demandées, en fonction des décisions prises lors de la phase de planification.**

   En cas de problème, n'hésitez pas à cliquer sur Aide dans la fenêtre de l'assistant afin d'ouvrir votre navigateur Web et d'afficher de l'aide pour l'assistant de configuration DHCP.

5. **Après avoir indiqué les informations requises, terminez la configuration du serveur en cliquant sur le bouton correspondant.**

6. **Lorsque vous êtes invité à démarrer l'assistant d'ajout d'adresses, cliquez sur Oui pour configurer les adresses IP du serveur.**

   L'assistant d'ajout d'adresses au réseau permet de spécifier les adresses à placer sous le contrôle de DHCP.

7. **Répondez aux invites en fonction des décisions prises lors de la phase de planification.**

   Pour plus d'informations, reportez-vous à la section “Décisions relatives à la gestion des adresses IP (liste des tâches)” à la page 330. En cas de problème, n'hésitez pas à cliquer sur le bouton d'aide dans la fenêtre de l'assistant afin d'ouvrir votre navigateur Web et d'afficher de l'aide pour l'assistant d'ajout d'adresses au réseau.

8. **Vérifiez vos sélections, puis cliquez sur le bouton de fin pour ajouter les adresses IP à la table de réseau.**

   Cela a pour effet de mettre à jour les enregistrements de la table de réseau pour chacune des adresses comprises dans la plage spécifiée.

Voir aussi Vous pouvez ajouter d'autres réseaux au serveur DHCP à l'aide de l'assistant de configuration du réseau, en procédant comme indiqué dans la section "Ajout de réseaux DHCP" à la page 374.

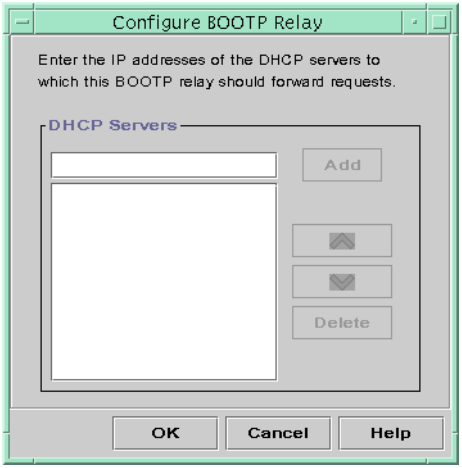
Configuration des agents de relais BOOTP

Lorsque vous configurez un agent de relais BOOTP, le gestionnaire DHCP effectue les actions suivantes :

- Il demande l'adresse IP d'un ou de plusieurs serveurs DHCP vers lesquels les requêtes doivent être relayées.
- Il enregistre les paramètres nécessaires au service de relais BOOTP.

La figure suivante présente l'écran affiché lorsque vous choisissez de configurer un agent de relais BOOTP.

FIGURE 14–3 Boîte de dialogue de configuration des agents de relais BOOTP dans le gestionnaire DHCP



▼ Configuration d'un agent de relais BOOTP (gestionnaire DHCP)

Avant de commencer Veuillez lire le Chapitre 13, "Planification pour le service DHCP (liste des tâches)" avant de configurer votre agent de relais BOOTP. Référez-vous notamment à la section "Sélection de l'hôte réservé au service DHCP" à la page 327 pour déterminer le système qu'il convient d'utiliser.

1 Connectez-vous au système serveur en tant que superutilisateur.

2 **Démarrez le gestionnaire DHCP.**

```
#/usr/sadm/admin/bin/dhcpmgr &
```

Si le système n'a pas été configuré comme serveur DHCP ou comme agent de relais BOOTP, l'assistant de configuration DHCP démarre. Si le système a déjà été configuré comme serveur DHCP, vous devez commencer par annuler la configuration du serveur. Pour plus d'informations, reportez-vous à la section "Annulation de la configuration des serveurs DHCP et des agents de relais BOOTP" à la page 345.

3 **Sélectionnez l'option de configuration en tant qu'agent de relais BOOTP.**

Cela a pour effet d'ouvrir la boîte de dialogue de configuration de l'agent de relais BOOTP.

4 **Saisissez l'adresse IP ou le nom d'hôte d'un ou plusieurs serveurs DHCP, puis cliquez sur le bouton d'ajout.**

Seuls les serveurs DHCP configurés sont capables de traiter les requêtes BOOTP ou DHCP reçues par cet agent de relais BOOTP.

5 **Cliquez sur OK pour quitter la boîte de dialogue.**

Dans le gestionnaire DHCP, vous disposez uniquement du menu Fichier pour quitter l'application et du menu Service pour gérer le serveur. Les options de menu désactivées ne présentent un intérêt que sur un serveur DHCP.

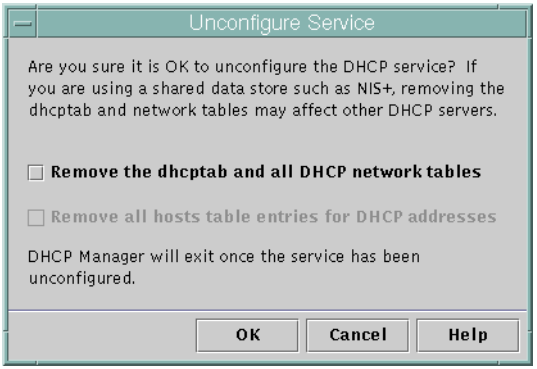
Annulation de la configuration des serveurs DHCP et des agents de relais BOOTP

Lorsque vous annulez la configuration d'un serveur DHCP ou d'un agent de relais BOOTP, le gestionnaire DHCP effectue les actions suivantes :

- Il arrête le processus du démon DHCP (`in.dhpcd`).
- Il supprime le fichier `/etc/inet/dhcpsvc.conf`, dans lequel sont consignées les informations au sujet du démarrage du démon et de l'emplacement du magasin de données.

La figure suivante présente l'écran affiché lorsque vous choisissez d'annuler la configuration d'un serveur DHCP.

FIGURE 14–4 Boîte de dialogue d'annulation de la configuration de service dans le gestionnaire DHCP



Données DHCP sur un serveur non configuré

Lorsque vous annulez la configuration d'un serveur DHCP, vous devez indiquer comment traiter la table `dhcptab` et les tables de réseau DHCP. Si les données sont partagées entre plusieurs serveurs, ne supprimez ni la table `dhcptab`, ni les tables de réseau DHCP. En cas de suppression des tables, DHCP deviendrait inutilisable sur votre réseau. Les données peuvent être partagées par le biais de NIS+ ou sur des systèmes de fichiers locaux exportés. Le fichier `/etc/inet/dhcpsvc.conf` contient le nom et l'emplacement du magasin de données utilisé.

Vous pouvez annuler la configuration d'un serveur DHCP en laissant les données intactes (il suffit pour cela de ne pas sélectionner les options de suppression des données). Si tel est votre choix, vous désactivez le serveur DHCP.

Si vous souhaitez transférer la propriété des adresses IP à un autre serveur DHCP, vous devez déplacer les données DHCP vers le serveur DHCP en question. N'oubliez pas de le faire avant d'annuler la configuration du serveur actuel. Pour plus d'informations à ce sujet, reportez-vous à la section "Transfert des données de configuration entre serveurs DHCP (liste de tâches)" à la page 427.

Si vous voulez vraiment effacer les données, il suffit de sélectionner une des options permettant de supprimer la table `dhcptab` et les tables de réseau. Si vous aviez généré des noms de clients pour les adresses DHCP, vous pouvez décider de supprimer ces entrées de la table des hôtes. Il est possible d'effacer les entrées correspondant aux noms des clients dans DNS, `/etc/inet/hosts` ou NIS+.

Avant d'annuler la configuration d'un agent de relais BOOTP, assurez-vous qu'aucun client n'utilise cet agent pour transférer les requêtes vers un serveur DHCP.

▼ Annulation de la configuration d'un serveur DHCP ou d'un agent de relais BOOTP (gestionnaire DHCP)

1. **Prenez le rôle de superutilisateur.**

2. **Lancez le gestionnaire DHCP.**

   ```
   #/usr/sadm/admin/bin/dhcpmgr &
   ```

3. **Choisissez l'option d'annulation de la configuration dans le menu Service.**

   La boîte de dialogue correspondante s'affiche. Si le serveur est un agent de relais BOOTP, la boîte de dialogue permet de confirmer l'annulation de la configuration de l'agent de relais. S'il s'agit, en revanche, d'un serveur DHCP, vous devez choisir comment traiter les données DHCP et effectuer des sélections dans la boîte de dialogue. Reportez-vous à la Figure 14–4.

4. **(Facultatif) Sélectionnez les options de suppression des données.**

   Si le serveur utilise des données partagées via NIS+ ou dans des fichiers partagés via NFS, il est recommandé de conserver les données. Si le serveur n'exploite pas de données partagées, vous pouvez alors envisager leur suppression en sélectionnant une ou les deux options proposées.

   Pour plus d'informations sur la suppression des données, reportez-vous à la section "Données DHCP sur un serveur non configuré" à la page 346.

5. **Cliquez sur OK pour annuler la configuration du serveur.**

   Cela a pour effet de fermer la boîte de dialogue d'annulation de la configuration de service et de quitter le gestionnaire DHCP.

Configuration et annulation de la configuration d'un serveur DHCP à l'aide des commandes dhcpconfig

Cette section vous aide à configurer et à annuler la configuration d'un serveur DHCP ou d'un agent de relais BOOTP à l'aide de dhcpconfig et des options de ligne de commande.

▼ Configuration d'un serveur DHCP (dhcpconfig -D)

Avant de commencer

Veuillez lire le Chapitre 13, "Planification pour le service DHCP (liste des tâches)" avant de configurer votre serveur DHCP. Conformez-vous notamment aux instructions de la section "Décisions relatives à la configuration de votre serveur DHCP (liste des tâches)" à la page 326 afin de réaliser les tâches suivantes :

- Sélectionner le système qui fera office de serveur DHCP ;
- Définir votre magasin de données, la stratégie de location et les informations du routeur.

1 Connectez-vous au système sur lequel vous souhaitez configurer le serveur DHCP.

2 Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 Configurez le serveur DHCP en entrant une commande au format suivant :

`#/usr/sbin/dhcpconfig -D -r` *datastore* **`-p`** *location*

magasin de données doit correspondre à l'une des valeurs suivantes : `SUNWfiles`, `SUNWbinfiles` ou `SUNWnisplus`.

emplacement désigne l'endroit lié au magasin de données dans lequel vous souhaitez conserver les données DHCP. Dans le cas des magasins de données `SUNWfiles` et `SUNWbinfiles`, vous devez impérativement spécifier un nom de chemin absolu. Pour `SUNWnisplus`, il doit s'agir d'un chemin de répertoire NIS+ complet.

Vous pourriez, par exemple, saisir une commande similaire à la suivante :

```
dhcpconfig -D -r SUNWbinfiles -p /var/dhcp
```

L'utilitaire `dhcpconfig` se sert des fichiers système et des fichiers de réseau de l'hôte pour déterminer les valeurs employées pour configurer le serveur DHCP. Reportez-vous à la page de manuel `dhcpconfig(1M)` pour connaître les options supplémentaires qu'il est possible d'associer à la commande `dhcpconfig` afin de remplacer les valeurs par défaut.

4 Ajoutez un ou plusieurs réseaux au service DHCP.

Pour savoir comment procéder, reportez-vous à la section "Ajout d'un réseau DHCP (`dhcpconfig`)" à la page 377.

▼ Configuration d'un agent de relais BOOTP (dhcpconfig -R)

Avant de commencer Sélectionnez le système que vous comptez utiliser comme agent de relais BOOTP, en tenant compte des conditions indiquées dans la section "Sélection de l'hôte réservé au service DHCP" à la page 327.

1. **Connectez-vous au serveur que vous souhaitez configurer comme agent de relais BOOTP.**

2. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3. **Configurez l'agent de relais BOOTP en entrant une commande au format suivant :**

   `# /usr/sbin/dhcpconfig -R` *server-addresses*

   Spécifiez une ou plusieurs adresses IP de serveurs DHCP vers lesquels vous désirez transférer les requêtes. Si vous indiquez plusieurs adresses, séparez-les par des virgules.

   Vous pourriez, par exemple, saisir une commande similaire à la suivante :

   ```
   /usr/sbin/dhcpconfig -R 192.168.1.18,192.168.42.132
   ```

▼ Annulation de la configuration d'un serveur DHCP ou d'un agent de relais BOOTP (dhcpconfig -U)

1. **Connectez-vous au système (serveur DHCP ou agent de relais BOOTP) dont vous souhaitez annuler la configuration.**

2. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 Annulez la configuration du serveur DHCP ou de l'agent de relais BOOTP :

```
# /usr/sbin/dhcpconfig -U
```

Si le serveur n'utilise pas de données partagées, vous pouvez également employer l'option `-x` pour supprimer la table `dhcptab` et les tables de réseau. Si le serveur utilise des données partagées, l'option `-x` est à proscrire. L'option `-h` permet quant à elle d'effacer les noms d'hôtes dans la table des hôtes. Pour plus d'informations sur les options `dhcpconfig`, reportez-vous à la page de manuel `dhcpconfig(1M)`.

Pour plus d'informations sur la suppression des données, reportez-vous à la section "Données DHCP sur un serveur non configuré" à la page 346.

◆ ◆ ◆ CHAPITRE 15

Administration de DHCP (tâches)

Ce chapitre décrit les différentes tâches que vous aurez besoin d'effectuer pour gérer le service DHCP. Ces tâches concernent aussi bien le serveur que l'agent de relais BOOTP et le client. Chaque tâche inclut une procédure vous aidant à réaliser la tâche dans le gestionnaire DHCP ainsi qu'une procédure détaillant la tâche équivalente avec les utilitaires de ligne de commande DHCP. Les utilitaires de ligne de commande DHCP sont décrits de façon approfondie dans les pages de manuel.

Avant de lire ce chapitre, vous devez d'abord avoir effectué la configuration initiale du service DHCP et du réseau. Le Chapitre 14, “Configuration du service DHCP (tâches)” traite de la configuration DHCP.

Le présent chapitre contient les informations suivantes :

À propos du gestionnaire DHCP

Le gestionnaire DHCP est une interface graphique (IG) très pratique pour procéder aux opérations d'administration du service DHCP.

Fenêtre du gestionnaire DHCP

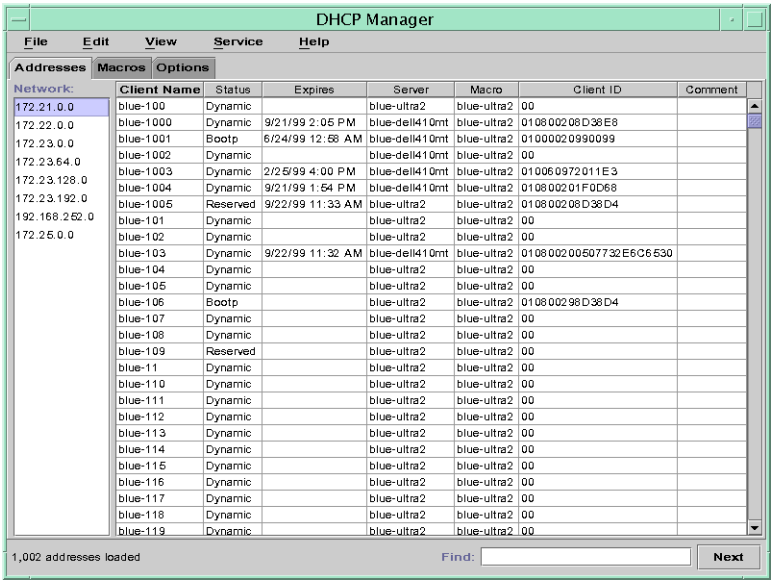
L'aspect de la fenêtre du gestionnaire DHCP dépend de la façon dont le serveur DHCP est configuré sur le système réservé au gestionnaire DHCP.

Le gestionnaire DHCP utilise une fenêtre à onglets lorsque le système est configuré en tant que serveur DHCP. Il suffit de cliquer sur l'onglet correspondant au type d'information qui vous intéresse. Le gestionnaire DHCP offre les onglets suivants :

- Onglet **Addresses** – Il répertorie l'ensemble des réseaux et des adresses IP sous le contrôle du service DHCP. Cet onglet permet de gérer les réseaux et les adresses IP. Vous pouvez ajouter ou supprimer des éléments de façon individuelle ou en bloc. Vous avez également la possibilité de changer individuellement les propriétés des réseaux ou des adresses IP ou d'appliquer simultanément la même modification à un bloc d'adresses. Vous accédez automatiquement à l'onglet Addresses au démarrage du gestionnaire DHCP.
- Onglet **Macros** – Il présente l'ensemble des macros disponibles dans la table de configuration DHCP (`dhcptab`) ainsi que les options utilisées au sein des macros. Cet onglet permet de créer ou de supprimer des macros. Vous pouvez également modifier des macros en ajoutant des options et en donnant des valeurs aux options.
- Onglet **Options** – Il récapitule toutes les options définies pour ce serveur DHCP. Les options présentées dans cet onglet ne sont pas les options standard définies dans le protocole DHCP. Il s'agit d'extensions des options standard. Elles font partie de la classe Extended, Vendor ou Site. Il est impossible de modifier les options standard. C'est la raison pour laquelle elles ne figurent pas dans cette liste.

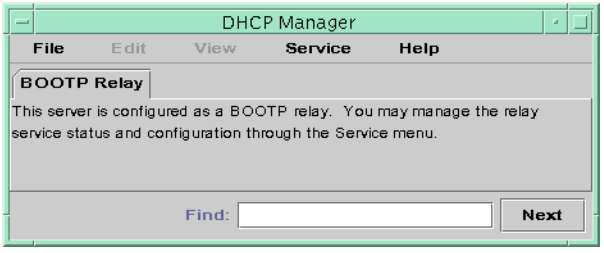
La figure suivante illustre une des présentations possibles de la fenêtre du gestionnaire DHCP lorsque vous lancez le gestionnaire DHCP sur un serveur DHCP.

FIGURE 15–1 Gestionnaire DHCP sur un système serveur DHCP



Lorsque le serveur est configuré en tant qu'agent de relais BOOTP, la fenêtre du gestionnaire DHCP n'affiche pas ces onglets. L'agent de relais BOOTP n'a pas besoin, en effet, des mêmes informations. Vous pouvez uniquement modifier les propriétés de l'agent de relais BOOTP et démarrer ou arrêter le démon DHCP à l'aide du gestionnaire DHCP. La figure suivante illustre une des présentations possibles de la fenêtre du gestionnaire DHCP sur un système configuré en tant qu'agent de relais BOOTP.

FIGURE 15–2 Gestionnaire DHCP sur un agent de relais BOOTP



Menus du gestionnaire DHCP

Le gestionnaire DHCP propose les menus suivants :

- **File** – Permet de quitter le gestionnaire DHCP.
- **Edit** – Permet d'effectuer des tâches d'administration pour les réseaux, les adresses, les macros et les options.
- **View** – Permet de changer l'apparence de l'onglet actuellement sélectionné.
- **Service** – Permet de gérer le démon DHCP et le magasin de données.
- **Help** – Permet d'ouvrir votre navigateur Web et d'afficher de l'aide au sujet du gestionnaire DHCP.

L'exécution du gestionnaire DHCP sur un agent de relais BOOTP a pour effet de désactiver les menus Edit et View.

Toutes les tâches d'administration DHCP sont effectuées au moyen des menus Edit et Service.

Les commandes du menu Edit servent à créer, supprimer et modifier des éléments dans l'onglet sélectionné. Il peut s'agir, en l'occurrence, de réseaux, d'adresses, de macros et d'options. Lorsque vous cliquez sur l'onglet Addresses, le menu Edit affiche également la liste des assistants. Les assistants présentent un ensemble de boîtes de dialogue qui vous aident à créer des réseaux et des adresses IP.

Le menu Service contient les commandes de gestion du démon DHCP. Il permet de réaliser les tâches suivantes :

- Démarrer et arrêter le démon DHCP
- Activer et désactiver le démon DHCP
- Modifier la configuration du serveur
- Annuler la configuration du serveur
- Convertir le magasin de données
- Exporter et importer des données sur le serveur

Démarrage et arrêt du gestionnaire DHCP

Vous devez exécuter le gestionnaire DHCP sur un système serveur DHCP en tant que superutilisateur. Si vous êtes obligé d'exécuter le gestionnaire DHCP à distance, vous pouvez transférer l'affichage sur votre système au moyen de la fonction d'affichage à distance X Window.

▼ Démarrage et arrêt du gestionnaire DHCP

1 Prenez le rôle de superutilisateur sur le système serveur DHCP.

2. **(Facultatif) Si vous êtes connecté à distance au système serveur DHCP, affichez le gestionnaire DHCP sur votre système local comme suit.**

   a. **Entrez la commande suivante sur le système local :**

      `# xhost +`*server-name*

   b. **Entrez la commande suivante sur le système serveur DHCP distant :**

      `# DISPLAY=`*local-hostname*`;export DISPLAY`

3. **Lancez le gestionnaire DHCP.**

   ```
   # /usr/sadm/admin/bin/dhcpmgr &
   ```

   Cela a pour effet d'ouvrir la fenêtre du gestionnaire DHCP. Si le serveur est configuré en tant que serveur DHCP, la fenêtre contient l'onglet Addresses. Si le serveur est configuré en tant qu'agent de relais BOOTP, la fenêtre s'affiche sans onglet.

4. **Pour arrêter le gestionnaire DHCP, choisissez Exit dans le menu File.**

   Cela a pour effet de fermer la fenêtre du gestionnaire DHCP.

Configuration de l'accès utilisateur aux commandes DHCP

Par défaut, seul un utilisateur root ou superutilisateur peut exécuter les commandes `dhcpconfig`, `dhtadm` et `pntadm`. Pour que les utilisateurs non root puissent également les utiliser, il est possible de configurer le contrôle d'accès basé sur les rôles (RBAC) pour ces commandes.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

Les pages de manuel suivantes sont également des sources de référence intéressantes : `rbac(5)`, `exec_attr(4)` et `user_attr(4)`.

La procédure suivante explique comment attribuer le profil de gestion DHCP qui permet à l'utilisateur d'exécuter les commandes DHCP.

▼ Octroi de l'accès aux commandes DHCP

1. **Connectez-vous au système serveur DHCP en tant que superutilisateur.**

2. **Éditez le fichier `/etc/user_attr` afin d'y ajouter une entrée sous la forme suivante. Prévoyez une entrée pour chaque utilisateur ou rôle censé gérer le service DHCP.**

   username`::::type=normal;profiles=DHCP Management`

Voici, par exemple, l'entrée qu'il convient d'ajouter pour un utilisateur appelé `ram` :

```
ram::::type=normal;profiles=DHCP Management
```

Démarrage et arrêt du service DHCP

Cette section décrit comment démarrer et arrêter le service DHCP à l'aide du gestionnaire DHCP et de la commande `dhcpconfig`. Vous pouvez également obtenir les mêmes résultats à l'aide des commandes de l'utilitaire SMF (Service Management Facility). Pour plus d'informations à ce sujet, reportez-vous à la section "Service DHCP et utilitaire SMF" à la page 358.

Les commandes que vous appliquez au service DHCP auront des effets différents sur le fonctionnement du démon DHCP. Il est donc important de bien comprendre les implications de chaque action afin de sélectionner la procédure qui permette d'obtenir le résultat voulu. Vous devez faire la distinction entre les termes suivants :

- **Les commandes de démarrage, d'arrêt et de redémarrage** modifient le comportement du démon uniquement pour la session actuelle. Si vous arrêtez le service DHCP, par exemple, le démon cesse de fonctionner, mais redevient actif lors du prochain redémarrage du système. Les tables de données DHCP ne sont pas concernées par l'arrêt du service. Vous pouvez vous servir des commandes du gestionnaire DHCP ou de l'utilitaire SMF pour démarrer et arrêter temporairement le service DHCP sans pour autant l'activer et le désactiver.
- **Les commandes d'activation et de désactivation** ont une incidence sur le démon lors de la session actuelle et des prochaines sessions. Si vous désactivez le service DHCP, le démon en cours d'exécution cesse de fonctionner et ne redevient pas actif lorsque vous redémarrez le serveur. Vous devrez activer le démon DHCP si vous souhaitez à nouveau le lancer automatiquement au démarrage du système. Les tables de données DHCP ne sont pas affectées. Vous pouvez faire appel au gestionnaire DHCP, à la commande `dhcpconfig` ou aux commandes SMF pour activer et désactiver le service DHCP.
- La **commande d'annulation de la configuration** arrête le démon, empêche son exécution au redémarrage du système et permet en plus de supprimer les tables de données DHCP. Il y a deux façons d'annuler la configuration du service DHCP : à l'aide du gestionnaire DHCP ou de la commande `dhcpconfig`. La procédure d'annulation de la configuration est décrite au Chapitre 14, "Configuration du service DHCP (tâches)".

Remarque – Si un serveur dispose de plusieurs interfaces réseau, mais que vous ne désirez pas offrir des services DHCP au niveau de tous les réseaux, reportez-vous à la section "Spécification des interfaces réseau placées sous le contrôle DHCP" à la page 372.

Les procédures suivantes expliquent comment démarrer, arrêter, activer et désactiver le service DHCP.

▼ Démarrage et arrêt du service DHCP (gestionnaire DHCP)

1. **Connectez-vous au système serveur DHCP en tant que superutilisateur.**
2. **Lancez le gestionnaire DHCP.**

   ```
   # /usr/sadm/admin/bin/dhcpmgr &
   ```

3. **Sélectionnez l'une des options suivantes :**

   - **Choisissez Start dans le menu Service pour lancer le service DHCP.**
   - **Choisissez Stop dans le menu Service pour arrêter le service DHCP.**

     Le démon DHCP cesse de fonctionner jusqu'à ce que vous le relanciez ou que vous redémarriez le système.
   - **Choisissez Restart dans le menu Service pour arrêter et relancer immédiatement le service DHCP.**

▼ Activation et désactivation du service DHCP (gestionnaire DHCP)

- **Dans le gestionnaire DHCP, sélectionnez l'une des options suivantes :**

  - **Choisissez Enable dans le menu Service pour configurer le démon DHCP de façon à l'exécuter automatiquement au démarrage du système.**

    Le service DHCP démarre immédiatement lorsqu'il est activé.
  - **Choisissez Disable dans le menu Service pour empêcher l'exécution automatique du démon DHCP au démarrage du système.**

    Le service DHCP s'arrête immédiatement lorsqu'il est désactivé.

▼ Activation et désactivation du service DHCP (`dhcpconfig -S`)

1. **Connectez-vous au système serveur DHCP.**

2 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 **Sélectionnez l'une des options indiquées ci-dessous :**

- **Pour activer le service DHCP, entrez la commande suivante :**

```
# /usr/sbin/dhcpconfig -S -e
```

- **Pour désactiver le service DHCP, entrez la commande suivante :**

```
# /usr/sbin/dhcpconfig -S -d
```

Service DHCP et utilitaire SMF

L'utilitaire de gestion des services (SMF) est décrit au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base*. Il est possible de faire appel à la commande SMF `svcadm` pour activer et démarrer le serveur DHCP, ou bien le désactiver et l'arrêter. Les commandes SMF ne permettent pas, en revanche, de modifier les options du service DHCP que vous définissez à l'aide des outils DHCP. Cela est notamment le cas des options de service stockées dans le fichier `/etc/dhcp/dhcpsvc.conf`.

Le tableau suivant montre la correspondance entre les commandes DHCP et les commandes SMF équivalentes.

TABLEAU 15–1 Commandes SMF pour les tâches du serveur DHCP

Tâche	Commande DHCP	Commande SMF
Activation du service DHCP	`dhcpconfig -S -e`	`svcadm enable svc:/network/dhcp-server`
Désactivation du service DHCP	`dhcpconfig -S -d`	`svcadm disable svc:/network/dhcp-server`
Démarrage du service DHCP uniquement pour la session actuelle	Aucune	`svcadm enable -t svc:/network/dhcp-server`
Arrêt du service DHCP pour la session actuelle	Aucune	`svcadm disable -t svc:/network/dhcp-server`

TABLEAU 15–1 Commandes SMF pour les tâches du serveur DHCP *(Suite)*

Tâche	Commande DHCP	Commande SMF
Redémarrage du service DHCP	`dhcpconfig -S -r`	`svcadm restart svc:/network/dhcp-server`

Modification des options de service DHCP (liste des tâches)

Vous pouvez modifier les valeurs de certaines fonctions supplémentaires du service DHCP auxquelles vous n'avez peut-être pas eu accès lors de la configuration initiale avec le gestionnaire DHCP. Vous pouvez modifier les options de service à partir de la boîte de dialogue de modification des options de service dans le gestionnaire DHCP ou spécifier les options qui vous intéressent à l'aide de la commande `dhcpconfig`.

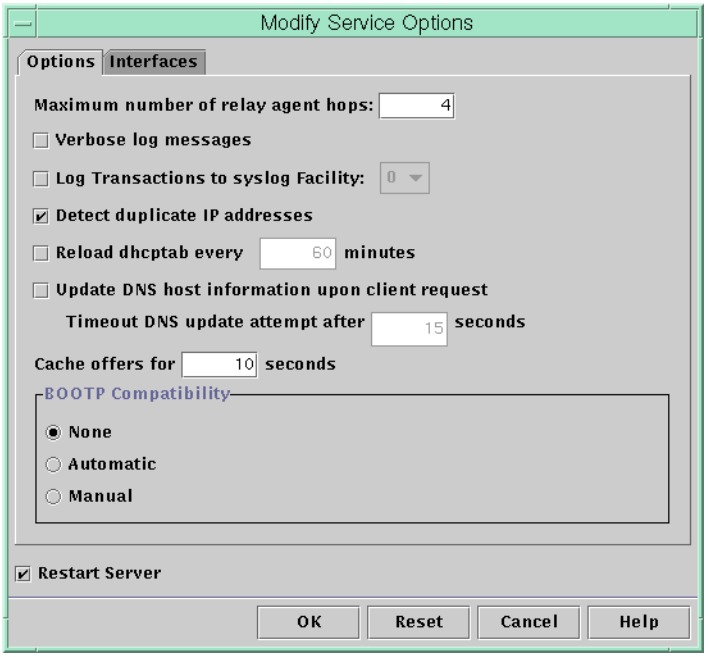
Le tableau suivant décrit la liste des tâches permettant de modifier les options de service DHCP. Le tableau comprend également des liens vers les procédures permettant d'effectuer chaque tâche.

Tâche	Description	Voir
Changement des options de journalisation.	Activez ou désactivez la journalisation et sélectionnez l'utilitaire `syslog` à exécuter pour consigner les transactions DHCP dans le journal.	"Génération des messages détaillés du fichier journal DHCP (gestionnaire DHCP)" à la page 362 "Génération des messages détaillés du fichier journal DHCP (ligne de commande)" à la page 363 "Activation et désactivation de la journalisation des transactions DHCP (gestionnaire DHCP)" à la page 363 "Activation et désactivation de la journalisation des transactions DHCP (ligne de commande)" à la page 364 "Journalisation des transactions DHCP dans un fichier `syslog` indépendant" à la page 365
Changement des options de mise à jour DNS.	Activez ou désactivez la fonction serveur permettant d'ajouter de façon dynamique des entrées DNS pour les clients fournissant un nom d'hôte. Indiquez le délai maximum dont le serveur dispose pour mettre à jour le service DNS.	"Activation de la mise à jour DNS dynamique pour les clients DHCP" à la page 367
Activation ou désactivation de la détection d'adresses IP en double.	Activez ou désactivez la capacité du serveur DHCP à déterminer si une adresse IP n'est pas déjà utilisée avant de la proposer à un client.	"Personnalisation des options de performance DHCP (gestionnaire DHCP)" à la page 370 "Personnalisation des options de performance DHCP (ligne de commande)" à la page 370

Tâche	Description	Voir
Redéfinition du mode de lecture des données de configuration par le serveur DHCP.	Activez ou désactivez la lecture automatique de `dhcptab` aux intervalles spécifiés ou changez l'intervalle entre chaque lecture.	"Personnalisation des options de performance DHCP (gestionnaire DHCP)" à la page 370 "Personnalisation des options de performance DHCP (ligne de commande)" à la page 370
Changement du nombre de sauts de l'agent de relais.	Augmentez ou réduisez le nombre de réseaux par lesquels une requête peut transiter avant d'être abandonnée par le démon DHCP.	"Personnalisation des options de performance DHCP (gestionnaire DHCP)" à la page 370 "Personnalisation des options de performance DHCP (ligne de commande)" à la page 370
Changement de la durée de mise en mémoire cache d'une offre d'adresse IP.	Augmentez ou réduisez la durée en secondes pendant laquelle le service DHCP garde en réserve une adresse IP avant de la proposer à un autre client.	"Personnalisation des options de performance DHCP (gestionnaire DHCP)" à la page 370 "Personnalisation des options de performance DHCP (ligne de commande)" à la page 370

La figure suivante représente la boîte de dialogue de modification des options de service du gestionnaire DHCP.

FIGURE 15–3 Boîte de dialogue de modification des options de service du gestionnaire DHCP



Modification des options de journalisation DHCP

Le service DHCP peut consigner les messages du service DHCP et les transactions DHCP dans `syslog`. Reportez-vous aux pages de manuel `syslogd(1M)` et `syslog.conf(4)` pour plus d'informations sur `syslog`.

Deux types de message du service DHCP sont consignés dans `syslog` :

- les messages d'erreur, qui vous avertissent des conditions empêchant le service DHCP de satisfaire une requête adressée par un client ou par vous-même ;
- les avertissements et les notifications, qui vous préviennent en cas de situation anormale, sans que cela n'empêche le service DHCP de répondre à une requête.

Vous avez la possibilité d'afficher un plus grand nombre d'informations en utilisant l'option du mode détaillé du démon DHCP. Des messages plus détaillés peuvent vous aider à résoudre les problèmes DHCP. Pour plus d'informations, reportez-vous à la section "Génération des messages détaillés du fichier journal DHCP (gestionnaire DHCP)" à la page 362.

Il peut également être utile de consigner les transactions dans un journal pour faciliter le dépannage. Les transactions donnent des informations au sujet de chaque échange effectué entre un serveur DHCP ou un agent de relais BOOTP et des clients. Voici les types de message indiqués dans les transactions DHCP :

- ASSIGN – Affectation d'adresse IP
- ACK – Accusé de réception du serveur attestant que le client accepte l'adresse IP proposée et envoi des paramètres de configuration par le serveur
- EXTEND – Extension du bail
- RELEASE – Libération de l'adresse IP
- DECLINE – Refus par le client de l'affectation d'adresse
- INFORM – Sollicitation par le client de paramètres de configuration réseau et non d'une adresse IP
- NAK – Non prise en compte par le serveur d'une requête du client désireux d'utiliser une adresse IP employée précédemment
- ICMP_ECHO – Détection par le serveur d'une adresse IP potentielle en cours d'utilisation par un autre hôte

Voici les types de message indiqués dans les transactions de l'agent de relais BOOTP :

- RELAY-CLNT – Message relayé du client DHCP vers un serveur DHCP
- RELAY–SRVR – Message relayé du serveur DHCP vers le client DHCP

La journalisation des transactions DHCP est désactivée par défaut. Lorsqu'elle est activée, elle fait appel par défaut à la fonction `local0` dans `syslog`. Le niveau de gravité `syslog` des messages de transaction DHCP générés correspond à *notice*. Cela signifie que les transactions

DHCP sont placées dans le fichier réservé aux autres notifications système. Comme la journalisation utilise la fonction `local`, les messages de transaction DHCP peuvent, cependant, être consignés à part. Pour ce faire, vous devez éditer le fichier `syslog.conf` afin de spécifier un fichier journal indépendant. Pour plus d'informations au sujet du fichier `syslog.conf`, reportez-vous à la page de manuel `syslog.conf(4)`.

Vous être libre de désactiver ou d'activer la journalisation des transactions et de changer la fonction `syslog` utilisée (entre `local0` et `local7`) comme indiqué à la section "Activation et désactivation de la journalisation des transactions DHCP (gestionnaire DHCP)" à la page 363. Dans le fichier `syslog.conf` du système serveur, vous pouvez également donner l'instruction à `syslogd` de stocker les messages de transaction DHCP dans un fichier à part. Pour plus d'informations, reportez-vous à la section "Journalisation des transactions DHCP dans un fichier `syslog` indépendant" à la page 365.

▼ Génération des messages détaillés du fichier journal DHCP (gestionnaire DHCP)

1 Choisissez Modify dans le menu Service du gestionnaire DHCP.

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

Vous accédez directement à l'onglet Options de la boîte de dialogue de modification des options de service. Reportez-vous à la Figure 15–3.

2 Sélectionnez Verbose Log Messages.

3 Choisissez ensuite Restart Server.

Cette option figure en bas de la boîte de dialogue.

4 Cliquez sur OK.

Le démon est exécuté en mode détaillé lors de cette session et de chacune des sessions suivantes jusqu'à ce que vous rétablissiez cette option. Le mode détaillé risque de limiter l'efficacité du démon en raison du délai nécessaire à l'affichage des messages.

▼ Génération des messages détaillés du fichier journal DHCP (ligne de commande)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Entrez la commande suivante pour configurer le mode détaillé :**

```
# /usr/sbin/dhcpconfig -P VERBOSE=true
```

Lors du prochain démarrage du serveur DHCP, celui-ci passe en mode détaillé jusqu'à ce que vous désactiviez ce mode.

Pour désactiver le mode détaillé, entrez la commande suivante :

```
# /usr/sbin/dhcpconfig -P VERBOSE=
```

Cette commande ne donne aucune valeur au mot-clé `VERBOSE`, ce qui a pour effet de supprimer le mot-clé du fichier de configuration du serveur.

Le mode détaillé risque de limiter l'efficacité du démon en raison du délai nécessaire à l'affichage des messages.

▼ Activation et désactivation de la journalisation des transactions DHCP (gestionnaire DHCP)

Cette procédure décrit comment activer et désactiver la journalisation des transactions dans le journal pour toutes les prochaines sessions serveur DHCP.

1 **Choisissez Modify dans le menu Service du gestionnaire DHCP.**

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2 **Sélectionnez Log Transactions to Syslog Facility.**

Pour désactiver la journalisation des transactions, il suffit de désélectionner cette option.

3 **(Facultatif) Sélectionnez une fonction locale comprise entre 0 et 7 à utiliser lors de la journalisation des transactions DHCP.**

Par défaut, les transactions DHCP sont stockées à l'emplacement prévu pour les notifications système, lequel dépend du mode de configuration de `syslogd`. Pour les consigner dans un fichier à part, reportez-vous à la section "Journalisation des transactions DHCP dans un fichier `syslog` indépendant" à la page 365.

Les fichiers de messages risquent très vite de devenir volumineux lorsque la journalisation des transactions est activée.

4 **Choisissez ensuite Restart Server.**

5 **Cliquez sur OK.**

Le démon consigne les transactions à l'emplacement `syslog` sélectionné pour cette session ainsi que pour chacune des sessions suivantes tant que vous ne désactivez pas la journalisation.

▼ Activation et désactivation de la journalisation des transactions DHCP (ligne de commande)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Procédez de l'une des façons suivantes :**

- **Pour activer la journalisation des transactions DHCP, entrez la commande suivante :**

```
# /usr/sbin/dhcpconfig -P LOGGING_FACILITY=syslog-local-facility
```

syslog-local-facility est un chiffre compris entre 0 et 7. Si vous omettez cette option, la valeur 0 est utilisée.

Par défaut, les transactions DHCP sont stockées à l'emplacement prévu pour les notifications système, lequel dépend du mode de configuration de `syslogd`. Pour les consigner dans un fichier à part, reportez-vous à la section "Journalisation des transactions DHCP dans un fichier `syslog` indépendant" à la page 365.

Les fichiers de messages risquent très vite de devenir volumineux lorsque la journalisation des transactions est activée.

- **Pour désactiver la journalisation des transactions DHCP, entrez la commande suivante :**

  ```
  # /usr/sbin/dhcpconfig -P LOGGING_FACILITY=
  ```

  Vous n'avez aucune valeur à spécifier pour le paramètre.

▼ Journalisation des transactions DHCP dans un fichier `syslog` indépendant

1. **Connectez-vous au serveur DHCP en tant que superutilisateur (ou équivalent).**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

   Il est possible qu'un rôle associé au profil de gestion DHCP ne soit pas suffisant pour réaliser cette tâche. Assurez-vous également qu'il donne à l'utilisateur le droit de modifier les fichiers `syslog`.

2. **Modifiez le fichier `/etc/syslog.conf` sur le système serveur afin d'ajouter une ligne sous le format suivant :**

   `local`*n*`.notice` *path-to-logfile*

   n représente le numéro de la fonction `syslog` que vous avez spécifié pour la journalisation des transactions, et *chemin-fichier-journal* le chemin d'accès complet au fichier dans lequel vous consignez les transactions.

   Voici, par exemple, la ligne que vous pourriez ajouter :

   ```
   local0.notice /var/log/dhcpsrvc
   ```

   Pour plus d'informations au sujet du fichier `syslog.conf`, reportez-vous à la page de manuel `syslog.conf(4)`.

Activation des mises à jour DNS dynamiques par un serveur DHCP

DNS offre des services nom-vers-adresse et adresse-vers-nom pour Internet. Dès qu'une correspondance DNS est établie, il est possible de se connecter à un système au moyen de son nom d'hôte ou de son adresse IP. Le système est joignable également hors de son domaine.

Le service DHCP peut exploiter le DNS de deux façons différentes :

- Le serveur DHCP peut rechercher le nom d'hôte mappé à une adresse IP que le serveur assigne au client. Le serveur renvoie ensuite le nom d'hôte du client ainsi que les autres données de configuration du client.
- S'il est configuré pour mettre à jour le DNS, le serveur DHCP peut essayer d'établir une correspondance DNS pour le compte d'un client. Le client a la possibilité de fournir son propre nom d'hôte lors d'une demande de service DHCP. S'il est configuré pour mettre à jour le DNS, le serveur DHCP essaie de mettre à jour le DNS en fonction du nom d'hôte suggéré par le client. Si l'opération réussit, le serveur DHCP renvoie au client le nom d'hôte demandé. Si l'opération échoue, le serveur DHCP renvoie au client un autre nom d'hôte.

Vous pouvez activer le service DHCP dans le but de mettre à jour le service DNS pour les clients DHCP qui fournissent leurs propres noms d'hôtes. Pour que la fonction de mise à jour du DNS soit opérationnelle, le serveur DNS, le serveur DHCP et le client DHCP doivent être configurés correctement. Le nom d'hôte demandé ne doit pas, en outre, être utilisé par un autre système du domaine.

La mise à jour du DNS par le serveur DHCP est possible si les conditions suivantes sont vérifiées :

- Le serveur DNS est conforme à la spécification RFC 2136.
- Le logiciel DNS est basé sur BIND v8.2.2, niveau de patch 5 ou ultérieur, que ce soit sur le système serveur DHCP ou le système serveur DNS.
- Le serveur DNS est configuré pour accepter les mises à jour DNS dynamiques provenant du serveur DHCP.
- Le serveur DHCP est configuré pour effectuer des mises à jour DNS dynamiques.
- La prise en charge DNS est configurée pour le réseau du client DHCP sur le serveur DHCP.
- Le client DHCP est configuré pour fournir un nom d'hôte demandé dans son message de requête DHCP.
- Le nom d'hôte demandé correspond à une adresse appartenant à DHCP. Le nom d'hôte ne doit pas nécessairement correspondre à une adresse.

▼ Activation de la mise à jour DNS dynamique pour les clients DHCP

Remarque – Rappelez-vous que les mises à jour DNS dynamiques présentent un *risque en matière de sécurité*.

Par défaut, le démon Solaris DNS Oracle Solaris (`in.named`) n'autorise pas les mises à jour dynamiques. Cette autorisation est accordée dans le fichier de configuration `named.conf` sur le système serveur DNS. Aucune autre protection n'est assurée. Avant de vous décider, évaluez les avantages que présente l'activation des mises à jour dynamiques pour les utilisateurs par rapport aux risques en matière de sécurité.

1. **Sur le serveur DNS, modifiez le fichier `/etc/named.conf` en tant que superutilisateur.**

2. **Recherchez la section `zone` correspondant au domaine approprié dans le fichier `named.conf`.**

3. **Ajoutez les adresses IP du serveur DHCP au mot-clé `allow-update`.**

   Si le mot-clé `allow-update` n'existe pas, insérez-le.

   Si le serveur DHCP réside, par exemple, aux adresses `10.0.0.1` et `10.0.0.2`, voici comment modifier le fichier `named.conf` de la zone `dhcp.domain.com` :

   ```
   zone "dhcp.domain.com" in {
                type master;
                file "db.dhcp";
                allow-update { 10.0.0.1; 10.0.0.2; };
   };

   zone "10.IN-ADDR.ARPA" in {
                type master;
                file "db.10";
                allow-update { 10.0.0.1; 10.0.0.2; };
   };
   ```

   Il est indispensable d'activer le mot-clé `allow-update` pour les deux zones afin d'autoriser le serveur DHCP à actualiser à la fois les enregistrements A et PTR sur le serveur DNS.

4. **Sur le serveur DHCP, lancez le gestionnaire DHCP.**

   ```
   # /usr/sadm/admin/bin/dhcpmgr &
   ```

   Pour plus d'informations à ce sujet, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

5. **Choisissez Modify dans le menu Service.**

   La boîte de dialogue de modification des options de service s'affiche.

6. **Sélectionnez l'option Update DNS Host Information Upon Client Request.**

7 **Indiquez le délai d'attente maximum d'une réponse du serveur DNS (en secondes), puis cliquez sur OK.**

La valeur par défaut proposée (15 secondes) est suffisante, en principe. N'hésitez pas à augmenter cette valeur si vous constatez que le délai d'attente est souvent dépassé.

8 **Cliquez sur l'onglet Macros et assurez-vous que le domaine DNS indiqué est celui qui convient.**

L'option `DNSdmain` doit être transmise avec le nom de domaine correct à tout client escomptant une prise en charge de la mise à jour DNS dynamique. Par défaut, `DNSdmain` est défini dans le cadre de la macro serveur, laquelle fait office de macro de configuration liée à chaque adresse IP.

9 **Configurez le client DHCP pour spécifier son nom d'hôte lors d'une demande de service DHCP.**

S'il s'agit d'un client DHCP , reportez-vous à la section "Activation d'un client DHCPv4 pour qu'il demande un nom d'hôte spécifique" à la page 449. Si votre client n'est pas un client DHCP, consultez la documentation propre à votre client pour savoir comment spécifier un nom d'hôte.

Enregistrement des noms d'hôtes clients

Si vous laissez au serveur DHCP le soin de générer des noms d'hôtes pour les adresses IP que vous intégrez au service DHCP, le serveur DHCP peut enregistrer ces noms d'hôtes dans NIS+, `/etc/inet/hosts` ou dans les services de noms DNS. L'enregistrement des noms d'hôtes n'est pas possible dans NIS dans la mesure où le système NIS n'offre pas de protocole permettant aux programmes d'actualiser et propager les cartes NIS.

Remarque – Le serveur DHCP peut mettre à jour le service DNS en fonction des noms d'hôtes générés à condition d'exécuter le serveur DNS et le serveur DHCP sur le même système.

Si un client DHCP fournit son nom d'hôte et que le serveur DNS est configuré pour autoriser les mises à jour dynamiques à partir du serveur DHCP, le serveur DHCP peut actualiser le service DNS pour le compte du client. Il est possible d'effectuer des mises à jour dynamiques même lorsque les serveurs DNS et DHCP fonctionnent sur des systèmes différents. Pour plus d'informations sur l'activation de cette fonction, reportez-vous à la section "Activation des mises à jour DNS dynamiques par un serveur DHCP" à la page 365.

Le tableau suivant indique la façon dont les noms d'hôtes clients sont enregistrés pour les systèmes clients DHCP en fonction des différents services de noms.

TABLEAU 15–2 Enregistrement des noms d'hôtes clients dans les services de noms

	Initiateur de l'enregistrement du nom d'hôte	
Service de noms	**Nom d'hôte généré par DHCP**	**Nom d'hôte fourni par le client DHCP**
NIS	Administrateur NIS	Administrateur NIS

TABLEAU 15–2 Enregistrement des noms d'hôtes clients dans les services de noms *(Suite)*

	Initiateur de l'enregistrement du nom d'hôte	
Service de noms	**Nom d'hôte généré par DHCP**	**Nom d'hôte fourni par le client DHCP**
NIS+	Outils DHCP	Outils DHCP
`/etc/hosts`	Outils DHCP	Outils DHCP
DNS	Outils DHCP, si le serveur DNS fonctionne sur le même système que le serveur DHCP Administrateur DNS, si le serveur DNS fonctionne sur un système différent	Serveur DHCP, en cas de configuration pour des mises à jour DNS dynamiques Administrateur DNS, si le serveur DHCP n'est pas configuré pour des mises à jour DNS dynamiques

Les clients DHCP peuvent demander des noms d'hôtes particuliers dans des requêtes DHCP s'ils sont configurés à cet effet, comme cela est indiqué dans la section "Activation d'un client DHCPv4 pour qu'il demande un nom d'hôte spécifique" à la page 449. Consultez la documentation du fournisseur des autres clients DHCP pour vérifier si la fonctionnalité est prise en charge.

Personnalisation des options de performance pour le serveur DHCP

Vous pouvez changer les options ayant un impact sur les performances du serveur DHCP. Ces options sont décrites dans le tableau suivant.

TABLEAU 15–3 Options affectant les performances du serveur DHCP

Option du serveur	Description	Mot-clé
Nombre maximum de sauts de l'agent de relais BOOTP	Si une requête transite par plus d'un nombre donné d'agents de relais BOOTP, elle est abandonnée. Par défaut, le nombre maximum de sauts (pour des agents de relais) est fixé à quatre. Ce nombre est apparemment suffisant pour la majorité des réseaux. Un réseau peut éventuellement nécessiter plus de quatre sauts si les requêtes DHCP transitent par plusieurs agents de relais BOOTP avant d'atteindre un serveur DHCP.	`RELAY_HOPS=`*entier*
Détection d'adresses en double	Par défaut, le serveur envoie une adresse IP sous forme de test ping avant d'offrir l'adresse à un client. S'il ne reçoit aucune réponse en retour, cela prouve que l'adresse n'est pas déjà utilisée. Vous pouvez désactiver cette fonction pour réduire la durée accordée au serveur pour effectuer une offre. Cela présente le risque, cependant, de créer des adresses IP en double.	`ICMP_VERIFY=TRUE/FALSE`

TABLEAU 15–3 Options affectant les performances du serveur DHCP *(Suite)*

Option du serveur	Description	Mot-clé
Rechargement automatique de `dhcptab` aux intervalles spécifiés	Le serveur peut être configuré dans le but de lire automatiquement le contenu de la table `dhcptab` à l'intervalle indiqué (en minutes). Si vos données de configuration du réseau ne sont pas souvent modifiées et que vous ne disposez pas de plusieurs serveurs DHCP, il est inutile de recharger automatiquement la table `dhcptab`. Il faut savoir, en outre, que le gestionnaire DHCP permet de demander au serveur de recharger la table `dhcptab` chaque fois que vous changez les données.	`RESCAN_INTERVAL=`*min*
Mise en cache des offres d'adresses IP pour les intervalles spécifiés	Lorsqu'un serveur propose une adresse IP à un client, l'offre est placée dans un cache pendant un certain temps. Tant que l'offre est maintenue dans le cache, l'adresse ne peut pas être proposée à un autre client. Il est possible de changer la durée (en secondes) de mise en cache de l'offre. La valeur par défaut est de 10 secondes. Sur des réseaux peu rapides, il peut être nécessaire d'augmenter cette valeur.	`OFFER_CACHE_TIMEOUT=`*sec*

Les procédures suivantes décrivent comment modifier ces options.

▼ Personnalisation des options de performance DHCP (gestionnaire DHCP)

1. **Choisissez Modify dans le menu Service du gestionnaire DHCP.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Changez les options qui vous intéressent.**

   Reportez-vous au Tableau 15–3 pour plus d'informations sur ces options.

3. **Choisissez ensuite Restart Server.**

4. **Cliquez sur OK.**

▼ Personnalisation des options de performance DHCP (ligne de commande)

Si vous procédez comme indiqué ci-après, les options que vous modifiez ne seront prises en compte qu'après avoir redémarré le serveur DHCP.

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Changez une ou plusieurs des options de performance :**

   `# /usr/sbin/dhcpconfig -P` *keyword=value,keyword=value...*

   mot-clé=valeur peut correspondre à l'un des mots-clés suivants :

`RELAY_HOPS=`*entier*	Indique le nombre maximum de sauts de l'agent de relais autorisés avant que le démon abandonne le datagramme DHCP ou BOOTP.
`ICMP_VERIFY=TRUE/FALSE`	Active ou désactive la détection automatique d'adresses IP en double. Il est déconseillé de donner la valeur `FALSE` à ce paramètre.
`RESCAN_INTERVAL=`*minutes*	Spécifie l'intervalle en minutes au bout duquel le serveur DHCP programme la relecture automatique des informations de la table `dhcptab`.
`OFFER_CACHE_TIMEOUT=`*secondes*	Fixe la durée de mise en cache (en secondes), par le serveur DHCP, des offres d'adresses IP transmises aux clients DHCP de détection. Elle équivaut à 10 secondes par défaut.

Exemple 15–1 Définition des options de performance DHCP

L'exemple suivant illustre comment spécifier l'ensemble des options de commande.

```
# dhcpconfig -P RELAY_HOPS=2,ICMP_VERIFY=TRUE,\
RESCAN_INTERVAL=30,OFFER_CACHE_TIMEOUT=20
```

Ajout, modification et suppression de réseaux DHCP (liste des tâches)

Lorsque vous configurez un serveur DHCP, vous devez également configurer au moins un réseau afin d'utiliser le service DHCP. Vous avez la possibilité, à tout moment, d'ajouter d'autres réseaux.

Le tableau suivant décrit la liste des tâches supplémentaires que vous pouvez effectuer lorsque vous utilisez des réseaux DHCP après leur configuration initiale. Cette liste des tâches propose les liens aux procédures correspondantes.

Tâche	Description	Voir
Activation ou désactivation du service DHCP sur des interfaces réseau du serveur.	Le comportement par défaut consiste à contrôler les requêtes DHCP pour l'ensemble des interfaces réseau. Pour éviter de prendre en compte toutes les interfaces, il suffit de retirer une interface de la liste des interfaces contrôlées.	"Spécification des interfaces réseau à placer sous le contrôle de DHCP (gestionnaire DHCP)" à la page 373
Ajout d'un nouveau réseau au service DHCP.	Place un réseau sous le contrôle DHCP, en vue de gérer des adresses IP sur le réseau.	"Ajout d'un réseau DHCP (gestionnaire DHCP)" à la page 376 "Ajout d'un réseau DHCP (`dhcpconfig`)" à la page 377
Changement des paramètres d'un réseau géré par DHCP.	Modifie les informations transmises aux clients d'un réseau donné.	"Modification de la configuration d'un réseau DHCP (gestionnaire DHCP)" à la page 378 "Modification de la configuration d'un réseau DHCP(`dhtadm`)" à la page 379
Exclusion d'un réseau du service DHCP.	Supprime un réseau de façon à ce que les adresses IP sur le réseau ne soient plus gérées par DHCP.	"Suppression d'un réseau DHCP (gestionnaire DHCP)" à la page 380 "Suppression d'un réseau DHCP (`pntadm`)" à la page 381

Spécification des interfaces réseau placées sous le contrôle DHCP

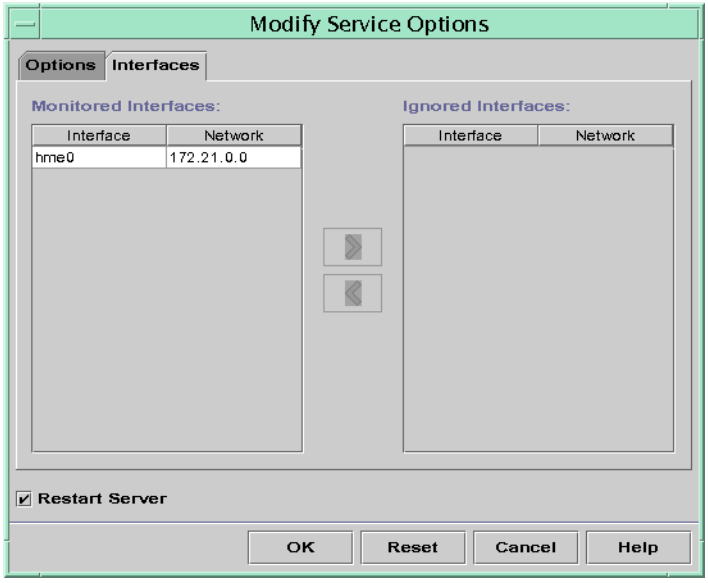
Par défaut, la commande `dhcpconfig` et l'assistant de configuration du gestionnaire DHCP se chargent tous les deux de configurer le serveur DHCP afin de contrôler l'ensemble des interfaces réseau du système serveur. Si vous ajoutez une nouvelle interface réseau au système serveur, le serveur DHCP contrôle automatiquement la nouvelle interface au démarrage du système. Vous pouvez ensuite placer d'autres réseaux sous le contrôle DHCP via l'interface réseau.

Il est possible également de désigner les interfaces réseau à contrôler et celles qu'il convient d'ignorer. Si vous ne souhaitez pas offrir un service DHCP sur un réseau donné, il faut éviter de prendre en compte l'interface correspondante.

Si vous choisissez d'ignorer une interface quelconque, puis installez une nouvelle interface, le serveur DHCP ignorera la nouvelle interface. Vous êtes tenu d'ajouter la nouvelle interface à la liste des interfaces contrôlées sur le serveur. Vous pouvez désigner les interfaces à l'aide du gestionnaire DHCP ou de l'utilitaire `dhcpconfig`.

Cette section décrit comment procéder pour spécifier les interfaces réseau que DHCP doit contrôler ou ignorer. La procédure mettant en jeu le gestionnaire DHCP nécessite l'ouverture de l'onglet Interfaces dans la boîte de dialogue de modification des options de service du gestionnaire DHCP, illustrée à la figure suivante.

FIGURE 15–4 Onglet Interfaces de la boîte de dialogue de modification des options de service dans le gestionnaire DHCP



▼ Spécification des interfaces réseau à placer sous le contrôle de DHCP (gestionnaire DHCP)

1. **Choisissez Modify dans le menu Service du gestionnaire DHCP.**

   La boîte de dialogue de modification des options de service s'affiche.

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Cliquez sur l'onglet Interfaces.**

3. **Sélectionnez l'interface réseau qui convient.**

4 **Cliquez sur les boutons fléchés pour insérer l'interface dans la liste appropriée.**

Ainsi, pour ignorer une interface, il suffit de sélectionner l'interface en question dans la liste Monitored Interfaces, puis de cliquer sur le bouton fléché droit. L'interface apparaît alors dans la liste Ignored Interfaces.

5 **Choisissez Restart Server et cliquez sur OK.**

Les modifications apportées ont un effet permanent.

▼ Spécification des interfaces réseau à placer sous le contrôle de DHCP (`dhcpconfig`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Entrez la commande suivante sur le système serveur DHCP :**

```
# /usr/sbin/dhcpconfig -P INTERFACES=int,int,...
```

int, int,... représente la liste des interfaces à contrôler. N'oubliez pas de séparer les noms des interfaces par des virgules.

Voici, par exemple, la commande qu'il convient d'entrer pour gérer uniquement `ge0` et `ge1` :

```
#/usr/sbin/dhcpconfig -P INTERFACES=ge0,ge1
```

Les interfaces à ignorer ne doivent pas figurer sur la ligne de commande `dhcpconfig`.

Les changements effectués à l'aide de cette commande ont un effet permanent.

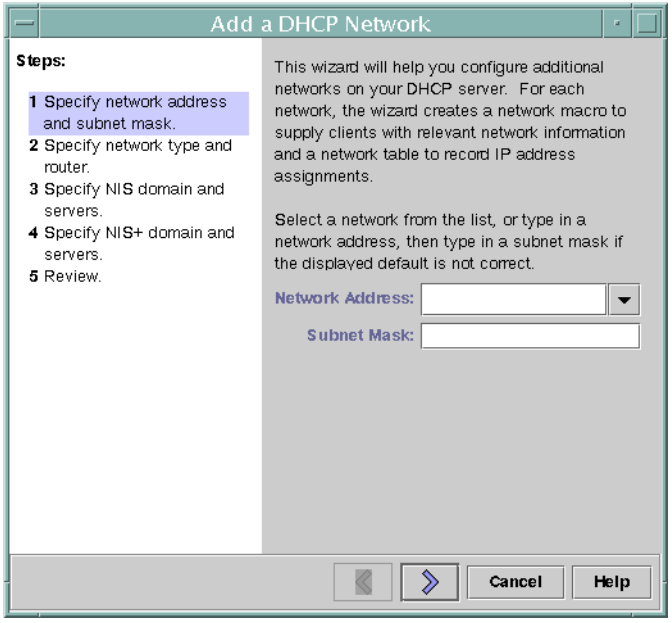
Ajout de réseaux DHCP

Lorsque vous configurez le serveur à l'aide du gestionnaire DHCP, vous définissez en même temps les paramètres de configuration du premier réseau. Le premier réseau correspond généralement au réseau local sur l'interface principale du système serveur. Si vous avez l'intention de configurer des réseaux supplémentaires, faites appel à l'assistant de configuration du réseau DHCP dans le gestionnaire DHCP.

Si vous vous servez de la commande `dhcpconfig -D` pour configurer le serveur, vous devez configurer séparément tous les réseaux censés utiliser le service DHCP. Pour plus d'informations, reportez-vous à la section "Ajout d'un réseau DHCP (`dhcpconfig`)" à la page 377.

La figure suivante représente la boîte de dialogue initiale de l'assistant de configuration du réseau DHCP dans le gestionnaire DHCP.

FIGURE 15–5 Assistant de configuration de réseau du gestionnaire DHCP



Lorsque vous configurez un nouveau réseau, le gestionnaire DHCP crée les composants suivants :

- Une table de réseau dans le magasin de données. Le nouveau réseau est répertorié dans la liste des réseaux à l'intérieur de l'onglet Addresses dans le gestionnaire DHCP.
- Une macro de réseau contenant les informations nécessaires aux clients résidant sur ce réseau. Le nom de la macro de réseau correspond à l'adresse IP du réseau. La macro de réseau est ajoutée à la table `dhcptab` dans le magasin de données.

▼ Ajout d'un réseau DHCP (gestionnaire DHCP)

1 **Dans le gestionnaire DHCP, cliquez sur l'onglet Addresses.**

La liste contient l'ensemble des réseaux déjà configurés pour le service DHCP.

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2 **Choisissez Network Wizard dans le menu Edit.**

3 **Sélectionnez les options qui vous intéressent ou entrez les informations demandées. En fonction des décisions prises lors de la phase de planification, déterminez les informations à spécifier.**

La phase de planification est décrite à la section "Planification de la configuration DHCP de vos réseaux distants" à la page 335.

En cas de difficulté, n'hésitez pas à cliquer sur le bouton d'aide dans la fenêtre de l'assistant. Votre navigateur Web vous donne diverses informations au sujet de l'assistant de configuration du réseau DHCP.

4 **Cliquez sur Finish pour achever la configuration du réseau après avoir spécifié les informations requises.**

L'assistant de configuration du réseau génère une table de réseau vide, présentée dans le volet gauche de la fenêtre.

Il crée également une macro de réseau dont le nom correspond à l'adresse IP du réseau.

5 **(Facultatif) Cliquez sur l'onglet Macros et sélectionnez la macro de réseau pour examiner son contenu.**

Vous pouvez confirmer que les informations indiquées dans l'assistant ont été insérées sous forme de valeurs d'options dans la macro de réseau.

Voir aussi Pour gérer les adresses IP du réseau sous DHCP, n'oubliez pas de les définir. Pour plus d'informations, reportez-vous à la section "Ajout d'adresses IP au service DHCP" à la page 389.

Si vous omettez de compléter la table de réseau, le serveur DHCP a toujours la possibilité de fournir des données de configuration aux clients. Pour plus d'informations, reportez-vous à la section "Configuration des clients DHCP pour qu'ils reçoivent uniquement des informations (liste des tâches)" à la page 424.

▼ Ajout d'un réseau DHCP (`dhcpconfig`)

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Entrez la commande suivante sur le système serveur DHCP :**

   ```
   # /usr/sbin/dhcpconfig -N network-address
   ```

   adresse-réseau représente l'adresse IP du réseau que vous souhaitez ajouter au service DHCP. Pour connaître les sous-options utilisables avec l'option `-N`, reportez-vous à la page de manuel `dhcpconfig`(1M).

   Si vous n'utilisez pas de sous-options, `dhcpconfig` utilise les fichiers du réseau pour obtenir des informations au sujet du réseau.

Voir aussi Pour gérer les adresses IP du réseau sous DHCP, n'oubliez pas de les définir. Pour plus d'informations, reportez-vous à la section "Ajout d'adresses IP au service DHCP" à la page 389.

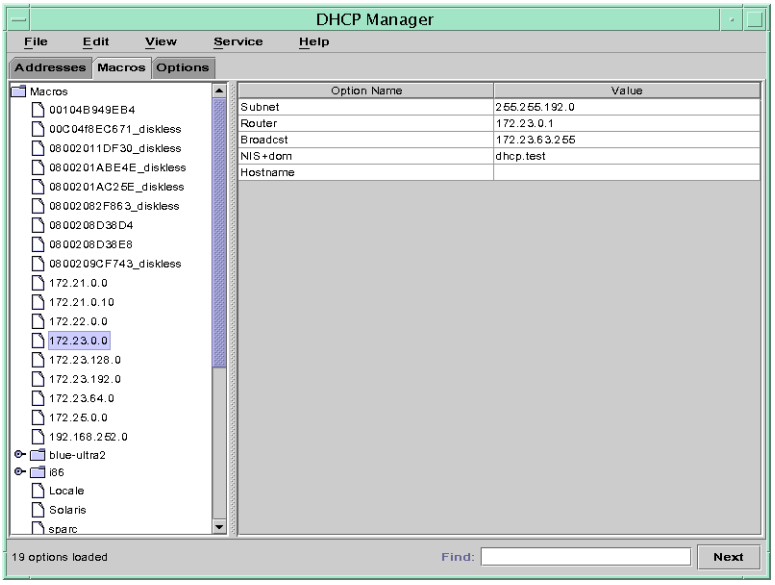
Si vous omettez de compléter la table de réseau, le serveur DHCP a toujours la possibilité de fournir des données de configuration aux clients. Pour plus d'informations, reportez-vous à la section "Configuration des clients DHCP pour qu'ils reçoivent uniquement des informations (liste des tâches)" à la page 424.

Modification des configurations de réseau DHCP

Après avoir ajouté un réseau au service DHCP, vous avez la possibilité de modifier les données de configuration d'origine. Ces données sont stockées dans la macro de réseau utilisée pour transmettre les informations aux clients sur le réseau. Vous devez modifier la macro de réseau pour changer la configuration du réseau.

La figure suivante illustre l'onglet Macros du gestionnaire DHCP.

FIGURE 15–6 Onglet Macros dans le gestionnaire DHCP



▼ Modification de la configuration d'un réseau DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Macros.**

   Toutes les macros définies pour ce serveur DHCP sont répertoriées dans le volet de gauche.

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez la macro de réseau dont le nom correspond à la configuration que vous modifiez.**

   Le nom de la macro de réseau est l'adresse IP du réseau.

3. **Choisissez Properties dans le menu Edit.**

   La boîte de dialogue des propriétés de la macro présente une table des options figurant dans la macro.

4. **Sélectionnez l'option que vous souhaitez modifier.**

   Le nom de l'option et sa valeur sont affichés dans des zones de texte dans la partie supérieure de la boîte de dialogue.

5 **(Facultatif) Changez le nom de l'option ou cliquez sur le bouton Select pour afficher une liste des noms d'options.**

La boîte de dialogue de sélection des options contient une liste de toutes les options standard DHCP, avec une brève description pour chacune d'entre elles.

6 **(Facultatif) Sélectionnez un nom d'option dans la boîte de dialogue, puis cliquez sur OK.**

Le nouveau nom de l'option est visible dans le champ Option Name.

7 **Donnez une nouvelle valeur à l'option, puis cliquez sur Modify.**

8 **(Facultatif) Vous pouvez également ajouter des options à la macro de réseau en cliquant sur Select dans la boîte de dialogue.**

Pour obtenir des informations générales sur la modification des macros, reportez-vous à la section "Modification des macros DHCP" à la page 404.

9 **Sélectionnez l'option Notify DHCP Server of Change, puis cliquez sur OK.**

Cette option demande au serveur DHCP de relire le contenu de la table `dhcptab` et d'appliquer immédiatement la modification dès que vous cliquez sur OK.

▼ Modification de la configuration d'un réseau DHCP(`dhtadm`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Repérez la macro où figurent des informations sur tous les clients du réseau.**

Le nom de la macro de réseau correspond à l'adresse IP du réseau.

Si vous ignorez le nom de cette macro, il suffit d'afficher la table `dhcptab` afin de répertorier toutes les macros à l'aide de la commande `dhtadm -P`.

3 **Entrez une commande sous le format suivant pour changer la valeur de l'option à modifier :**

```
# dhtadm -M -m macro-name -e 'symbol=value' -g
```

Pour plus d'informations au sujet des options de ligne de commande `dhtadm`, reportez-vous à la page de manuel `dhtadm(1M)`.

Exemple 15–2 Modification d'une macro DHCP à l'aide de la commande `dhtadm`

Pour remplacer, par exemple, la durée du bail de la macro `10.25.62.0` par 57600 secondes et le domaine NIS par `sem.example.com`, voici les commandes qu'il convient d'entrer :

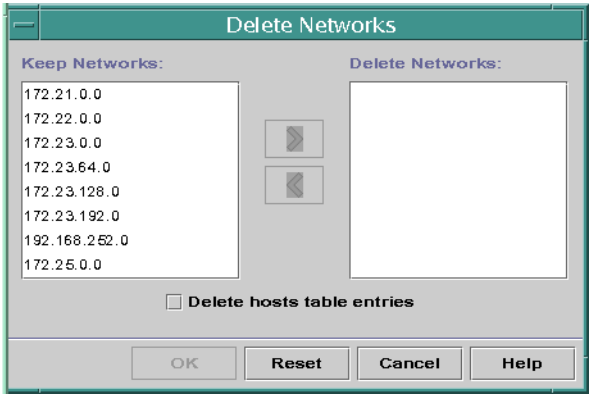
```
# dhtadm -M -m 10.25.62.0 -e 'LeaseTim=57600' -g

# dhtadm -M -m 10.25.62.0 -e 'NISdmain=sem.example.com' -g
```

L'option `-g` oblige le démon DHCP à relire la table `dhcptab` et à appliquer les modifications.

Suppression de réseaux DHCP

Le gestionnaire DHCP permet de supprimer plusieurs réseaux à la fois. Vous avez la possibilité d'effacer automatiquement les entrées de la table d'hôtes associées aux adresses IP gérées par DHCP sur ces réseaux. La figure suivante représente la boîte de dialogue de suppression des réseaux du gestionnaire DHCP.

FIGURE 15–7 Boîte de dialogue de suppression des réseaux du gestionnaire DHCP



La commande `pntadm` vous demande d'effacer chaque entrée d'adresse IP du réseau avant de supprimer ce réseau. Vous ne pouvez supprimer qu'un réseau à la fois.

▼ Suppression d'un réseau DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Addresses.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section “Démarrage et arrêt du gestionnaire DHCP” à la page 354.

2. **Choisissez Delete Networks dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue de suppression des réseaux.

3. **Dans la liste Keep Networks, sélectionnez les réseaux que vous avez l'intention de supprimer.**

   Maintenez la touche Contrôle enfoncée pendant que vous cliquez sur les réseaux en question. Pour sélectionner une série de réseaux, maintenez la touche Majuscule enfoncée pendant que vous cliquez.

4. **Cliquez sur le bouton contenant une flèche vers la droite pour transférer les réseaux sélectionnés dans la liste Delete Networks.**

5. **Si vous souhaitez effacer les entrées de la table d'hôtes pour les adresses DHCP de ce réseau, cochez la case Delete Host Table Entries.**

   Le fait d'effacer les entrées de la table des hôtes ne supprime pas les enregistrements d'hôtes au niveau du serveur DNS pour ces adresses. Les entrées sont retirées uniquement du service de noms local.

6. **Cliquez sur OK.**

▼ Suppression d'un réseau DHCP (`pntadm`)

Cette procédure a pour effet d'effacer les adresses IP du réseau dans la table de réseau DHCP avant de supprimer le réseau. La suppression des adresses permet de s'assurer que les noms d'hôtes sont retirés du fichier `hosts` ou de la base de données.

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Entrez une commande sous ce format pour retirer une adresse IP et son nom d'hôte du service de noms :**

   ```
   # pntadm -D -y IP-address
   ```

   Pour supprimer, par exemple, l'adresse IP `10.25.52.1`, voici la commande qu'il convient d'entrer :

   ```
   # pntadm -D -y 10.25.52.1
   ```

   L'option `-y` indique qu'il faut supprimer le nom d'hôte.

3 **Réexécutez la commande `pntadm -D -y` pour chaque adresse que compte le réseau.**

Il peut être intéressant de créer un script afin d'exécuter la commande `pntadm` lorsque vous supprimez de nombreuses adresses.

4 **Une fois toutes les adresses effacées, entrez la commande suivante pour retirer le réseau du service DHCP.**

```
# pntadm -R network-IP-address
```

Pour supprimer, par exemple, le réseau `10.25.52.0`, voici la commande qu'il convient d'entrer :

```
# pntadm -R 10.25.52.0
```

Pour plus d'informations au sujet de l'utilitaire `pntadm`, reportez-vous à la page de manuel `pntadm(1M)`.

Prise en charge des clients BOOTP via le service DHCP (liste des tâches)

Pour prendre en charge les clients BOOTP sur votre serveur DHCP, vous devez configurer celui-ci pour qu'il soit compatible BOOTP. Pour désigner les clients BOOTP qui seront capables d'utiliser votre serveur DHCP, vous pouvez enregistrer les clients BOOTP dans la table de réseau du serveur DHCP. Il est possible également de réserver certaines adresses IP en vue de les allouer automatiquement aux clients BOOTP.

Remarque – Les adresses BOOTP sont assignées de façon permanente, que vous choisissiez ou non d'allouer explicitement un bail permanent à l'adresse.

Le tableau suivant décrit la liste des tâches que vous pouvez être amené à effectuer pour prendre en charge les clients BOOTP. Cette liste des tâches propose les liens aux procédures correspondantes.

Tâche	Description	Voir
Configuration de la prise en charge automatique BOOTP.	Fournit des adresses IP à un client BOOTP quelconque sur un réseau géré par DHCP ou sur un réseau relié à un réseau DHCP par un agent de relais. Vous devez réserver un pool d'adresses à l'usage exclusif des clients BOOTP. Cela est d'autant plus utile si le serveur doit gérer un grand nombre de clients BOOTP.	"Configuration de la prise en charge d'un client BOOTP (gestionnaire DHCP)" à la page 383

Tâche	Description	Voir
Configuration de la prise en charge manuelle BOOTP.	Fournit des adresses IP uniquement aux clients BOOTP enregistrés de façon manuelle auprès du service DHCP. Dans cette optique, vous êtes tenu de lier un ID de client à une adresse IP dédiée aux clients BOOTP. Vous pouvez envisager cette solution pour un petit nombre de clients BOOTP ou lorsque vous souhaitez limiter les clients BOOTP susceptibles de faire appel au serveur DHCP.	"Configuration de la prise en charge des clients BOOTP enregistrés (gestionnaire DHCP)" à la page 384

▼ Configuration de la prise en charge d'un client BOOTP (gestionnaire DHCP)

1. **Choisissez Modify dans le menu Service du gestionnaire DHCP.**

   La boîte de dialogue de modification des options de service s'affiche.

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez l'option Automatic dans la section BOOTP Compatibility de la boîte de dialogue.**

3. **Choisissez Restart Server et cliquez sur OK.**

4. **Cliquez sur l'onglet Addresses.**

5. **Sélectionnez les adresses que vous souhaitez réserver aux clients BOOTP.**

   Pour sélectionner une plage d'adresses, cliquez sur la première adresse, maintenez la touche Majuscule enfoncée, puis cliquez sur la dernière adresse. Pour sélectionner des adresses non contiguës, cliquez sur les adresses de votre choix en maintenant la touche Contrôle enfoncée.

6. **Choisissez Properties dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue de modification de plusieurs adresses.

7. **Dans la section BOOTP, sélectionnez l'option Assign All Addresses Only to BOOTP Clients.**

   Choisissez Keep Current Settings pour toutes les autres options, de façon à préserver les paramètres actuels.

8. **Cliquez sur OK.**

   N'importe quel client BOOTP peut désormais obtenir une adresse à partir de ce serveur DHCP.

▼ Configuration de la prise en charge des clients BOOTP enregistrés (gestionnaire DHCP)

1. **Choisissez Modify dans le menu Service du gestionnaire DHCP.**

   La boîte de dialogue de modification des options de service s'affiche.

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez l'option Manual dans la section BOOTP Compatibility de la boîte de dialogue.**

3. **Choisissez Restart Server et cliquez sur OK.**

4. **Cliquez sur l'onglet Addresses.**

5. **Sélectionnez l'adresse que vous souhaitez allouer à un client BOOTP en particulier.**

6. **Choisissez Properties dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue des propriétés des adresses.

7. **Cliquez sur l'onglet Lease dans la boîte de dialogue des propriétés des adresses.**

8. **Entrez l'identificateur du client dans le champ Client ID.**

   Dans le cas d'un client BOOTP Oracle Solaris sur un réseau Ethernet, l'ID client correspond à une chaîne de caractères dérivée de l'adresse Ethernet hexadécimale du client. L'ID client contient un préfixe qui indique le type ARP (Address Resolution Protocol) pour Ethernet (01). Un client BOOTP possédant l'adresse Ethernet `8:0:20:94:12:1e` utiliserait, par exemple, l'ID de client `0108002094121E` .

   Astuce – En tant que superutilisateur d'un système client Oracle Solaris, entrez la commande suivante pour obtenir l'adresse Ethernet de l'interface :

   ```
   # ifconfig -a
   ```

   ---

9. **Sélectionnez l'option Reserved pour réserver l'adresse IP à ce client.**

10. **Sélectionnez l'option Assign Only to BOOTP Clients et cliquez sur OK.**

    Dans l'onglet Addresses, BOOTP s'affiche dans le champ Status et l'ID client que vous avez spécifié figure dans le champ Client ID.

Traitement des adresses IP dans le service DHCP (liste des tâches)

Vous pouvez faire appel au gestionnaire DHCP ou utiliser la commande `pntadm` pour ajouter des adresses IP, modifier leurs propriétés et supprimer des adresses du service DHCP. Avant de commencer à travailler avec des adresses IP, il est conseillé de se reporter au Tableau 15–4 pour se familiariser avec les propriétés des adresses IP. Ce tableau contient des informations destinées tout particulièrement aux utilisateurs du gestionnaire DHCP et de la commande `pntadm`.

Remarque – Le Tableau 15–4 contient plusieurs exemples illustrant l'utilisation de `pntadm` pour définir les propriétés des adresses IP pendant l'ajout ou la modification d'adresses IP. Pour plus d'informations au sujet de la commande `pntadm`, reportez-vous à la page de manuel `pntadm(1M)`.

La liste suivante présente les tâches qu'il convient de réaliser pour ajouter, modifier ou supprimer des adresses IP. Cette liste des tâches propose également les liens aux procédures correspondantes.

Tâche	Description	Voir
Ajout d'une ou plusieurs adresses IP au service DHCP.	Ajoute des adresses IP sur des réseaux déjà gérés par le service DHCP grâce au gestionnaire DHCP.	"Ajout d'une adresse IP unique (gestionnaire DHCP)" à la page 391 "Duplication d'une adresse IP existante (gestionnaire DHCP)" à la page 391 "Ajout de plusieurs adresses IP (gestionnaire DHCP)" à la page 392 "Ajout d'adresses IP (`pntadm`)" à la page 392
Modification des propriétés d'une adresse IP.	Modifie toute propriété d'adresse IP décrite dans le Tableau 15–4.	"Modification des propriétés des adresses IP (gestionnaire DHCP)" à la page 394 "Modification des propriétés des adresses IP (`pntadm`)" à la page 395

Tâche	Description	Voir
Suppression des adresses IP du service DHCP.	Empêche DHCP d'utiliser les adresses IP indiquées.	"Marquage des adresses IP comme inutilisables (gestionnaire DHCP)" à la page 396 "Marquage des adresses IP comme inutilisables (`pntadm`)" à la page 397 "Suppression des adresses IP du service DHCP (gestionnaire DHCP)" à la page 398 "Suppression des adresses IP du service DHCP (`pntadm`)" à la page 398
Affectation d'une adresse IP fixe à un client DHCP.	Configure un client de façon à ce qu'il reçoive la même adresse IP chaque fois que le client demande sa configuration.	"Affectation d'une adresse IP fixe à un client DHCP (gestionnaire DHCP)" à la page 400 "Affectation d'une adresse IP fixe à un client DHCP (`pntadm`)" à la page 401

Le tableau suivant présente et décrit les propriétés des adresses IP.

TABLEAU 15–4 Propriétés des adresses IP

Propriétés	Description	Mode de spécification dans la commande `pntadm`
Adresse réseau	Adresse du réseau contenant l'adresse IP avec laquelle vous travaillez. L'adresse réseau figure dans la liste Networks de l'onglet Addresses dans le gestionnaire DHCP.	L'adresse réseau doit être le dernier argument sur la ligne de commande `pntadm` utilisée pour créer, modifier ou supprimer une adresse IP. Voici comment ajouter, par exemple, une adresse IP au réseau `10.21.0.0` : **`pntadm -A`** *options adresse-ip* **`10.21.0.0`**
Adresse IP	Adresse que vous avez décidé de créer, modifier ou supprimer. L'adresse IP figure dans la première colonne de l'onglet Addresses dans le gestionnaire DHCP.	L'adresse IP doit accompagner les options `-A`, `-M` et `-D` associées à la commande `pntadm`. Voici comment modifier, par exemple, l'adresse IP `10.21.5.12` : **`pntadm -M 10.21.5.12`** *options* **`10.21.0.0`**
Nom du client	Nom d'hôte mappé à l'adresse IP dans la table des hôtes. Ce nom peut être généré automatiquement par le gestionnaire DHCP lors de la création des adresses. Si vous créez une simple adresse, vous pouvez fournir le nom.	Spécifiez le nom du client à l'aide de l'option `-h`. Pour spécifier par exemple le nom de client `carotte12` pour `10.21.5.12`, entrez : **`pntadm -M 10.21.5.12 -h carotte12 10.21.0.0`**

TABLEAU 15–4 Propriétés des adresses IP *(Suite)*

Propriétés	Description	Mode de spécification dans la commande `pntadm`
Serveur propriétaire	Serveur DHCP chargé de gérer l'adresse IP et de répondre à la demande d'allocation d'adresse IP du client DHCP.	Spécifiez le nom du serveur propriétaire à l'aide de l'option `-s`. Pour rendre par exemple le serveur `bleu2` propriétaire de `10.21.5.12`, entrez : **`pntadm -M 10.21.5.12 -s bleu2 10.21.0.0`**
Macro de configuration	Macro utilisée par le serveur DHCP pour obtenir les options de configuration du réseau à partir de la table `dhcptab`. Plusieurs macros sont créées automatiquement lorsque vous configurez un serveur, puis ajoutez des réseaux. Pour plus d'informations au sujet des macros, reportez-vous à la section "À propos des macros DHCP" à la page 318 Une macro serveur, allouée en tant que macro de configuration pour chaque adresse, est également générée lors de la création des adresses.	Spécifiez le nom de la macro à l'aide de l'option `-m`. Pour assigner par exemple l'adresse `10.21.5.12` à la macro serveur `bleu2`, entrez : **`pntadm -M 10.21.5.12 -m bleu2 10.21.0.0`**
ID client	Chaîne de texte unique au sein du service DHCP. Si l'ID client correspond à 00, cela signifie que l'adresse n'est allouée à aucun client. Si vous spécifiez un ID client lors de la modification des propriétés d'une adresse IP, celle-ci est liée exclusivement à ce client. L'ID client est déterminé par le fournisseur du client DHCP. Si votre client n'est pas un client DHCP, reportez-vous à la documentation propre à votre client pour plus d'informations.	Spécifiez l'ID client à l'aide de l'option `-i`. Voici comment assigner, par exemple, l'ID client `08002094121E` à l'adresse `10.21.5.12` : **`pntadm -M 10.21.5.12 -i 0108002094121E 10.21.0.0`**

TABLEAU 15–4 Propriétés des adresses IP *(Suite)*

Propriétés	Description	Mode de spécification dans la commande `pntadm`
	En ce qui concerne les clients DHCP, l'ID client est dérivé de l'adresse matérielle hexadécimale du client. L'ID client inclut un préfixe qui représente le code ARP pour le type de réseau, comme par exemple 01 pour Ethernet. Les codes ARP sont attribués par un organisme vérifiant l'unicité des adresses réseau sur Internet (IANA, Internet Assigned Numbers Authority) dans la section des paramètres ARP de la norme des numéros assignés publiée sur `http://www.iana.com/numbers.html` Par exemple, un client Oracle Solaris dont l'adresse Ethernet hexadécimale est : `8:0:20:94:12:1e` utilise l'ID client `0108002094121E`. L'ID client est indiqué dans le gestionnaire DHCP et dans la commande `pntadm` lorsqu'un client est en train d'utiliser une adresse. **Conseil :** en tant que superutilisateur du système client Oracle Solaris, entrez la commande suivante pour obtenir l'adresse Ethernet de l'interface : `ifconfig -adladm show-phys -m`	
Réservée	Le paramètre qui définit l'adresse est réservé exclusivement au client identifié par l'ID de client. Le serveur DHCP n'est pas en mesure alors de récupérer l'adresse. Si vous sélectionnez cette option, vous attribuez manuellement l'adresse au client.	Choisissez de réserver l'adresse ou attribuez-la manuellement à l'aide de l'option `-f`. Voici comment réserver, par exemple, l'adresse IP `10.21.5.12` à un client : **`pntadm -M 10.21.5.12 -f MANUAL 10.21.0.0`**
Type ou stratégie de location	Paramètre qui détermine la façon dont DHCP gère l'utilisation des adresses IP par les clients. Vous avez le choix entre un bail dynamique ou permanent. Pour obtenir une explication complète, reportez-vous à la section "Choix entre un bail dynamique ou permanent" à la page 332.	Attribuez l'adresse de façon permanente à l'aide de l'option `-f`. Par défaut, les adresses sont louées de façon dynamique. Voici comment louer à titre permanent, par exemple, l'adresse IP `10.21.5.12` : **`pntadm -M 10.21.5.12 -f PERMANENT 10.21.0.0`**
Date d'expiration du bail	Date à laquelle le bail expire (applicable uniquement en cas de spécification d'un bail dynamique). Vous devez entrer la date au format *jj/mm/aaaa*.	Définissez la date d'expiration du bail à l'aide de l'option `-e`. Voici comment indiquer, par exemple, que le bail expire au 1er janvier 2006 : **`pntadm -M 10.21.5.12 -e 01/01/2006 10.21.0.0`**

TABLEAU 15–4 Propriétés des adresses IP *(Suite)*

Propriétés	Description	Mode de spécification dans la commande `pntadm`
Paramètre BOOTP	Paramètre indiquant que l'adresse est réservée pour des clients BOOTP. Pour plus d'informations au sujet de la prise en charge des clients BOOTP, reportez-vous à la section "Prise en charge des clients BOOTP via le service DHCP (liste des tâches)" à la page 382.	Réservez une adresse aux clients BOOTP à l'aide de l'option `-f`. Voici comment réserver, par exemple, l'adresse IP `10.21.5.12` aux clients BOOTP : **`pntadm -M 10.21.5.12 -f BOOTP 10.21.0.0`**
Paramètre inutilisable	Paramètre signifiant que l'adresse ne peut pas être allouée à un client.	Marquez l'adresse comme étant inutilisable à l'aide de l'option `-f`. Voici comment marquer, par exemple, l'adresse IP `10.21.5.12` comme inutilisable : **`pntadm -M 10.21.5.12 -f UNUSABLE 10.21.0.0`**

Ajout d'adresses IP au service DHCP

Avant d'ajouter des adresses IP, vous devez ajouter le réseau propriétaire des adresses au service DHCP. Pour plus d'informations au sujet de l'ajout de réseaux, reportez-vous à la section "Ajout de réseaux DHCP" à la page 374.

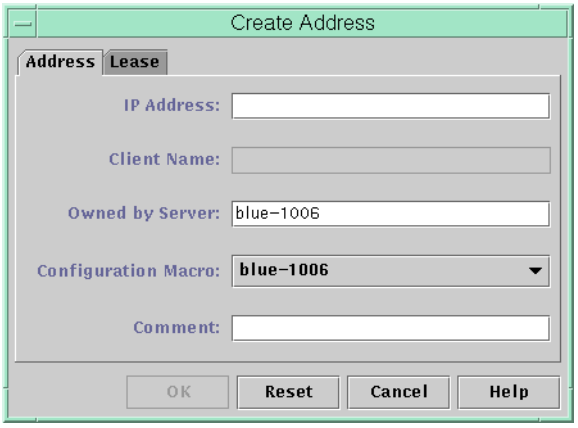
Vous pouvez ajouter des adresses avec le gestionnaire DHCP ou à l'aide de la commande `pntadm`.

Sur les réseaux déjà gérés par le service DHCP, il existe différentes façons d'ajouter des adresses avec le gestionnaire DHCP:

- **Ajout d'une seule adresse IP** – Placez une nouvelle adresse IP sous le contrôle de DHCP.
- **Duplication d'une adresse IP existante** – Copiez les propriétés d'une adresse IP gérée par DHCP et fournissez une nouvelle adresse IP et un nouveau nom de client..
- **Ajout d'une plage d'adresses IP** – Servez-vous de l'assistant d'ajout d'adresses pour placer une série d'adresses IP sous le contrôle de DHCP.

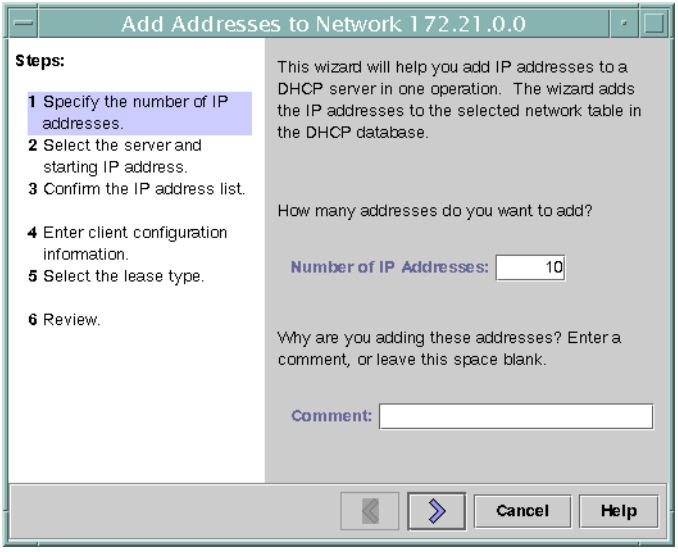
La figure suivante représente la boîte de dialogue de création d'adresse. À la différence de la boîte de dialogue de création d'adresse, dans la boîte de dialogue de duplication d'adresse, les zones de texte affichent les valeurs d'une adresse existante.

FIGURE 15–8 Boîte de dialogue de création d'adresse dans le gestionnaire DHCP



La figure suivante présente la première boîte de dialogue de l'assistant d'ajout d'adresses au réseau, dont vous avez besoin pour ajouter une série d'adresses IP.

FIGURE 15–9 Assistant d'ajout d'adresses au réseau dans le gestionnaire DHCP



▼ Ajout d'une adresse IP unique (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Addresses.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez le réseau auquel vous souhaitez ajouter la nouvelle adresse IP.**

3. **Choisissez Create dans le menu Edit.**

   Cela a pour effet d'afficher la boîte de dialogue de création d'adresse.

4. **Sélectionnez ou entrez les valeurs des paramètres d'adresse dans les onglets Addresse et Lease.**

   Cliquez sur le bouton d'aide pour afficher de l'aide dans un navigateur Web. Le Tableau 15–4 contient également des explications détaillées sur les différents paramètres.

5. **Cliquez sur OK.**

▼ Duplication d'une adresse IP existante (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Addresses.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez le réseau où figure la nouvelle adresse IP.**

3. **Sélectionnez l'adresse pour laquelle vous souhaitez dupliquer les propriétés.**

4. **Choisissez Duplicate dans le menu Edit.**

5. **Spécifiez la nouvelle adresse IP dans le champ correspondant.**

6. **(Facultatif) Indiquez un nouveau nom de client pour l'adresse.**

   Choisissez impérativement un nom différent de celui utilisé par l'adresse que vous dupliquez.

7. **(Facultatif) Modifiez d'autres valeurs d'option, si nécessaire.**

   La plupart des autres valeurs d'option doivent rester les mêmes.

8. **Cliquez sur OK.**

▼ Ajout de plusieurs adresses IP (gestionnaire DHCP)

1 **Dans le gestionnaire DHCP, cliquez sur l'onglet Addresses.**

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section “Démarrage et arrêt du gestionnaire DHCP” à la page 354.

2 **Sélectionnez le réseau auquel vous souhaitez ajouter les nouvelles adresses IP.**

3 **Choisissez Address Wizard dans le menu Edit.**

La boîte de dialogue d'ajout d'adresses au réseau vous invite à définir les valeurs des propriétés des adresses IP. Pour plus d'informations sur les propriétés, reportez-vous au Tableau 15–4 ou cliquez sur le bouton d'aide dans la boîte de dialogue. La section “Décisions relatives à la gestion des adresses IP (liste des tâches)” à la page 330 contient également des précisions utiles.

4 **Cliquez sur la flèche vers la droite pour faire défiler chaque écran, puis cliquez sur Finish au niveau du dernier écran.**

L'onglet Addresses est actualisé en fonction des nouvelles adresses.

▼ Ajout d'adresses IP (`pntadm`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section “Configuration de l'accès utilisateur aux commandes DHCP” à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuring RBAC (Task Map)” du *System Administration Guide: Security Services*.

2 **Ajoutez des adresses IP en entrant une commande sous le format suivant :**

```
# pntadm -A ip-address options network-address
```

Pour connaître les différentes options utilisables avec `pntadm -A`, reportez-vous à la page de manuel `pntadm`(1M). De plus, le Tableau 15–4 illustre des exemples de commandes `pntadm` permettant de spécifier des options.

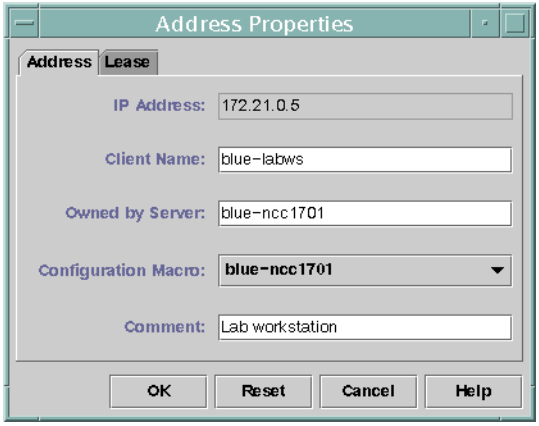
Remarque – Vous pouvez écrire un script afin d'ajouter plusieurs adresses à la fois avec `pntadm`. Voir l'Exemple 18–1.

Modification d'adresses IP dans le service DHCP

Vous pouvez modifier les propriétés d'adresse décrites dans le Tableau 15–4 à l'aide du gestionnaire DHCP ou de la commande `pntadm -M`. Pour plus d'informations au sujet de la commande `pntadm -M`, reportez-vous à la page de manuel `pntadm(1M)`.

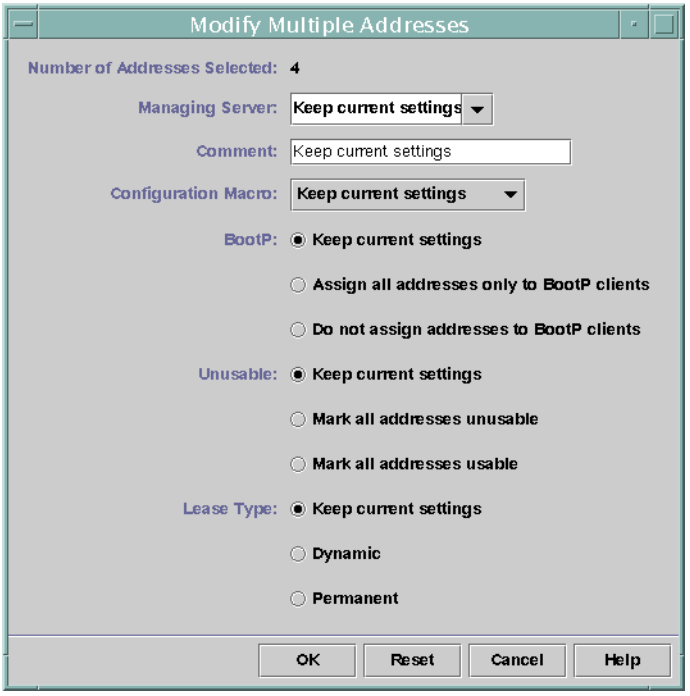
La figure suivante présente la boîte de dialogue des propriétés d'adresse utilisée pour changer les propriétés des adresses IP.

FIGURE 15–10 Boîte de dialogue des propriétés d'adresse dans le gestionnaire DHCP



La figure suivante présente la boîte de dialogue de modification des adresses prévue pour changer plusieurs adresses IP.

FIGURE 15–11 Boîte de dialogue de modification des adresses dans le gestionnaire DHCP



▼ Modification des propriétés des adresses IP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Addresses.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section “Démarrage et arrêt du gestionnaire DHCP” à la page 354.

2. **Sélectionnez le réseau de l'adresse IP.**

3. **Choisissez la ou les adresses IP que vous avez l'intention de modifier.**

   Pour changer plusieurs adresses à la fois, cliquez sur chacune d'elles tout en maintenant la touche Contrôle enfoncée. Pour sélectionner un bloc d'adresses, maintenez la touche Majuscule enfoncée pendant que vous cliquez.

4. **Choisissez Properties dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue des propriétés d'adresse ou de modification des adresses.

5 **Changez les propriétés qui conviennent.**

Cliquez sur le bouton d'aide ou reportez-vous au Tableau 15–4 pour plus d'informations sur les propriétés.

6 **Cliquez sur OK.**

▼ Modification des propriétés des adresses IP (`pntadm`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Redéfinissez les propriétés des adresses IP en entrant une commande sous le format suivant :**

```
# pntadm -M ip-address options network-address
```

De nombreuses options (documentées dans la page de manuel `pntadm`(1M)) sont utilisables avec la commande `pntadm`.

Le Tableau 15–4 contient des exemples de commande `pntadm` spécifiant des options.

Suppression d'adresses IP du service DHCP

Vous avez parfois intérêt à ce que le service DHCP cesse de gérer une adresse IP en particulier ou un groupe entier d'adresses. La méthode à suivre pour supprimer une adresse de DHCP varie selon que vous souhaitez appliquer le changement de façon temporaire ou permanente.

- Pour que les clients DHCP cessent temporairement d'exploiter les adresses, vous pouvez marquer les adresses en question comme inutilisables dans la boîte de dialogue des propriétés d'adresses, en procédant comme indiqué à la section "Marquage des adresses IP comme inutilisables par le service DHCP" à la page 396.
- Pour que les clients DHCP cessent définitivement d'exploiter les adresses, il convient de supprimer les adresses des tables de réseau DHCP, en procédant comme indiqué à la section "Suppression d'adresses IP du service DHCP" à la page 397.

Marquage des adresses IP comme inutilisables par le service DHCP

Vous pouvez vous servir de la commande `pntadm -M` avec l'option `-f UNUSABLE` pour désigner les adresses considérées comme inexploitables.

Dans le gestionnaire DHCP, pour marquer les adresses de façon individuelle, vous devez procéder à partir de la boîte de dialogue des propriétés d'adresses illustrée à la Figure 15–10. Pour marquer plusieurs adresses, utilisez la boîte de dialogue de modification des adresses illustrée à la Figure 15–11, comme dans la procédure suivante.

▼ Marquage des adresses IP comme inutilisables (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Addresses.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez le réseau de l'adresse IP.**

3. **Sélectionnez la ou les adresses IP que vous souhaitez signaler comme inutilisables.**

   Pour marquer plusieurs adresses comme inutilisables, cliquez sur chacune d'elles tout en maintenant la touche Contrôle enfoncée. Pour sélectionner un bloc d'adresses, maintenez la touche Majuscule enfoncée pendant que vous cliquez.

4. **Choisissez Properties dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue des propriétés d'adresse ou de modification des adresses.

5. **Si vous modifiez une seule adresse, cliquez sur l'onglet Lease.**

6. **Sélectionnez l'option Address is Unusable.**

   Si vous modifiez plusieurs adresses, sélectionnez l'option Mark All Addresses Unusable.

7. **Cliquez sur OK.**

▼ Marquage des adresses IP comme inutilisables (`pntadm`)

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Marquez des adresses IP comme inutilisables en entrant une commande sous le format suivant :**

   `# pntadm -M` *ip-address* `-f UNUSABLE` *network-address*

   Voici comment indiquer que l'adresse `10.64.3.3` est inutilisable :

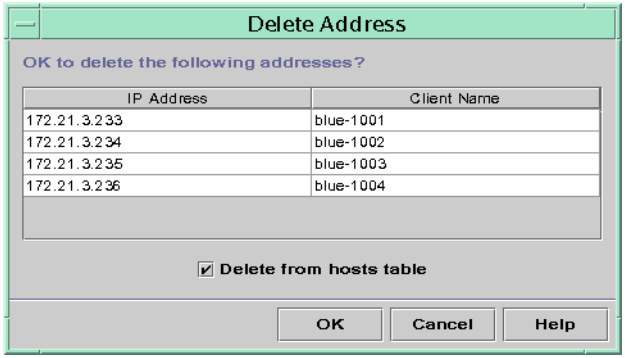
   ```
   pntadm -M 10.64.3.3 -f UNUSABLE 10.64.3.0
   ```

Suppression d'adresses IP du service DHCP

Il est recommandé de supprimer les adresses IP des tables de réseau DHCP pour éviter qu'elles restent sous le contrôle de DHCP. Pour ce faire, vous pouvez au choix exécuter la commande `pntadm -D` ou procéder à partir de la boîte de dialogue de suppression d'adresse dans le gestionnaire DHCP.

La figure suivante représente la boîte de dialogue de suppression d'adresse.

FIGURE 15–12 Boîte de dialogue de suppression d'adresse dans le gestionnaire DHCP



▼ Suppression des adresses IP du service DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Addresses.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez le réseau de l'adresse IP.**

3. **Choisissez la ou les adresses IP que vous avez l'intention de supprimer.**

   Pour supprimer plusieurs adresses à la fois, cliquez sur chacune d'elles tout en maintenant la touche Contrôle enfoncée. Pour sélectionner un bloc d'adresses, maintenez la touche Majuscule enfoncée pendant que vous cliquez.

4. **Choisissez Delete dans le menu Edit.**

   La boîte de dialogue de suppression d'adresse répertorie les adresses que vous avez sélectionnées pour vous permettre de confirmer leur suppression.

5. **Si vous voulez supprimer les noms d'hôtes de la table des hôtes, sélectionnez l'option Delete From Hosts Table.**

   Si les noms d'hôtes ont été générés par le gestionnaire DHCP, vous souhaiterez éventuellement effacer les noms de la table des hôtes.

6. **Cliquez sur OK.**

▼ Suppression des adresses IP du service DHCP (`pntadm`)

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Supprimez des adresses IP en entrant une commande sous le format suivant :**

   ```
   # pntadm -D ip-address options network-address
   ```

   Si vous incluez l'option `-y`, le nom d'hôte est supprimé du service de noms chargé de sa gestion.

Pour supprimer, par exemple, l'adresse `10.64.3.3` du réseau `10.64.3.0` et effacer le nom d'hôte correspondant, entrez la commande suivante :

```
pntadm -D 10.64.3.3 -y 10.64.3.0
```

Attribution d'une adresse IP réservée à un client DHCP

Le service DHCP essaie de fournir la même adresse IP à un client ayant déjà obtenu une adresse via DHCP. Il est possible, toutefois, que l'adresse ait été réallouée à un autre client.

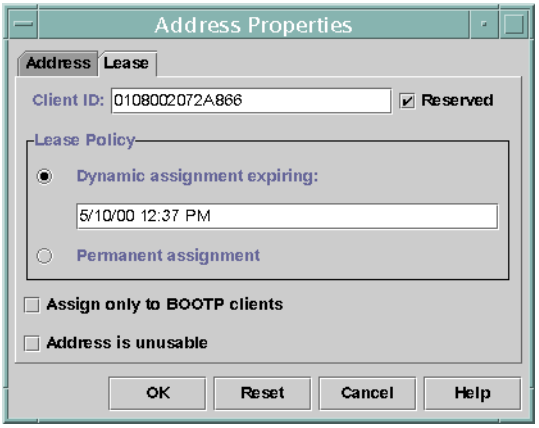
Les routeurs, les serveurs NIS ou NIS+, les serveurs DNS et les autres hôtes essentiels au réseau ne doivent pas faire partie des clients DHCP. Les hôtes offrant des services au réseau ne doivent pas compter sur le réseau pour obtenir leurs adresses IP. Il faut également veiller à ce que les clients tels que les serveurs d'impression ou les serveurs de fichiers aient des adresses IP fixes. Ces clients peuvent obtenir leurs configurations réseau et une adresse IP fixe du serveur DHCP.

Vous pouvez configurer le serveur DHCP de façon à ce qu'il propose toujours la même adresse IP au client chaque fois que celui-ci demande sa configuration. Pour ce faire, il convient d'assigner manuellement l'ID client à l'adresse IP que vous comptez réserver au client. Il est possible de mettre en place un bail dynamique ou permanent pour l'adresse réservée. Le bail dynamique permet d'effectuer plus facilement le suivi de l'utilisation de l'adresse. Un client sans disque est un exemple de client pour lequel il faut prévoir une adresse réservée avec un bail dynamique. Le bail permanent n'offre, en revanche, aucune possibilité de suivi. À partir du moment où le client obtient un bail permanent, il n'a plus besoin en effet de recontacter le serveur. Pour obtenir des données de configuration à jour, la seule solution pour le client est de libérer l'adresse IP et de recommencer la négociation du bail DHCP.

Vous pouvez vous servir de la commande `pntadm -M` ou de la boîte de dialogue des propriétés d'adresses dans le gestionnaire DHCP pour définir les propriétés du bail.

La figure suivante montre le contenu de l'onglet Lease de la boîte de dialogue des propriétés d'adresses qui permet de modifier le bail.

FIGURE 15–13 Onglet Lease de la boîte de dialogue des propriétés d'adresses dans le gestionnaire DHCP



▼ Affectation d'une adresse IP fixe à un client DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Addresses.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez le réseau qui convient.**

3. **Cliquez deux fois sur l'adresse IP que vous comptez réserver au client.**

   Cela a pour effet d'ouvrir la boîte de dialogue des propriétés d'adresses.

4. **Cliquez sur l'onglet Lease.**

5. **Entrez l'identificateur du client dans le champ Client ID.**

   L'ID client est dérivé de l'adresse matérielle du client. Pour plus d'informations, reportez-vous à l'entrée ID client du Tableau 15–4.

6. **Sélectionnez l'option Reserved pour éviter que l'adresse IP soit récupérée par le serveur.**

7. **Dans la section Lease Policy de la fenêtre, sélectionnez l'option d'affectation dynamique ou permanente.**

   Optez pour un bail dynamique si vous préférez que le client négocie le renouvellement des baux, ce qui vous permet d'effectuer le suivi de l'utilisation des adresses. Comme vous avez sélectionné l'option Reserved, l'adresse ne peut pas être récupérée même en cas d'attribution

d'un bail dynamique. Il est inutile de spécifier une date d'expiration pour ce bail. Le serveur DHCP calcule la date d'expiration sur la base de la durée du bail.

Si vous optez pour un bail permanent, vous ne pouvez pas assurer le suivi de l'utilisation de l'adresse IP sauf si vous activez la journalisation des transactions.

8 **Cliquez sur OK.**

▼ Affectation d'une adresse IP fixe à un client DHCP (`pntadm`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Définissez les indicateurs de bail en entrant une commande sous le format suivant :**

`# pntadm -M` *ip-address* `-i` *client-id* `-f MANUAL+BOOTP` *network-address*

Voici comment configurer, par exemple, le client DHCP possédant l'adresse MAC `08:00:20:94:12:1E` de façon à ce qu'il reçoive toujours l'adresse IP `10.21.5.12` :

```
pntadm -M 10.21.5.12 -i 0108002094121E -f MANUAL+BOOTP 10.21.0.0
```

Astuce – Pour plus d'informations sur les identificateurs de clients, reportez-vous à l'entrée ID client du Tableau 15–4.

Utilisation des macros DHCP (liste des tâches)

Les macros DHCP sont des conteneurs des options DHCP. Le service DHCP se sert des macros pour réunir des options à transmettre aux clients. Le gestionnaire DHCP et l'utilitaire `dhcpconfig` créent automatiquement plusieurs macros lorsque vous configurez le serveur. Pour plus d'informations au sujet des macros, reportez-vous à la section "À propos des macros DHCP" à la page 318 Pour plus d'informations sur les macros générées par défaut, reportez-vous au Chapitre 14, "Configuration du service DHCP (tâches)".

Lorsque des modifications se produisent sur votre réseau, il peut être nécessaire de changer les données de configuration transmises aux clients. Vous avez besoin, pour cela, d'intervenir au niveau des macros DHCP. Vous pouvez afficher, créer, modifier, dupliquer et supprimer des macros DHCP.

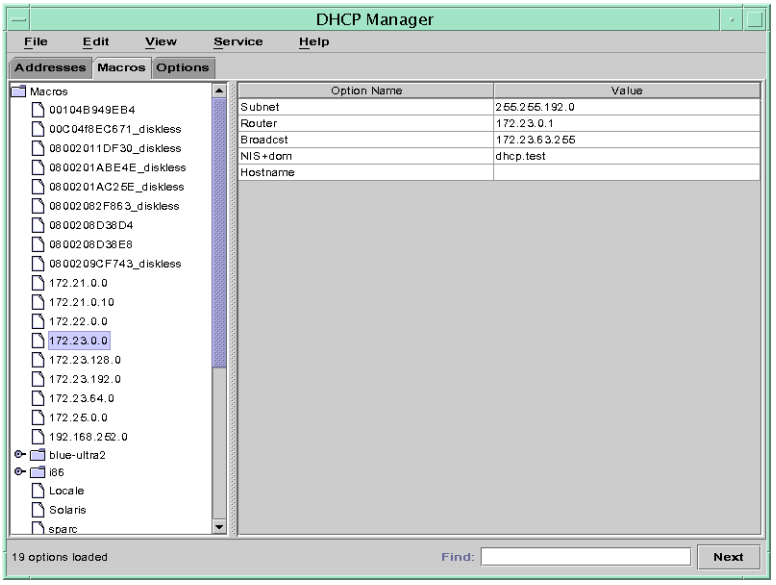
Lorsque vous manipulez des macros, il est essentiel de comprendre le fonctionnement des options DHCP standard, lesquelles sont décrites dans la page de manuel `dhcp_inittab(4)`.

La liste suivante présente les différentes tâches permettant de consulter, créer, modifier et supprimer des macros DHCP. La liste contient également des liens vers des sections expliquant en détails comment effectuer chacune de ces tâches.

Tâche	Description	Voir
Affichage des macros DHCP	Présente une liste de toutes les macros définies sur le serveur DHCP.	"Affichage des macros définies sur un serveur DHCP (gestionnaire DHCP)" à la page 403 "Affichage des macros définies sur un serveur DHCP (`dhtadm`)" à la page 404
Création des macros DHCP	Définit de nouvelles macros utiles aux clients DHCP.	"Création d'une macro DHCP (gestionnaire DHCP)" à la page 409 "Création d'une macro DHCP (`dhtadm`)" à la page 410
Modification des valeurs transmises dans des macros aux clients DHCP.	Procédez aux modifications voulues : changez les options existantes, ajoutez des options aux macros ou supprimez des options des macros.	"Modification des valeurs des options dans une macro DHCP (gestionnaire DHCP)" à la page 405 "Modification des valeurs des options dans une macro DHCP (`dhtadm`)" à la page 406 "Ajout d'options à une macro DHCP (gestionnaire DHCP)" à la page 406 "Ajout d'options à une macro DHCP (`dhtadm`)" à la page 407 "Suppression des options d'une macro DHCP (gestionnaire DHCP)" à la page 408 "Suppression des options d'une macro DHCP (`dhtadm`)" à la page 408
Suppression des macros DHCP	Supprimez les macros DHCP devenues inutiles.	"Suppression d'une macro DHCP (gestionnaire DHCP)" à la page 411 "Suppression d'une macro DHCP (`dhtadm`)" à la page 412

La figure suivante illustre l'onglet Macros de la fenêtre du gestionnaire DHCP.

FIGURE 15–14 Onglet Macros dans le gestionnaire DHCP



▼ Affichage des macros définies sur un serveur DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Macros.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

   La section Macros à gauche de la fenêtre affiche toutes les macros définies sur le serveur DHCP, classées par ordre alphabétique. Les macros précédées d'une icône de dossier contiennent des références à d'autres macros, alors que celles précédées d'une icône de document ne font référence à aucune autre macro.

2. **Pour ouvrir un dossier de macros, cliquez sur l'icône représentant une poignée à gauche de l'icône de dossier.**

   Vous obtenez alors la liste des macros faisant partie de la macro sélectionnée.

3. **Pour afficher le contenu d'une macro, cliquez sur le nom de la macro.**

   Cela a pour effet d'afficher les options et les valeurs qui leur sont attribuées.

▼ Affichage des macros définies sur un serveur DHCP (dhtadm)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichez les macros en entrant la commande suivante :**

```
# dhtadm -P
```

Cette commande permet d'obtenir une sortie standard du contenu formaté de la table `dhcptab`, avec l'ensemble des macros et des symboles définis sur le serveur DHCP.

Modification des macros DHCP

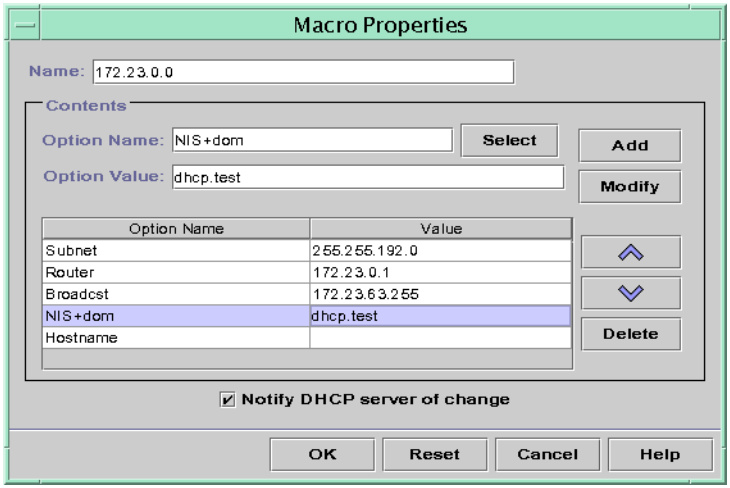
Il peut s'avérer nécessaire de modifier des macros si certains aspects du réseau évoluent et si un ou plusieurs clients DHCP ont besoin de connaître les changements apportés. Vous pouvez, par exemple, ajouter un routeur ou un serveur NIS, mettre en place un nouveau sous-réseau ou changer la stratégie de location.

Avant de commencer à modifier une macro, déterminez le nom de l'option DHCP que vous avez l'intention de changer, ajouter ou supprimer. Les options DHCP standard sont répertoriées dans l'aide du gestionnaire DHCP et dans la page de manuel `dhcp_inittab(4)`.

Modifiez les macros à l'aide de la commande `dhtadm -M -m` ou du gestionnaire DHCP. Pour plus d'informations au sujet de la commande `dhtadm`, reportez-vous à la page de manuel `dhtadm(1M)`.

La figure suivante représente la boîte de dialogue des propriétés de macro du gestionnaire DHCP.

FIGURE 15–15 Boîte de dialogue des propriétés de macro dans le gestionnaire DHCP



▼ Modification des valeurs des options dans une macro DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Macros.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez la macro à modifier.**

3. **Choisissez Properties dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue des propriétés de macros.

4. **Sélectionnez l'option que vous avez l'intention de modifier dans la table des options.**

   Le nom de l'option et sa valeur figurent respectivement dans les champs Option Name et Option Value.

5. **Dans le champ Option Value, sélectionnez l'ancienne valeur et entrez la nouvelle valeur de l'option.**

6. **Cliquez sur Modifier.**

   La nouvelle valeur s'affiche dans la table des options.

7 **Cochez la case Notify DHCP Server of Change.**

Cette option demande au serveur DHCP de relire le contenu de la table `dhcptab` et d'appliquer immédiatement la modification dès que vous cliquez sur OK.

8 **Cliquez sur OK.**

▼ Modification des valeurs des options dans une macro DHCP (`dhtadm`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Redéfinissez les valeurs des options en entrant une commande sous le format suivant :**

```
# dhtadm -M -m macroname -e 'option=value:option=value' -g
```

Voici comment changer, par exemple, la durée du bail et le décalage du temps universel dans la macro `bluenote` :

```
# dhtadm -M -m bluenote -e 'LeaseTim=43200:UTCOffst=28800' -g
```

▼ Ajout d'options à une macro DHCP (gestionnaire DHCP)

1 **Dans le gestionnaire DHCP, cliquez sur l'onglet Macros.**

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2 **Sélectionnez la macro à modifier.**

3 **Choisissez Properties dans le menu Edit.**

Cela a pour effet d'ouvrir la boîte de dialogue des propriétés de macros.

4 **Dans le champ Option Name, spécifiez le nom d'une option en procédant de l'une des façons suivantes :**

- **Cliquez sur le bouton Select à côté du champ Option Name pour sélectionner une option permettant d'ajouter la macro.**

  La boîte de dialogue de sélection d'option contient une liste alphabétique des noms des options et descriptions des catégories standard. Pour ajouter une option ne faisant pas partie de la catégorie standard, servez-vous de la liste Category.

  Pour plus d'informations au sujet des catégories de macros, reportez-vous à la section "À propos des macros DHCP" à la page 318.

- **Tapez `Include` pour inclure une référence à une macro existante dans la nouvelle macro.**

5 **Entrez la valeur de l'option dans le champ Option Value.**

Si vous avez entré **`Include`** en guise de nom d'option, vous devez spécifier le nom d'une macro existante dans le champ Option Value.

6 **Cliquez sur Add.**

L'option est placée à la fin de la liste des options dans cette macro. Pour changer la position de l'option dans la macro, sélectionnez l'option et cliquez sur les boutons fléchés pour la faire monter ou descendre dans la liste.

7 **Cochez la case Notify DHCP Server of Change.**

Cette option demande au serveur DHCP de relire le contenu de la table `dhcptab` et d'appliquer immédiatement la modification dès que vous cliquez sur OK.

8 **Cliquez sur OK.**

▼ Ajout d'options à une macro DHCP (`dhtadm`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez des options à une macro en entrant une commande sous le format suivant :**

```
# dhtadm -M -m macroname -e 'option=value' -g
```

Voici comment autoriser, par exemple, la négociation de baux dans la macro `bluenote` :

```
# dhtadm -M -m bluenote -e 'LeaseNeg=_NULL_VALUE' -g
```

S'il n'est pas nécessaire de spécifier de valeur pour une option, spécifiez `_NULL_VALUE` en guise de valeur pour cette option.

▼ Suppression des options d'une macro DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Macros.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez la macro à modifier.**

3. **Choisissez Properties dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue des propriétés de macros.

4. **Sélectionnez l'option que vous avez l'intention de supprimer de la macro.**

5. **Cliquez sur Delete.**

   L'option est retirée de la liste des options pour cette macro.

6. **Cochez la case Notify DHCP Server of Change.**

   Cette option demande au serveur DHCP de relire le contenu de la table `dhcptab` et d'appliquer immédiatement la modification dès que vous cliquez sur OK.

7. **Cliquez sur OK.**

▼ Suppression des options d'une macro DHCP (`dhtadm`)

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Supprimez une option d'une macro en entrant une commande sous le format suivant :**

```
# dhtadm -M -m macroname -e 'option=' -g
```

Voici comment empêcher, par exemple, la négociation de baux dans la macro `bluenote` :

```
# dhtadm -M -m bluenote -e 'LeaseNeg=' -g
```

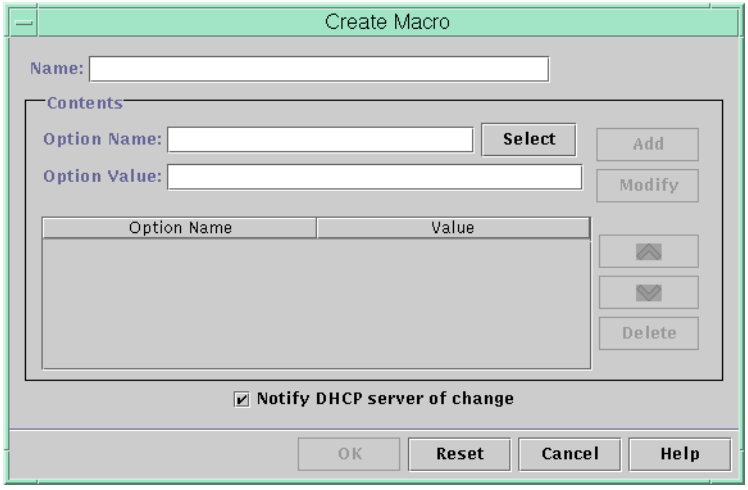
Si une option est spécifiée sans valeur, elle est supprimée de la macro.

Création de macros DHCP

Il peut être intéressant d'ajouter de nouvelles macros à votre service DHCP de façon à répondre aux besoins spécifiques de certains clients. Pour ce faire, vous pouvez faire appel à la commande `dhtadm -A -m` ou à la boîte de dialogue de création de macro du gestionnaire DHCP. Pour plus d'informations au sujet de la commande `dhtadm`, reportez-vous à la page de manuel `dhtadm(1M)`.

La figure suivante présente la boîte de dialogue de création de macro du gestionnaire DHCP.

FIGURE 15–16 Boîte de dialogue de création de macro dans le gestionnaire DHCP



▼ Création d'une macro DHCP (gestionnaire DHCP)

1 **Dans le gestionnaire DHCP, cliquez sur l'onglet Macros.**

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section “Démarrage et arrêt du gestionnaire DHCP” à la page 354.

2 **Choisissez Create dans le menu Edit.**

La boîte de dialogue de création de macro s'ouvre.

3 **Donnez un nom unique à la macro.**

Le nom peut être composé de 128 caractères alphanumériques. Si vous utilisez un nom qui correspond à un identificateur de classe de fournisseur, une adresse réseau ou un ID client, la macro est automatiquement traitée pour les clients concernés. Cela n'est pas le cas, en revanche, si vous utilisez un nom différent. Il faut, en effet, que la macro soit assignée à une adresse IP spécifique ou incorporée à une autre macro traitée automatiquement. Pour plus d'informations, reportez-vous à la section "Traitement des macros par le serveur DHCP" à la page 318.

4 **Cliquez sur le bouton Select juste à côté du champ Option Name.**

La boîte de dialogue de sélection d'option contient une liste alphabétique des noms des options et descriptions des catégories standard. Pour ajouter une option ne faisant pas partie de la catégorie standard, servez-vous de la liste Category. Sélectionnez la catégorie qui vous intéresse dans la liste Category. Pour plus d'informations au sujet des catégories d'options, reportez-vous à la section "À propos des options DHCP" à la page 317.

5 **Sélectionnez l'option que vous souhaitez ajouter à la macro et cliquez sur OK.**

La boîte de dialogue des propriétés de macros affiche l'option choisie dans le champ Option Name.

6 **Entrez la valeur de l'option dans le champ Option Value et cliquez sur Add.**

L'option est placée à la fin de la liste des options dans cette macro. Pour changer la position de l'option dans la macro, sélectionnez l'option et cliquez sur les boutons fléchés pour la faire monter ou descendre dans la liste.

7 **Répétez l'Étape 5 et l'Étape 6 pour chaque option à ajouter à la macro.**

8 **Lorsque vous avez terminé, sélectionnez l'option Notify DHCP Server of Change.**

Cette option demande au serveur DHCP de relire le contenu de la table `dhcptab` et d'appliquer immédiatement la modification dès que vous cliquez sur OK.

9 **Cliquez sur OK.**

▼ Création d'une macro DHCP (`dhtadm`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Créez une macro en entrant une commande sous le format suivant :**

```
# dhtadm -A -m macroname -d ':option=value:option=value:option=value:' -g
```

Le nombre de couples *option=valeur* qu'il est possible d'inclure dans l'argument de `-d` n'est pas limité. L'argument doit commencer et se terminer par le signe deux-points. Chaque couple *option=valeur* doit également être délimité par ce symbole. La chaîne entière doit être placée entre guillemets.

Pour créer, par exemple, la macro `bluenote`, entrez la commande suivante :

```
# dhtadm -A -m bluenote -d ':Router=10.63.6.121\ :LeaseNeg=_NULL_VALUE:DNSserv=10.63.2
```

S'il n'est pas nécessaire de spécifier de valeur pour une option, spécifiez `_NULL_VALUE` en guise de valeur pour cette option.

Suppression de macros DHCP

Il peut être nécessaire, parfois, de supprimer une macro du service DHCP. Lorsque vous supprimez, par exemple, un réseau du service DHCP, vous avez également la possibilité d'effacer la macro de réseau qui lui est associée.

Pour supprimer les macros, vous pouvez au choix exécuter la commande `dhtadm -D -m` ou le gestionnaire DHCP.

▼ Suppression d'une macro DHCP (gestionnaire DHCP)

1 **Dans le gestionnaire DHCP, cliquez sur l'onglet Macros.**

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2 **Sélectionnez la macro à supprimer.**

Vous êtes invité à confirmer la suppression de la macro spécifiée dans la boîte de dialogue de suppression de macro.

3 **Cochez la case Notify DHCP Server of Change.**

Cette option demande au serveur DHCP de relire le contenu de la table `dhcptab` et d'appliquer immédiatement la modification dès que vous cliquez sur OK.

4 **Cliquez sur OK.**

▼ Suppression d'une macro DHCP (`dhtadm`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Supprimez une macro en entrant une commande sous le format suivant :**

```
# dhtadm -D -m macroname -g
```

Pour supprimer, par exemple, la macro `bluenote`, voici la commande qu'il convient d'entrer :

```
# dhtadm -D -m bluenote -g
```

Utilisation des options DHCP (liste des tâches)

Les options sont des mots-clés spécifiques aux paramètres de configuration de réseau que le serveur DHCP peut transmettre aux clients. Dans le service DHCP, vous n'êtes pas en mesure de créer, supprimer ou modifier les options DHCP standard. Comme les options standard sont définies par le protocole DHCP, il vous est impossible de les changer. Les tâches que vous pouvez effectuer s'appliquent uniquement aux options que vous créez pour votre site. C'est la raison pour laquelle l'onglet Options dans le gestionnaire DHCP est vide la première fois que vous configurez votre service DHCP.

Si vous créez des options sur le serveur DHCP, vous devez aussi ajouter des informations au sujet des options sur le client DHCP. En ce qui concerne le client DHCP, vous devez modifier le fichier `/etc/dhcp/inittab` afin d'ajouter des entrées pour les nouvelles options. Pour plus d'informations au sujet de ce fichier, reportez-vous à la page de manuel `dhcp_inittab(4)`.

Si vous disposez de clients DHCP qui ne sont pas des clients Oracle Solaris, consultez la documentation de ces clients pour savoir comment ajouter des options ou des symboles. Pour plus d'informations à propos des options dans DHCP , reportez-vous à la section "À propos des options DHCP" à la page 317.

Vous pouvez, au choix, exécuter le gestionnaire DHCP ou la commande `dhtadm` pour créer, modifier ou supprimer des options.

Astuce – Les options sont appelées des *symboles* dans le jargon DHCP. La commande `dhtadm` et la page de manuel correspondante font également référence aux options sous l'appellation symboles.

La liste suivante présente les différentes tâches permettant de créer, modifier et supprimer des options DHCP. Elle propose également des liens aux procédures correspondantes.

Tâche	Description	Voir
Création d'options DHCP.	Ajoutez de nouvelles options pour les informations non gérables par une option DHCP standard.	"Création des options DHCP (gestionnaire DHCP)" à la page 416 "Création des options DHCP (`dhtadm`)" à la page 417 "Modification des informations relatives aux options du client DHCP" à la page 421
Modification des options DHCP.	Changez les propriétés des options DHCP que vous avez créées.	"Modification des propriétés des options DHCP (gestionnaire DHCP)" à la page 418 "Modification des propriétés des options DHCP (`dhtadm`)" à la page 419
Suppression des options DHCP.	Effacez des options DHCP que vous avez créées.	"Suppression des options DHCP (gestionnaire DHCP)" à la page 420 "Suppression des options DHCP (`dhtadm`)" à la page 421

Avant de créer des options DHCP, vous devez vous familiariser aux propriétés d'option répertoriées dans le tableau suivant.

TABLEAU 15–5 Propriétés des options DHCP

Propriété d'option	Description
Catégorie	La *catégorie* d'une option doit correspondre à l'une des trois catégories suivantes : ■ Vendor – Options spécifiques à la plate-forme fournisseur d'un client, soit matérielle ou logicielle. ■ Site – Options spécifiques à votre site. ■ Extend – Dernières options ajoutées au protocole DHCP, mais pas encore implémentées en tant qu'options standard dans DHCP.

TABLEAU 15–5 Propriétés des options DHCP *(Suite)*

Propriété d'option	Description
Code	Le *code* est le numéro unique que vous assignez à une option. Il est impossible d'utiliser le même pour une autre option au sein de la même catégorie. À chaque catégorie d'options correspond un code particulier : ■ Vendor – Valeurs de code comprises entre 1 et 254 pour chaque classe fournisseur ■ Site – Valeurs de code comprises entre 128 et 254 ■ Extend – Valeurs de code comprises entre 77 et 127
Type de données	Le *type de données* indique les données qu'il est possible d'assigner en tant que valeur à l'option. La liste suivante décrit les différents types de données valides. ■ ASCII – Valeur de chaîne de texte. ■ BOOLEEN – Aucune valeur n'est associée avec les données booléennes. La présence de l'option indique qu'une condition est vérifiée. Son absence signifie, au contraire, que la condition n'est pas vérifiée. Admettons, par exemple, que l'option `Hostname` possède le type de données Booléen. Si `Hostname` figure dans une macro, le serveur DHCP recherche le nom d'hôte associé à l'adresse assignée. ■ IP – Une ou plusieurs adresses IP au format de numérotation décimale avec points (*xxx.xxx.xxx.xxx*). ■ OCTET – Représentation ASCII non interprétée de données binaires. Un ID client utilise, par exemple, le type de données octet. Vous pouvez utiliser des chiffres (0 à 9), des lettres (A à F et a à f). Deux caractères ASCII sont nécessaires pour représenter 8 bits de données. ■ UNUMBER8, UNUMBER16, UNUMBER32, UNUMBER64, SNUMBER8, SNUMBER16, SNUMBER32 ou SNUMBER64 – Valeur numérique. L'initiale U ou S indique respectivement si le nombre est non signé ou signé. Les chiffres de fin indiquent le nombre de bits de codage du nombre.
Granularité	La *granularité* spécifie le nombre d'instances de données nécessaires pour représenter une valeur d'option complète. Le type de données IP et une granularité de 2 signifient, par exemple, que la valeur d'option doit contenir deux adresses IP.
Maximum	Nombre maximum de valeurs pouvant être spécifiées pour l'option. Prenons l'exemple suivant : maximum = 2, granularité = 2 et type de données = IP. Dans ce cas, la valeur d'option doit contenir un maximum de deux couples d'adresses IP.

TABLEAU 15–5 Propriétés des options DHCP *(Suite)*

Propriété d'option	Description
Classes client fournisseur	Cette option est disponible à condition d'avoir choisi la catégorie Vendor. Les classes client fournisseur identifient les classes client auxquelles l'option Vendor est associée. La classe est une chaîne de caractères ASCII représentant le type de machine client ou le système d'exploitation. La chaîne de la classe pour certains modèles de stations de travail Sun est, par exemple, `SUNW.Sun-Blade-100`. Ce type d'option permet de définir les paramètres de configuration transmis à tous les clients de la même classe et *uniquement* les clients de cette classe. Vous êtes libre de spécifier plusieurs classes client. Seuls les clients DHCP pour lesquels la valeur de classe client correspond à une classe que vous spécifiez reçoivent les options délimitées par cette classe. La classe client est déterminée par le fournisseur du client DHCP. Pour les clients DHCP qui ne sont pas des clients Oracle Solaris, reportez-vous à la documentation correspondante du fournisseur pour la classe client. Pour les clients Oracle Solaris, vous pouvez obtenir la classe client Vendor en entrant la commande `prtconf -b` sur le client. Pour spécifier la classe client Vendor, remplacez par des points les virgules de la chaîne renvoyée par la commande `uname.` Si, par exemple, la chaîne `SUNW,Sun-Blade-100` est renvoyée par la commande prtconf -b, définissez la classe client Vendor sous la forme suivante : `SUNW.Sun-Blade-100`.

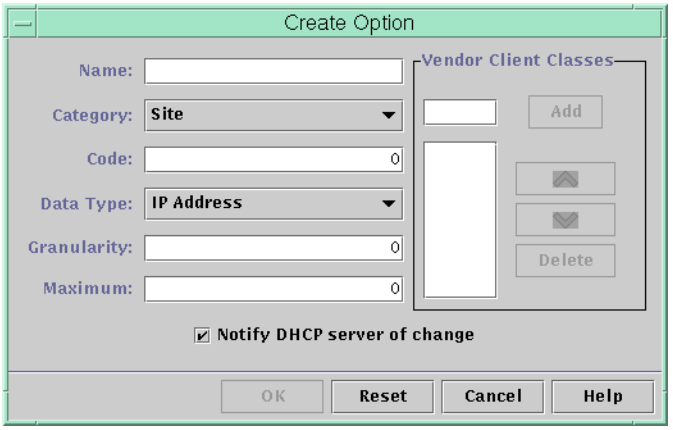
Création des options DHCP

Si vous avez besoin de communiquer des données client pour lesquelles aucune option n'existe dans le protocole DHCP, il suffit de créer une option. Pour connaître toutes les options définies dans DHCP avant de créer votre propre option, reportez-vous à la page de manuel `dhcp_inittab(4)`.

Servez-vous, au choix, de la commande `dhtadm -A -s` ou de la boîte de dialogue de création d'option dans le gestionnaire DHCP pour créer des options.

La figure suivante présente la boîte de dialogue de création d'option du gestionnaire DHCP.

FIGURE 15–17 Boîte de dialogue de création d'option dans le gestionnaire DHCP



▼ Création des options DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Options.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Choisissez Create dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue de création d'option.

3. **Donnez un nom descriptif à la nouvelle option.**

   Ce nom peut être composé d'un maximum de 128 caractères alphanumériques, espaces compris.

4. **Entrez ou sélectionnez des valeurs pour chaque paramètre dans la boîte de dialogue.**

   Pour plus d'informations sur les différents paramètres, reportez-vous au Tableau 15–5 ou affichez l'aide du gestionnaire DHCP.

5. **Lorsque vous avez terminé, sélectionnez l'option Notify DHCP Server of Change.**

   Cette option demande au serveur DHCP de relire le contenu de la table `dhcptab` et d'appliquer immédiatement la modification dès que vous cliquez sur OK.

6. **Cliquez sur OK.**

   Vous pouvez, à présent, ajouter l'option aux macros et assigner une valeur à l'option à transmettre aux clients.

▼ Création des options DHCP (`dhtadm`)

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Créez une option DHCP en entrant une commande sous le format suivant :**

   ```
   # dhtadm -A -s option-name -d 'category,code,data-type,granularity,maximum' -g
   ```

   nom-option — Chaîne alphanumérique composée d'un maximum de 128 caractères.

   catégorie — Trois possibilités : `Site`, `Extend` ou `Vendor=`*liste-de-classes* . *liste-de-classes* désigne une liste de classes de clients fournisseur séparées par des virgules auxquelles l'option s'applique. Pour savoir comment déterminer la classe de clients fournisseur, reportez-vous au Tableau 15–5.

   code — Valeur numérique convenant à la catégorie d'options. Voir la description donnée dans le Tableau 15–5.

   type-données — Information définie par un mot-clé indiquant le type de données transmis avec l'option. Voir la description donnée dans le Tableau 15–5.

   granularité — Information définie par un nombre non négatif. Voir la description donnée dans le Tableau 15–5.

   maximum — Nombre non négatif. Voir la description donnée dans le Tableau 15–5.

Exemple 15–3 Création d'une option DHCP avec `dhtadm`

La commande suivante aurait pour effet de créer une option appelée `NouvOpt` faisant partie de la catégorie Site. Le code de l'option est 130. Un nombre entier unique non signé de 8 bits peut être défini comme valeur de cette option.

```
# dhtadm -A -s NouvOpt -d 'Site,130,UNUMBER8,1,1' -g
```

La commande suivante aurait pour effet de créer une option appelée `NewServ` dans la catégorie Vendor. Elle s'applique aux clients dont le type de machine est `SUNW,Sun-Blade-100` ou `SUNW,Sun-Blade-1000`. Le code de l'option est 200. Une adresse IP peut être définie comme valeur de cette option.

```
# dhtadm -A -s NewServ -d 'Vendor=SUNW.Sun-Blade-100 \ SUNW.Sun-Blade-1000,200,IP,1,1'
```

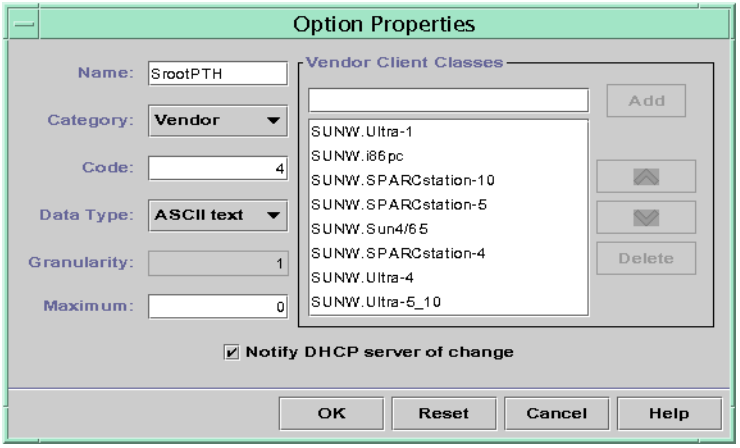
Modification des options DHCP

Si vous avez créé des options pour votre service DHCP, vous avez la possibilité de changer les propriétés de ces options. Pour ce faire, vous pouvez faire appel à la commande `dhtadm -M -s` ou à la boîte de dialogue des propriétés d'options du gestionnaire DHCP.

Vous devez modifier les informations relatives aux options du client DHCP pour répercuter les modifications apportées au service DHCP. Reportez-vous à la section “Modification des informations relatives aux options du client DHCP” à la page 421.

La figure suivante représente la boîte de dialogue des propriétés d'options du gestionnaire DHCP.

FIGURE 15–18 Boîte de dialogue des propriétés d'options dans le gestionnaire DHCP



▼ Modification des propriétés des options DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Options.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section “Démarrage et arrêt du gestionnaire DHCP” à la page 354.

2. **Sélectionnez l'option que vous souhaitez modifier.**

3. **Choisissez Properties dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue des propriétés d'options.

4 **Modifiez les propriétés comme bon vous semble.**

Pour plus d'informations sur les propriétés, reportez-vous au Tableau 15–5 ou affichez l'aide du gestionnaire DHCP.

5 **Lorsque vous avez terminé, sélectionnez l'option Notify DHCP Server of Change.**

Les changements sont appliqués à la table `dhcptab` . Le serveur DHCP est invité à relire le contenu de la table `dhcptab` et à appliquer les changements.

6 **Cliquez sur OK.**

▼ Modification des propriétés des options DHCP (`dhtadm`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Modifiez une option en entrant une commande sous le format suivant :**

```
# dhtadm -M -s option-name -d 'category,code,data-type,granularity,maximum' -g
```

nom-option Indique le nom de l'option que vous avez l'intention de changer.

catégorie Il peut s'agir de `Site`, `Extend` ou `Vendor=`*liste-de-classes*. *liste-de-classes* désigne une liste de classes de clients fournisseur séparées par des virgules auxquelles l'option s'applique. Exemple : `SUNW.Sun-Blade-100 SUNW.Ultra-80 SUNWi86pc`.

code Spécifie une valeur numérique convenant à la catégorie d'options. Voir la description donnée dans le Tableau 15–5.

type-données Spécifie un mot-clé indiquant le type de données transmis avec l'option. Voir la description donnée dans le Tableau 15–5.

granularité Nombre non négatif. Voir la description donnée dans le Tableau 15–5.

maximum Nombre non négatif. Voir la description donnée dans le Tableau 15–5.

Vous êtes tenu de définir l'ensemble des propriétés d'option DHCP à l'aide du commutateur `-d`, et non pas uniquement les propriétés que vous avez l'intention de changer.

Exemple 15–4 Modification d'une option DHCP avec `dhtadm`

La commande suivante aurait pour effet de modifier une option appelée `NouvOpt` . Il s'agit d'une option de la catégorie Site. Le code de l'option est 135. Un nombre entier unique non signé de 8 bits peut être défini comme valeur de cette option.

```
# dhtadm -M -s NouvOpt -d 'Site,135,UNUMBER8,1,1'
```

La commande suivante aurait pour effet de créer une option appelée `NouvServ` faisant partie de la catégorie Vendor. L'option s'applique, à présent, aux clients dont le type de machine est `SUNW,Sun-Blade-100` ou `SUNW,i86pc`. Le code de l'option est 200. Une adresse IP peut être définie comme valeur de cette option.

```
# dhtadm -M -s NewServ -d 'Vendor=SUNW.Sun-Blade-100 \ SUNW.i86pc,200,IP,1,1' -g
```

Suppression des options DHCP

Il est impossible de supprimer des options DHCP standard. Cependant, si vous avez défini des options pour votre service DHCP, vous avez la possibilité de supprimer ces options au moyen du gestionnaire DHCP ou de la commande `dhtadm`.

▼ Suppression des options DHCP (gestionnaire DHCP)

1. **Dans le gestionnaire DHCP, cliquez sur l'onglet Options.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Sélectionnez l'option que vous souhaitez supprimer.**

3. **Choisissez Delete dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue de suppression des options.

4. **Lorsque vous avez terminé, sélectionnez l'option Notify DHCP Server of Change.**

   Cette option demande au serveur DHCP de relire le contenu de la table `dhcptab` et d'appliquer immédiatement la modification dès que vous cliquez sur OK.

5. **Cliquez sur OK.**

▼ Suppression des options DHCP (`dhtadm`)

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Supprimez une option DHCP en entrant une commande sous le format suivant :**

   ```
   # dhtadm -D -s option-name -g
   ```

Modification des informations relatives aux options du client DHCP

Si vous ajoutez une nouvelle option DHCP à votre serveur DHCP, vous devez ajouter une entrée complémentaire dans les informations relatives aux options de chaque client DHCP. Si vous avez un client qui n'est pas un client DHCP, consultez la documentation de référence de ce client pour savoir comment ajouter des options ou des symboles.

Pour les clients DHCP, vous devez modifier le fichier `/etc/dhcp/inittab` et ajouter une entrée pour chaque option ajoutée au serveur DHCP. Si vous changez par la suite l'option sur le serveur, vous êtes dans l'obligation de modifier l'entrée dans le fichier `/etc/dhcp/inittab` du client.

Pour plus d'informations sur la syntaxe du fichier `/etc/dhcp/inittab`, reportez-vous à la page de manuel `dhcp_inittab(4)`.

Remarque – Si vous avez ajouté des options DHCP au fichier `dhcptags` dans une version précédente d'Oracle Solaris, vous devez ajouter ces options au fichier `/etc/dhcp/inittab` . Pour plus d'informations, reportez-vous à la section "Informations relatives aux options DHCP" à la page 488.

Prise en charge de l'installation réseau Oracle Solaris avec le service DHCP

Vous pouvez utiliser le protocole DHCP pour installer Oracle Solaris sur certains systèmes client de votre réseau. Seuls les systèmes `sun4u` et x86 répondant à la configuration matérielle requise pour exécuter Oracle Solaris peuvent utiliser cette fonction. Pour plus d'informations sur la configuration automatique des systèmes clients du réseau au moment de leur initialisation à l'aide de DHCP, reportez-vous au Chapitre 2, “Préconfiguration des informations de configuration système – Tâches” du *Guide d'installation Oracle Solaris 10 9/10 : installations réseau*.

Le service DHCP prend également en charge les systèmes clients Oracle Solaris installés et initialisés à distance à partir de serveurs sur une connexion WAN en utilisant le protocole HTTP. Cette méthode est désignée sous le nom d'*installation et d'initialisation via une connexion WAN*. Grâce à la méthode d'initialisation par le biais d'une connexion WAN, vous pouvez installer Oracle Solaris sur des systèmes SPARC sur un réseau public de très grande taille, même si l'infrastructure de ce réseau n'est pas sécurisée. Vous pouvez combiner l'initialisation via une connexion WAN avec des fonctions de sécurité afin de préserver la confidentialité des données et l'intégrité de l'image d'installation.

Avant d'utiliser DHCP pour initialiser et installer des systèmes clients à distance via une connexion WAN, vous devez configurer le serveur DHCP pour fournir les informations suivantes aux clients :

- adresse IP du serveur proxy
- emplacement du programme `wanboot-cgi`

Pour plus d'informations sur la configuration du serveur DHCP afin qu'il fournisse ces informations, reportez-vous au Chapitre 2, “Préconfiguration des informations de configuration système – Tâches” du *Guide d'installation Oracle Solaris 10 9/10 : installations réseau*. Pour plus d'informations sur l'initialisation et l'installation des systèmes clients avec un serveur DHCP sur un WAN, reportez-vous au Chapitre 10, “Initialisation via connexion WAN - Présentation” du *Guide d'installation Oracle Solaris 10 9/10 : installations réseau*.

Pour plus d'informations sur la prise en charge des clients sans disque, reportez-vous à la section “Prise en charge des clients d'initialisation à distance et sans disque (liste des tâches)” à la page 423.

Prise en charge des clients d'initialisation à distance et sans disque (liste des tâches)

Le service DHCP peut prendre en charge des systèmes clients Oracle Solaris capables de monter leurs fichiers de système d'exploitation à distance à partir d'une autre machine (le serveur SE). Ces clients sont généralement appelés des *clients sans disque*. Il s'agit en quelque sorte de clients d'initialisation distants persistants. Chaque fois qu'un client sans disque s'initialise, il doit se procurer le nom et l'adresse IP du serveur hébergeant les fichiers du système d'exploitation du client. Il peut alors démarrer à distance à partir de ces fichiers.

Chaque client sans disque possède sa propre partition racine sur le serveur SE, laquelle est partagée avec le nom d'hôte du client. Le serveur DHCP doit toujours renvoyer la même adresse IP à un client sans disque. Cette adresse doit rester mappée au même nom d'hôte dans le service de noms (DNS, par exemple). Lorsqu'un client sans disque reçoit la même adresse IP, il utilise un nom d'hôte cohérent et a la possibilité d'accéder à sa partition racine sur le serveur SE.

Outre l'adresse IP et le nom d'hôte, le serveur DHCP peut fournir l'emplacement des fichiers du système d'exploitation du client sans disque. Vous devez, cependant, créer des options et des macros afin de transmettre les informations dans un paquet de message DHCP.

La liste des tâches suivante présente les tâches à effectuer pour prendre en charge les clients sans disque ou tout autre client d'initialisation à distance persistant. Elle propose également les liens aux procédures correspondantes.

Tâche	Description	Voir
Configurez les services du système d'exploitation sur un serveur Oracle Solaris.	Servez-vous de la commande `smosservice` pour créer des fichiers de système d'exploitation pour les clients.	Chapitre 7, “Gestion des clients sans disque (tâches)” du *Guide d'administration système : administration de base* Voir aussi la page de manuel `smosservice`(1M).
Configuration du service DHCP dans le but de prendre en charge les clients d'initialisation du réseau.	Servez-vous du gestionnaire DHCP ou de la commande `dhtadm` pour créer de nouvelles options et macros Vendor pouvant être utilisées par le serveur DHCP pour transmettre les informations d'initialisation aux clients. Si vous avez déjà défini les options nécessaires aux clients d'installation du réseau, il suffit de créer les macros pour les types de client Vendor des clients sans disque.	Chapitre 2, “Préconfiguration des informations de configuration système – Tâches” du *Guide d'installation Oracle Solaris 10 9/10 : installations réseau*

Tâche	Description	Voir
Allocation d'adresses IP réservées aux clients sans disque.	Servez-vous du gestionnaire DHCP pour indiquer que l'adresse est réservée ou exécutez la commande `pntadm` pour marquer les adresses en mode `MANUAL` pour les clients sans disque.	"Attribution d'une adresse IP réservée à un client DHCP" à la page 399
Configuration des clients sans disque pour le service SE.	Servez-vous de la commande `smdiskless` pour ajouter la prise en charge du système d'exploitation sur le serveur SE pour chaque client. Spécifiez l'adresse IP que vous avez réservée à chaque client.	Chapitre 7, "Gestion des clients sans disque (tâches)" du *Guide d'administration système : administration de base* Voir aussi la page de manuel `smdiskless`(1M).

Configuration des clients DHCP pour qu'ils reçoivent uniquement des informations (liste des tâches)

Sur certains réseaux, vous pouvez faire en sorte que le service DHCP fournisse uniquement des données de configuration aux clients. Les systèmes clients ayant besoin d'informations et non de baux, peuvent utiliser le client DHCP pour adresser un message `INFORM`. Le message `INFORM` demande au serveur DHCP d'envoyer les données de configuration appropriées au client.

Il est possible de configurer le serveur DHCP dans le but de prendre en charge les clients recherchant uniquement des informations. Pour ce faire, il convient de créer une table de réseau vide correspondant au réseau hébergeant les clients. Cette table permet au serveur DHCP de répondre aux clients à partir du réseau en question.

La liste des tâches suivante présente les tâches à effectuer pour gérer les clients ayant besoin uniquement d'informations. Elle propose également les liens aux procédures correspondantes.

Tâche	Description	Voir
Création d'une table de réseau vide.	Servez-vous du gestionnaire DHCP ou de la commande `pntadm` pour créer une table pour le réseau hébergeant les clients souhaitant recevoir uniquement des informations.	"Ajout de réseaux DHCP" à la page 374
Création de macros afin d'obtenir les informations demandées par les clients.	Servez-vous du gestionnaire DHCP ou de la commande `dhtadm` pour créer des macros permettant de transmettre les informations requises aux clients.	"Création de macros DHCP" à la page 409

Tâche	Description	Voir
Demande d'émission d'un message `INFORM` par le client DHCP.	Exécutez la commande `ifconfig` *int* `dhcp inform` pour obliger le client DHCP à adresser un message `INFORM`.	"Démarrage du client DHCP" à la page 440 "Options de la commande `ifconfig` utilisées par le client DHCP" à la page 445 Page de manuel `ifconfig(1M)`

Conversion à un autre format de magasin de données DHCP

DHCP offre un utilitaire permettant de convertir les données de configuration DHCP d'un magasin de données au format d'un autre magasin de données. Plusieurs raisons peuvent motiver cette opération de conversion. L'augmentation du nombre de clients DHCP exige, par exemple, des performances ou une capacité supérieures du service DHCP. Il peut également être intéressant de répartir les charges du serveur DHCP entre plusieurs serveurs. Le chapitre "Sélection du magasin de données DHCP" à la page 327 compare les avantages et les inconvénients de chaque type de magasin de données.

Remarque – Si vous avez effectué une mise à niveau d'Oracle Solaris à partir d'une version antérieure à Solaris 8 7/01, veuillez prendre en compte cette remarque.

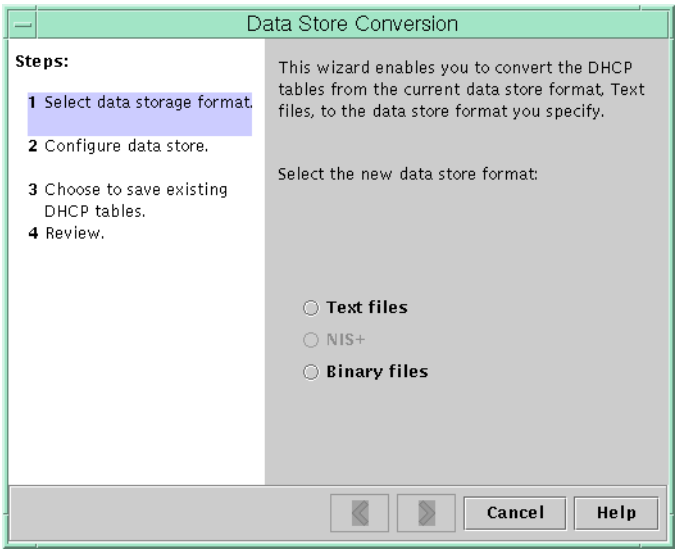
Lorsque vous exécutez un outil DHCP après avoir installé Oracle Solaris, vous êtes invité à convertir vos données au format du nouveau magasin de données. Il faut savoir, en effet, que le format des données stockées dans les fichiers et dans NIS+ a changé dans la version Solaris 8 7/01. Si vous ne convertissez pas vos données, le serveur DHCP continuera à exploiter le contenu des anciennes tables de données. Étant donné que le serveur est capable uniquement de prolonger les baux des clients existants, vous n'aurez pas la possibilité d'enregistrer de nouveaux clients DHCP ou de profiter des outils de gestion DHCP avec les anciennes tables de données.

L'utilitaire de conversion est également pratique pour les sites envisageant la conversion d'un magasin de données de type Sun à un format tiers. Après avoir analysé les entrées du magasin de données existant, l'utilitaire ajoute de nouvelles entrées avec le même contenu dans le nouveau magasin de données. L'accès au magasin de données est géré, module par module, pour chaque magasin de données. Cette approche permet à l'utilitaire de conversion d'adapter les données DHCP d'un magasin de données au format de tout autre magasin de données. Chaque magasin de données doit disposer d'un module accessible au service DHCP. Reportez-vous au *Solaris DHCP Service Developer's Guide* (en anglais) pour plus d'informations sur la rédaction d'un module permettant de prendre en charge un magasin de données d'une tierce partie.

La conversion du magasin de données peut être assurée par le gestionnaire DHCP au moyen de l'assistant de conversion des magasins de données ou à l'aide de la commande `dhcpconfig -C`.

La boîte de dialogue initiale de l'assistant est représentée à la figure suivante.

FIGURE 15–19 Boîte de dialogue de l'assistant de conversion des magasins de données dans le gestionnaire DHCP



Avant de lancer la conversion, vous devez préciser s'il est nécessaire ou non de sauvegarder les anciennes tables du magasin de données (`dhcptab` et tables de réseau). L'utilitaire de conversion se charge d'arrêter le serveur DHCP, de convertir le magasin de données, puis de redémarrer le serveur une fois l'opération terminée. Si vous n'avez pas souhaité sauvegarder les anciennes tables, l'utilitaire les supprime après s'être assuré que la conversion a réussi. La procédure de conversion peut prendre du temps. Elle est exécutée en arrière-plan et un compteur permet de suivre le déroulement de l'opération.

▼ Conversion du magasin de données DHCP (gestionnaire DHCP)

1. **À partir du gestionnaire DHCP, choisissez Convert Data Store dans le menu Service.**

   Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section “Démarrage et arrêt du gestionnaire DHCP” à la page 354.

   Cela a pour effet de lancer l'assistant de conversion des magasins de données.

2. **Répondez aux invites de l'assistant.**

   Si vous avez des difficultés à fournir les informations demandées, cliquez sur le bouton d'aide pour obtenir des détails sur chaque boîte de dialogue.

3 **Vérifiez vos sélections, puis cliquez sur Finish pour commencer la conversion du magasin de données.**

Le serveur DHCP redémarre dès que la conversion est terminée. Le serveur utilise immédiatement le nouveau magasin de données.

▼ Conversion du magasin de données DHCP (`dhcpconfig -C`)

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Convertissez le magasin de données en entrant une commande au format suivant :**

```
# /usr/sbin/dhcpconfig -C -r resource -p path
```

ressource correspond au nouveau type de magasin de données, tel que `SUNWbinfiles`

path représente le chemin d'accès aux données, tel que `/var/dhcp`

Si vous souhaitez conserver les données d'origine dans l'ancien magasin de données à l'issue de la conversion, spécifiez l'option `-k`. Par exemple, pour convertir votre magasin de données au format `SUNWbinfiles` et sauvegarder l'ancien magasin de données, entrez la commande suivante :

```
# /usr/sbin/dhcpconfig -C -r SUNWbinfiles -p /var/dhcp -k
```

Pour plus d'informations au sujet de l'utilitaire `dhcpconfig`, reportez-vous à la page de manuel `dhcpconfig(1M)`.

Transfert des données de configuration entre serveurs DHCP (liste de tâches)

Le gestionnaire DHCP et l'utilitaire `dhcpconfig` permettent de transférer tout ou partie des données de configuration DHCP d'un serveur DHCP à un autre. Vous pouvez transférer des réseaux entiers ainsi que toutes les adresses IP, macros et options associées aux réseaux. Mais vous pouvez également choisir de transférer uniquement les adresses IP, les macros et les

options qui vous intéressent. Vous êtes libre, en outre, de copier des macros et des options sans pour autant supprimer celles figurant sur le premier serveur.

Vous pouvez envisager le transfert des données de configuration lorsque vous souhaitez :

- ajouter un serveur en vue de partager les charges DHCP ;
- remplacer le système du serveur DHCP ;
- changer le chemin d'accès au magasin de données, tout en continuant à utiliser le même magasin de données.

La liste des tâches suivante indique les procédures à suivre pour transférer les données de configuration DHCP. La liste comprend également des liens vers des procédures expliquant comment effectuer cette tâche.

Tâche	Description	Voir
1. Exportation des données à partir du premier serveur.	Sélectionnez les données que vous souhaitez déplacer vers un autre serveur et créez un fichier des données exportées.	"Exportation des données à partir d'un serveur DHCP (gestionnaire DHCP)" à la page 430 "Exportation des données à partir d'un serveur DHCP (`dhcpconfig -X`)" à la page 430
2. Importation des données sur le deuxième serveur.	Copiez les données exportées vers le magasin de données d'un autre serveur DHCP.	"Importation des données sur un serveur DHCP (gestionnaire DHCP)" à la page 431 "Importation des données sur un serveur DHCP (`dhcpconfig -I`)" à la page 432
3. Modification des données importées en fonction du nouvel environnement de serveur.	Adaptez les données de configuration du serveur à celles du nouveau serveur.	"Modification des données DHCP importées (gestionnaire DHCP)" à la page 432 "Modification des données DHCP importées (`pntadm`, `dhtadm`)" à la page 433

Dans le gestionnaire DHCP, vous devez faire successivement appel à l'assistant d'exportation des données et à l'assistant d'importation des données pour transférer les données d'un serveur à un autre. Il convient ensuite de modifier les macros dans l'onglet Macros. Les figures suivantes représentent les boîtes de dialogue initiales des deux assistants.

FIGURE 15–20 Boîte de dialogue d'exportation des données dans le gestionnaire DHCP

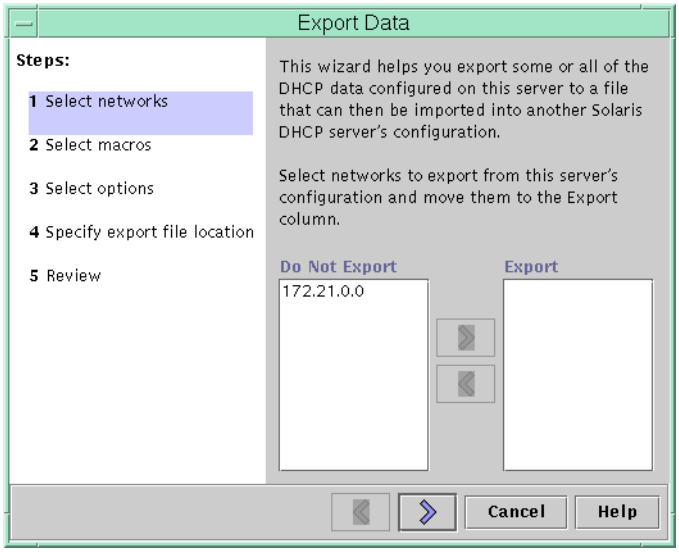
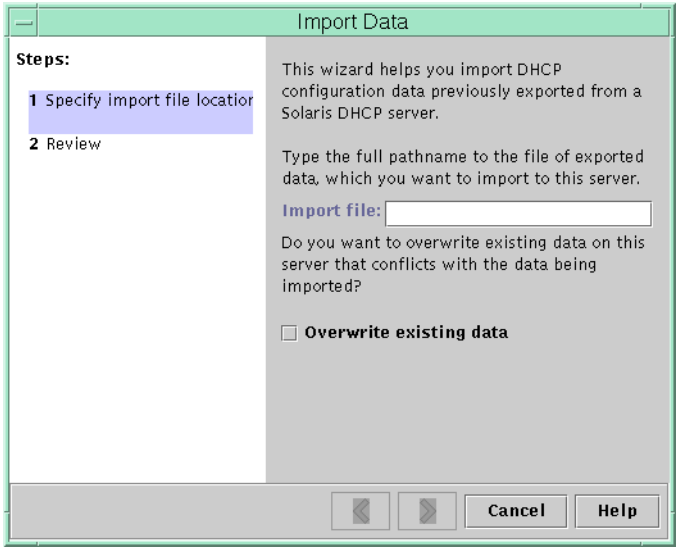


FIGURE 15–21 Boîte de dialogue d'importation des données dans le gestionnaire DHCP



▼ Exportation des données à partir d'un serveur DHCP (gestionnaire DHCP)

1 **Lancez le gestionnaire DHCP sur le serveur source (c'est-à-dire celui à partir duquel vous souhaitez déplacer ou copier des données).**

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2 **Choisissez Export Data dans le menu Service.**

L'assistant d'exportation des données illustré à la Figure 15–20 s'ouvre.

3 **Répondez aux invites de l'assistant.**

En cas de problème, cliquez sur le bouton d'aide pour obtenir plus de précisions sur les invites.

4 **Transférez le fichier d'exportation vers un système de fichiers accessible au serveur DHCP chargé de l'importation des données.**

Voir aussi Importez les données en procédant comme indiqué à la section "Importation des données sur un serveur DHCP (gestionnaire DHCP)" à la page 431.

▼ Exportation des données à partir d'un serveur DHCP (`dhcpconfig -X`)

1 **Connectez-vous au serveur à partir duquel vous souhaitez déplacer ou copier des données.**

2 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 **Exportez les données.**

Vous pouvez exporter l'intégralité ou certaines parties des données DHCP.

- **Pour exporter des adresses, macros et options spécifiques, entrez une commande sous le format suivant :**

```
# dhcpconfig -X filename -a network-addresses -m macros -o options
```

nom-du-fichier est le nom de chemin complet du fichier dans lequel vous souhaitez stocker les données exportées compressées. Vous spécifiez les adresses réseau, les macros DHCP et les options DHCP à exporter dans des listes séparées par des virgules. L'exemple suivant montre comment exporter des adresses réseau, macros et options spécifiques.

```
# dhcpconfig -X /var/dhcp/0dhcp1065_data \ -a 10.63.0.0,10.62.0.0 \ -m 10.63.0.0,10
```

- **Pour exporter l'intégralité des données DHCP, entrez une commande contenant le mot-clé `ALL`.**

  ```
  # dhcpconfig -X filename -a ALL -m ALL -o ALL
  ```

  nom-du-fichier est le nom de chemin complet du fichier dans lequel vous souhaitez stocker les données exportées compressées. Le mot-clé `ALL` peut être associé aux options de la commande afin d'exporter l'ensemble des adresses réseau, macros ou options. L'exemple suivant montre comment utiliser le mot-clé `ALL`.

  ```
  # dhcpconfig -X /var/dhcp/dhcp1065_data -a ALL -m ALL -o ALL
  ```

Astuce – Pour éviter d'exporter un type de données, il suffit d'omettre l'option de commande `dhcpconfig` correspondant à ce type de données. Si vous omettez, par exemple, de spécifier l'option `-m`, aucune macro DHCP ne sera exportée.

Pour plus d'informations au sujet de la commande `dhcpconfig`, reportez-vous à la page de manuel `dhcpconfig(1M)`.

4 **Déplacez le fichier d'exportation vers un emplacement accessible au serveur DHCP chargé de l'importation des données.**

Voir aussi Importez les données en procédant comme indiqué à la section "Importation des données sur un serveur DHCP (`dhcpconfig -I`)" à la page 432.

▼ Importation des données sur un serveur DHCP (gestionnaire DHCP)

1 **Lancez le gestionnaire DHCP sur le serveur vers lequel vous souhaitez transférer les données exportées depuis un serveur DHCP.**

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2 **Choisissez Import Data dans le menu Service.**

L'assistant d'importation des données illustré à la Figure 15–21 s'ouvre.

3 **Répondez aux invites de l'assistant.**

En cas de problème, cliquez sur le bouton d'aide pour obtenir plus de précisions sur les invites.

4 **Apportez les modifications voulues aux données importées, si cela est nécessaire.**

Voir "Modification des données DHCP importées (gestionnaire DHCP)" à la page 432

▼ Importation des données sur un serveur DHCP (`dhcpconfig -I`)

1 **Connectez-vous au serveur sur lequel vous souhaitez importer les données.**

2 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 **Importez les données en entrant une commande sous le format suivant :**

```
# dhcpconfig -I filename
```

nom-du-fichier désigne le fichier contenant les données précédemment exportées.

4 **Apportez les modifications voulues aux données importées, si cela est nécessaire.**

Voir "Modification des données DHCP importées (`pntadm`, `dhtadm`)" à la page 433.

▼ Modification des données DHCP importées (gestionnaire DHCP)

1 **Lancez le gestionnaire DHCP depuis le serveur sur lequel vous avez importé des données.**

Pour plus d'informations au sujet du gestionnaire DHCP, reportez-vous à la section "Démarrage et arrêt du gestionnaire DHCP" à la page 354.

2. **Examinez les données importées afin d'identifier les informations spécifiques au réseau nécessitant des modifications.**

   Si vous avez transféré des réseaux, par exemple, vous devez ouvrir l'onglet Addresses et changer le serveur propriétaire des adresses dans les réseaux importés. Vous devrez éventuellement accéder à l'onglet Macros afin de spécifier les noms de domaines corrects pour NIS, NIS+ ou DNS dans certaines macros.

3. **Ouvrez l'onglet Addresses et sélectionnez le réseau que vous avez importé.**

4. **Pour sélectionner toutes les adresses, cliquez sur la première adresse, maintenez la touche Maj enfoncée, puis cliquez sur la dernière adresse.**

5. **Choisissez Properties dans le menu Edit.**

   Cela a pour effet d'ouvrir la boîte de dialogue de modification de plusieurs adresses.

6. **À l'invite du serveur de gestion, sélectionnez le nom du nouveau serveur.**

7. **Lorsque vous êtes invité à spécifier une macro de configuration, sélectionnez celle qui doit être appliquée à tous les clients de ce réseau, puis cliquez sur OK.**

8. **Ouvrez l'onglet Macros.**

9. **Servez-vous du bouton Find afin de localiser les options pour lesquelles il peut être nécessaire de changer les valeurs.**

   Le bouton Find figure en bas de la fenêtre.

   `DNSdmain`, `DNSserv` , `NISservs`, `NIS+serv` et `NISdmain` sont des exemples d'options susceptibles d'être modifiées sur le nouveau serveur.

10. **Changez les options dans les macros appropriées.**

    Pour plus d'informations sur la modification des options, reportez-vous à la section "Modification des propriétés des options DHCP (gestionnaire DHCP)" à la page 418.

▼ Modification des données DHCP importées (`pntadm`, `dhtadm`)

1. **Connectez-vous au serveur sur lequel vous avez importé des données.**

2. **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil de gestion DHCP.**

   Pour plus d'informations au sujet de ce profil, reportez-vous à la section "Configuration de l'accès utilisateur aux commandes DHCP" à la page 355.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 **Examinez les tables de réseau pour identifier les données qu'il convient de modifier.**

Si vous avez transféré des réseaux, par exemple, utilisez la commande `pntadm -P` *adresse-réseau* pour afficher les tables correspondant aux réseaux déplacés.

4 **Modifiez les données des adresses IP à l'aide de la commande `pntadm`.**

Vous devrez éventuellement changer le serveur propriétaire et la macro de configuration pour les adresses importées. Pour changer, par exemple, le serveur propriétaire (`10.60.3.4`) et la macro (`dhcpsrv-1060`) de l'adresse `10.63.0.2`, utilisez la commande suivante :

```
pntadm -M 10.63.0.2 -s 10.60.3.4 -m dhcpsrv-1060 10.60.0.0
```

Si vous avez un grand nombre d'adresses, il est recommandé de créer un fichier script regroupant toutes les commandes permettant de modifier chaque adresse. Exécutez le script à l'aide de la commande `pntadm -B` laquelle exécute `pntadm` en mode de traitement par lots. Voir la page de manuel `pntadm(1M)`.

5 **Examinez les macros `dhcptab` pour identifier les options nécessitant des changements de valeurs.**

Utilisez la commande `dhtadm -P` pour afficher l'intégralité de la table `dhcptab` à l'écran. Exécutez `grep` ou un autre outil pour rechercher les options ou les valeurs susceptibles d'être modifiées.

6 **Modifiez les options dans les macros (si besoin est) à l'aide de la commande `dhtadm -M`.**

Vous devrez, par exemple, changer certaines macros afin de spécifier les noms de domaines et les serveurs appropriés pour NIS, NIS+ ou DNS. La commande suivante permet, par exemple, de modifier les valeurs de `DNSdmain` et `DNSserv` dans la macro `mymacro` :

```
dhtadm -M -m mymacro -e 'DNSserv=dnssrv2:DNSdmain=example.net' -g
```

◆ ◆ ◆ CHAPITRE 16

Configuration et administration du client DHCP

Ce chapitre traite du client DHCP (Dynamic Host Configuration Protocol) faisant partie d'Oracle Solaris. Il décrit le mode de fonctionnement des protocoles DHCPv4 et DHCPv6 du client et explique comment vous pouvez modifier le comportement du client.

L'un de ces protocoles, à savoir le protocole DHCPv4, fait depuis longtemps partie d'Oracle Solaris. Il permet aux serveurs DHCP de transmettre des paramètres de configuration tels que les adresses réseau IPv4 aux nœuds IPv4.

L'autre protocole, DHCPv6, joue le même rôle auprès des serveurs DHCP en leur donnant la possibilité de communiquer des paramètres de configuration (adresses réseau IPv6, par exemple) aux nœuds IPv6. DHCPv6 est la contrepartie sans état à la spécification « Autoconfiguration d'adresse sans état IPv6 » (RFC 2462). Ce protocole peut être utilisé indépendamment du mode sans état ou lui être associé afin d'obtenir des données de configuration.

Le présent chapitre contient les informations suivantes :

À propos du client DHCP

Le client DHCP correspond au démon `dhcpagent` faisant partie d'Oracle Solaris. Lorsque vous installez Oracle Solaris, vous êtes invité à configurer les interfaces réseau par le biais du service DHCP. Si vous choisissez d'utiliser le protocole DHCPv4, ce dernier est activé sur votre système pendant l'installation d'Oracle Solaris. Il n'existe aucune option spécifique au protocole DHCPv6 à appliquer lors de l'installation. Et qu'en est-il si IPv6 est activé ? DHCPv6 est également activé sur un réseau local compatible avec DHCPv6.

Vous ne devez effectuer aucune autre action sur le client Oracle Solaris pour utiliser le protocole DHCP. La configuration du serveur DHCP détermine les informations communiquées aux systèmes clients DHCP faisant appel au service DHCP.

Si un système client exécute déjà Oracle Solaris sans le service DHCP, vous devez le reconfigurer pour pouvoir utiliser le service DHCP. Vous pouvez également reconfigurer un système client DHCP de façon à ce qu'il cesse d'utiliser le protocole DHCP et qu'il exploite les informations de réseau statiques que vous fournissez. Pour plus d'informations, reportez-vous à la section “Activation et désactivation d'un client DHCP ” à la page 443.

Serveur DHCPv6

Aucun serveur DHCPv6 n'est disponible par le biais de Sun Microsystems pour Oracle Solaris. Les serveurs proposés par des tiers sont compatibles avec DHCPv6 de Sun. Si le réseau comporte un serveur DHCPv6, le client DHCPv6 de Sun l'utilise.

Pour plus d'informations sur le serveur Sun DHCPv4, reportez-vous à la section “Le serveur DHCP” à la page 310.

Différences entre DHCPv4 et DHCPv6

Les deux principales différences entre DHCPv4 et DHCPv6 concernent les aspects suivants :

- **Modèle administratif**
  - DHCPv4–L'administrateur active DHCP pour chaque interface. L'administration se fait sur la base d'une interface logique.
  - DHCPv6–Aucune configuration explicite n'est utile. Ce protocole est activé sur une interface physique donnée.
- **Détails du protocole**
  - DHCPv4–Le serveur DHCP fournit le masque de sous-réseau pour chaque adresse. Une option de nom d'hôte définit le nom du nœud à l'échelle du système.
  - DHCPv6–Le masque de sous-réseau est fourni par les publications du routeur, et non par le serveur DHCPv6. Il n'existe pas d'option de nom d'hôte DHCPv6.

Modèle administratif

DHCPv4 exige une configuration explicite du client. Vous devez configurer le système DHCPv4 pour effectuer une procédure d'adressage chaque fois que cela est nécessaire, soit lors de l'installation initiale du système ou soit de façon dynamique par le biais des options `ifconfig(1M)`

DHCPv6 ne nécessite pas de configuration explicite du client. DHCP est une caractéristique inhérente du réseau. Le signal permettant d'utiliser ce protocole est acheminé dans les messages des publications du routeur à partir des routeurs locaux. Le client DHCP crée et détruit automatiquement les interfaces logiques chaque fois que cela est nécessaire.

Le mécanisme DHCPv6 est très similaire, d'un point de vue administratif, à la configuration d'adresse sans état (automatique) IPv6 existante. Dans le cas d'une configuration d'adresse sans état, il est nécessaire d'appliquer un indicateur au routeur local afin d'indiquer que, pour un nombre donné de préfixes, chaque client est tenu de configurer automatiquement une adresse par lui-même en utilisant le préfixe publié plus un jeton d'interface local ou un nombre aléatoire. En ce qui concerne DHCPv6, les mêmes préfixes sont exigés mais les adresses sont acquises et gérées via un serveur DHCPv6 au lieu d'être assignées de façon aléatoire.

Adresse MAC et ID de client

DHCPv4 utilise l'adresse MAC et un ID de client facultatif pour identifier le client dans le but d'assigner une adresse. Chaque fois que le même client se connecte au réseau, il obtient la même adresse dans la mesure du possible.

DHCPv6 procède essentiellement de la même manière, mais rend l'ID de client obligatoire et impose une structure. L'ID de client dans DHCPv6 se compose de deux parties : Un identificateur unique DHCP (DUID) et un identificateur d'association d'identité (IAID). Le DUID identifie le **système** client (et non pas seulement une interface, comme dans DHCPv4), et l'IAID identifie l'interface sur ce système.

Comme indiqué dans le document RFC 3315, une association d'identité est le moyen utilisé par un serveur et un client pour identifier, regrouper et gérer un ensemble d'adresses IPv6 liées. Le client doit lier au moins une association d'identité (IA) distincte à chacune de ses interfaces réseau. Il utilise ensuite les IA assignées pour obtenir des informations de configuration d'un serveur pour cette interface. Pour plus d'informations sur les IA, reportez-vous à la section suivante (Détails du protocole).

Il est possible également d'associer DUID+IAID avec DHCPv4. Vous pouvez concaténer ces identificateurs sans ambiguïté pour vous en servir comme ID de client. Pour des raisons de compatibilité, cela ne s'applique pas aux interfaces IPv4 standard. En revanche, pour les interfaces logiques (`hme0:1`), DUID+IAID est utilisé si aucun ID de client n'est configuré.

À la différence d'IPv4 DHCP, DHCPv6 n'offre pas d'option « nom de client ». Il n'y a donc aucun moyen de nommer vos systèmes en les basant uniquement sur DHCPv6. Si vous avez besoin de connaître le nom DNS associé à une adresse fournie par DHCPv6, utilisez la résolution inverse

DNS (requête adresse vers nom via la fonction `getaddrinfo(3SOCKET)`) pour obtenir le nom correspondant. Si vous utilisez uniquement DHCPv6 et souhaitez attribuer un nom spécifique à un nœud, vous devez alors définir `/etc/nodename` sur votre système.

Détails du protocole

Avec DHCPv4, le serveur DHCP fournit le masque du sous-réseau à associer à l'adresse assignée. Avec DHCPv6, le masque du sous-réseau (appelé aussi « longueur du préfixe ») est attribué par les publications du routeur et n'est pas géré par le serveur DHCP.

DHCPv4 dispose d'une option Hostname prévue pour définir le nom du nœud à l'échelle du système. DHCPv6 ne propose pas ce type d'option.

Pour configurer un ID de client pour DHCPv6, vous devez spécifier un DUID au lieu de permettre au système d'en choisir un automatiquement. Vous pouvez le faire de façon globale pour le démon ou procéder interface par interface. Pour définir le DUID global, respectez le format suivant (notez la présence du point initial) :

`.v6.CLIENT_ID=`*DUID*

Pour configurer une interface de façon à utiliser un DUID précis (et donner l'impression que le système est constitué de multiples clients indépendants pour le serveur DHCPv6), tapez la commande suivante :

`hme0.v6.CLIENT ID=`*DUID*

À chaque association d'identité (IA) correspond un type d'adresse. Une association d'identité pour des adresses temporaires (IA_TA) contient, par exemple, des adresses provisoires, alors qu'une association d'identité pour des adresses non temporaires (IA_NA) dispose d'adresses allouées de façon permanente. La version de DHCPv6 décrite dans ce manuel offre uniquement des associations IA_NA.

Oracle Solaris assigne sur demande une IAID à chaque interface. Cette dernière est stockée dans un fichier à l'intérieur du système de fichiers racine de façon à rester la même pendant tout le cycle de vie de la machine.

Interfaces logiques

Au niveau du client DHCPv4, chaque interface logique est considérée comme indépendante et comme une unité d'administration. Outre l'interface logique numéro zéro (laquelle adopte par défaut l'adresse MAC de l'interface comme identificateur), l'utilisateur a la possibilité de configurer des interfaces logiques spécifiques afin d'exécuter DHCP en spécifiant un CLIENT_ID dans le fichier de configuration `dhcpagent`. Exemple :

```
hme0:1.CLIENT_ID=orangutan
```

DHCPv6 ne procède pas de la même manière. L'interface logique numéro zéro sur une interface IPv6, à la différence d'IPv4, est toujours une adresse lien-local. une adresse lien-local sert à assigner automatiquement une adresse IP à un périphérique sur un réseau IP lorsque aucune autre méthode d'affectation n'est disponible, comme par exemple un serveur DHCP. L'interface logique numéro zéro ne peut pas être placée sous le contrôle de DHCP. Aussi, même si DHCPv6 est exécuté sur l'interface logique numéro zéro (appelée également interface « physique »), il alloue les adresses uniquement aux interfaces logiques n'ayant pas le numéro zéro.

En réponse à une demande du client DHCPv6, le serveur DHCPv6 renvoie une liste d'adresses à configurer par le client.

Négociation d'options

Dans DHCPv6, vous disposez d'une fonction de demande d'option qui donne une indication au serveur sur les préférences d'affichage du client. Si toutes les options possibles ont été transmises du serveur au client, il est possible qu'une partie des informations doive être abandonnée en chemin. Le serveur peut utiliser l'indication pour sélectionner les options à inclure dans la réponse. Il peut également l'ignorer et choisir d'inclure d'autres éléments. Par exemple, sur Oracle Solaris, les options de préférence peuvent contenir le domaine d'adresse DNS ou NIS d'Oracle Solaris, mais ne contiendront probablement pas le serveur NetBIOS.

Le même type d'indication est fourni pour DHCPv4, mais sans la fonction de demande d'option spéciale. Au lieu de cela, DHCPv4 utilise la liste `PARAM_REQUEST_LIST` dans `/etc/default/dhcpagent`.

Syntaxe de configuration

Configurez le client DHCPv6 de la même manière que le client DHCPv4 existant, à l'aide de `/etc/default/dhcpagent`.

La syntaxe inclut en plus le marqueur ".v6", inséré entre le nom de l'interface (le cas échéant) et le paramètre à configurer. Par exemple, la liste des demandes d'option IPv4 globale est configurée comme suit :

```
PARAM_REQUEST_LIST=1,3,6,12,15,28,43
```

Il est possible de configurer une interface individuelle afin d'omettre l'option de nom d'hôte comme suit :

```
hme0.PARAM_REQUEST_LIST=1,3,6,15,28,43
```

Pour définir une liste de demandes globale pour DHCPv6, n'oubliez pas le point initial :

```
.v6.PARAM_REQUEST_LIST=23,24
```

Suivez cet exemple pour configurer une interface individuelle :

```
hme0.v6.PARAM_REQUEST_LIST=21,22,23,24
```

À titre de référence, voici à quoi ressemble un fichier `/etc/default/dhcpagent` pour la configuration DHCPv6 :

```
# 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
```

Démarrage du client DHCP

Dans la plupart des cas, vous n'avez pas à intervenir pour lancer le client DHCPv6. Le démon `in.ndpd` démarre automatiquement DHCPv6 lorsque cela est nécessaire. Il peut être nécessaire de définir `/etc/hostname6.$IFNAME` pour configurer une interface afin de la monter pour IPv6 au démarrage. Le programme d'installation s'en charge, cependant, si vous activez IPv6 sur votre système au moment de l'installation.

Cependant, pour le protocole DHCPv4, vous devez demander le démarrage du client, si cela n'a pas été fait lors de l'installation d'Oracle Solaris. Reportez-vous à la section “Activation du client DHCP ” à la page 444.

Le démon `dhcpagent` obtient les informations de configuration nécessaires aux autres processus impliqués dans l'initialisation du système. C'est pour cette raison que les scripts de démarrage du système lancent `dhcpagent` au tout début du processus d'initialisation et attendent l'arrivée des informations de configuration du réseau provenant du serveur DHCP.

Bien que la procédure par défaut consiste à exécuter DHCPv6, vous pouvez en décider autrement. Vous pouvez arrêter DHCPv6 à l'aide de la commande `ifconfig`. Rien ne vous empêche également de désactiver DHCPv6 pour éviter son lancement au redémarrage. Il suffit pour cela de modifier le fichier `/etc/inet/ndpd.conf`.

L'exemple suivant montre comment arrêter immédiatement DHCPv6 sur l'interface appelée `hme0`.

```
ex# echo ifdefault StatefulAddrConf false >> /etc/inet/ndpd.conf
ex# pkill -HUP -x in.ndpd
ex# ifconfig hme0 inet6 dhcp release
```

La présence du fichier `/etc/dhcp.`*interface* (par exemple, `/etc/dhcp.ce0` sur un système Sun Fire 880) oblige les scripts de démarrage à utiliser DHCPv4 sur l'interface spécifiée. Dès qu'ils trouvent un fichier `dhcp.`*interface*, les scripts de démarrage exécutent `dhcpagent`.

Après le démarrage, `dhcpagent` attend de recevoir des instructions pour configurer une interface réseau. Les scripts de démarrage exécutent la commande `ifconfig` *interface* `dhcp start`, qui donne l'instruction à `dhcpagent` de démarrer DHCPv4 comme indiqué à la section "Mode de fonctionnement du protocole DHCP" à la page 307. Si le fichier `dhcp.`*interface* contient des commandes, celles-ci sont ajoutées à l'option `dhcp start` de la commande `ifconfig`. Pour plus d'informations sur les options utilisées avec la commande `ifconfig` *interface* `dhcp`, reportez-vous à la page de manuel `ifconfig(1M)`.

Communication DHCPv6

À la différence de DHCPv4, lequel est appelé par configuration manuelle, DHCPv6 est exécuté par les publications du routeur (RAs). Selon le mode de configuration du routeur, le système appelle automatiquement DHCPv6 au niveau de l'interface sur laquelle le message Router Advertisement a été reçu et utilise DHCP pour obtenir une adresse et d'autres paramètres, ou demande uniquement les données autres que l'adresse (serveurs DNS, par exemple) avec DHCPv6.

Le démon `in.ndpd` réceptionne le message des publications du routeur. Il effectue cette opération de façon automatique sur toutes les interfaces montées pour IPv6 sur le système. Lorsque `in.ndpd` découvre un RA exigeant l'exécution de DHCPv6, il fait appel à DHCPv6.

Pour éviter que `in.ndpd` ne démarre DHCPv6, il suffit de modifier le contenu du fichier `/etc/inet/ndpd.conf`.

Vous pouvez également arrêter DHCPv6 en utilisant l'une des versions suivantes de la commande `ifconfig` :

```
ifconfig <interface> inet6 dhcp drop
```

Ou :

```
ifconfig <interface> inet6 dhcp release
```

Gestion des données de configuration réseau par les protocoles client DHCP

Les protocoles client DHCPv4 et DHCPv6 procèdent de différentes manières pour gérer les données de configuration réseau. Avec DHCPv4, la négociation porte sur le bail d'une seule adresse et de quelques options supplémentaires. Avec DHCPv6, la négociation concerne un lot d'adresses et un ensemble d'options.

Pour plus d'informations sur l'interaction entre le client DHCPv4 et le serveur, reportez-vous au Chapitre 12, "À propos de DHCP (présentation)".

Traitement des données de configuration réseau par le client DHCPv4

Après avoir obtenu un paquet de données du serveur DHCP, `dhcpagent` se charge de configurer l'interface réseau et d'afficher l'interface. Le démon contrôle l'interface pendant toute la durée du bail de l'adresse IP et gère les données de configuration dans une table interne. Les scripts de démarrage du système utilisent la commande `dhcpinfo` pour extraire les valeurs des options de configuration à partir de la table interne. Les valeurs servent à configurer le système et lui permettent de communiquer sur le réseau.

Le démon `dhcpagent` attend de façon passive pendant un laps de temps qui équivaut généralement à la moitié de la durée du bail. Il envoie ensuite une demande de prolongement du bail à un serveur DHCP. Si le système signale à `dhcpagent` que l'interface est arrêtée ou que l'adresse IP a changé, le démon ne prend pas le contrôle de l'interface tant qu'il n'en reçoit pas l'instruction de la commande `ifconfig`. Si `dhcpagent` constate que l'interface fonctionne et que l'adresse n'a pas changé, le démon demande un renouvellement de bail au serveur. Si le renouvellement n'est pas possible, `dhcpagent` arrête l'interface à la fin du bail.

Chaque fois que `dhcpagent` effectue une action ayant trait au bail, le démon recherche un fichier exécutable appelé `/etc/dhcp/eventhook`. S'il trouve un fichier exécutable ayant ce nom, `dhcpagent` lance ce fichier. Pour plus d'informations sur l'utilisation d'un fichier exécutable d'événement, reportez-vous à la section "Scripts d'événement client DHCP" à la page 455.

Traitement des données de configuration réseau par le client DHCPv6

La communication DHCPv6 entre le client et le serveur commence par l'envoi d'un message de sollicitation par le client qui lui permet de localiser les serveurs. En guise de réponse, tous les serveurs disponibles pour le service DHCP envoient un message de publication. Le message du serveur contient plusieurs enregistrements IA_NA ainsi que d'autres options (telles que les adresses serveur DNS) susceptibles d'être fournies par le serveur.

Un client peut demander des adresses particulières (et même un grand nombre) en définissant ses propres enregistrements IA_NA/IAADDR dans son message de requête. Cela est généralement le cas lorsqu'il possède d'anciennes adresses enregistrées et qu'il souhaite obtenir les mêmes du serveur, dans la mesure du possible. Quel que soit le comportement du client (même s'il ne demande aucune adresse), le serveur peut fournir un nombre quelconque d'adresses au client lors d'une même transaction DHCPv6.

Voici comme se déroule le dialogue entre les clients et les serveurs.

- Un client envoie un message de sollicitation pour localiser les serveurs.
- Les serveurs envoient un message de publication pour signaler qu'ils se mettent à la disposition du service DHCP.
- Un client envoie un message de requête pour demander des paramètres de configuration, ainsi que des adresses IP, aux serveurs possédant les valeurs de préférence les plus élevées. Les valeurs de préférence sont définies par l'administrateur et vont de 0 à 255.

- Le serveur envoie un message de réponse dans lequel figurent les baux des adresses et les données de configuration.

Si la valeur de préférence dans le message de publication équivaut à 255, le client DHCPv6 sélectionne immédiatement ce serveur. Si le serveur privilégié ne répond pas ou ne parvient pas à adresser un message en réponse au message de requête, le client continue de rechercher des serveurs (en fonction de l'ordre de préférence) jusqu'à ce qu'il ne reste plus de messages de publication. Arrivé à ce stade, le client recommence la procédure en envoyant à nouveau des messages de sollicitation.

Le serveur choisi envoie un message de réponse contenant les adresses assignées et les paramètres de configuration en réponse à un message de sollicitation ou de requête.

Arrêt du client DHCP

Lors de la mise à l'arrêt, le client envoie un message de libération au serveur ayant alloué des adresses au client pour lui indiquer qu'il n'utilisera plus une ou plusieurs adresses assignées. Lors de l'arrêt normal du système client DHCPv4, `dhcpagent` écrit les données de configuration actuelles dans le fichier `/etc/dhcp/` *interface*`.dhc` ou dans le fichier `/etc/dhcp/` *interface*`.dh6` pour DHCPv6. Par défaut, le bail est enregistré au lieu d'être libéré. Le serveur DHCP ignore donc si l'adresse IP est en cours d'utilisation, ce qui permet au client de récupérer facilement l'adresse lors du prochain démarrage. L'action par défaut est la même que celle initiée par la commande `ifconfig <interface> dhcp drop`.

Si le bail dans ce fichier est encore valide au redémarrage du système, `dhcpagent` envoie une requête abrégée afin d'utiliser la même adresse IP et les mêmes données de configuration. Dans le cas de DHCPv4, il s'agit du message de requête. Dans le cas de DHCPv6, Il s'agit du message de confirmation.

Si le serveur DHCP autorise cette requête, `dhcpagent` peut exploiter les informations qu'il a inscrites sur disque lors de l'arrêt du système. Dans le cas contraire, `dhcpagent` lance la séquence du protocole DHCP décrite à la section "Mode de fonctionnement du protocole DHCP" à la page 307. Le client est en mesure ainsi d'obtenir de nouvelles données de configuration réseau.

Activation et désactivation d'un client DHCP

Pour activer le client DHCP sur un système qui exécute déjà Oracle Solaris sans le service DHCP, vous devez d'abord annuler la configuration du système. Au démarrage du système, vous devez ensuite exécuter plusieurs commandes afin de configurer le système et d'activer le client DHCP.

Remarque – Dans de nombreux déploiements, il est d'usage de configurer des parties vitales de l'infrastructure en fonction d'adresses IP statiques, au lieu de faire appel au service DHCP. Les raisons pour lesquelles il est préférable de désigner comme clients des périphériques du réseau (routeurs et certains serveurs, par exemple) sortent du cadre de ce manuel.

▼ Activation du client DHCP

Cette procédure est uniquement nécessaire si le protocole DHCPv4 n'a pas été activé lors de l'installation d'Oracle Solaris. Elle ne présente aucun intérêt pour DHCPv6.

1. **Connectez-vous au système client en tant que superutilisateur.**

2. **Si ce système fait appel à la préconfiguration plutôt qu'à la configuration interactive, modifiez le fichier `sysidcfg`. Ajoutez la sous-clé `dhcp` au mot-clé `network_interface` dans le fichier `sysidcfg`.**

   Par exemple, `network_interface=hme0 {dhcp}`. Pour plus d'informations, reportez-vous à la page de manuel `sysidcfg(4)`.

3. **Annulez la configuration et mettez le système hors tension.**

   ```
   # sys-unconfig
   ```

   Reportez-vous à la page de manuel `sys-unconfig(1M)` pour plus d'informations sur les données de configuration qui sont supprimées par cette commande.

4. **Réinitialisez le système après la mise hors tension.**

   Si le système recourt à la préconfiguration, la sous-clé `dhcp` du fichier `sysidcfg` configure le système pour utiliser le client DHCP au redémarrage du système.

   Dans le cas contraire, vous êtes invité à spécifier les informations de la configuration système par les programmes `sysidtool` au redémarrage du système. Pour plus d'informations, reportez-vous à la page de manuel `sysidtool(1M)`.

5. **Lorsque vous êtes invité à utiliser DHCP pour configurer les interfaces réseau, choisissez Oui.**

▼ Désactivation d'un client DHCP

1. **Connectez-vous au système client en tant que superutilisateur.**

2. **Si vous avez utilisé un fichier `sysidcfg` pour préconfigurer le système, supprimez la sous-clé `dhcp` du mot-clé `network_interface`.**

3 **Annulez la configuration et mettez le système hors tension.**

```
# sys-unconfig
```

Reportez-vous à la page de manuel `sys-unconfig(1M)` pour plus d'informations sur les données de configuration qui sont supprimées par cette commande.

4 **Réinitialisez le système après la mise hors tension.**

Si le système fait appel à la préconfiguration, vous n'êtes pas invité à spécifier les informations de configuration et le client DHCP n'est pas configuré.

Dans le cas contraire, vous êtes invité à spécifier les informations de la configuration système par les programmes `sysidtool` au redémarrage du système. Pour plus d'informations, reportez-vous à la page de manuel `sysidtool(1M)`.

5 **Lorsque vous êtes invité à utiliser DHCP pour configurer les interfaces réseau, choisissez Non.**

Administration du client DHCP

Le logiciel client DHCP n'exige pas d'opérations d'administration dans des conditions normales d'utilisation. Le démon `dhcpagent` démarre automatiquement au redémarrage du système, rénégocie les baux et s'interrompt à l'arrêt du système. Vous ne pouvez pas lancer et interrompre manuellement le démon `dhcpagent`. En revanche, en tant que superutilisateur sur le système client, vous pouvez utiliser la commande `ifconfig` pour changer la façon dont le démon `dhcpagent` gère l'interface réseau, si nécessaire.

Options de la commande `ifconfig` utilisées par le client DHCP

Cette section récapitule les options de commande décrites dans la page de manuel `ifconfig(1M)` La version DHCPv4 de ces commandes se différencie de la version DHCPv6 simplement par le mot-clé « inet6 ». Insérez le mot-clé « inet6 » dans la version DHCPv6, mais omettez-le lorsque vous exécutez DHCPv4.

La commande `ifconfig` vous permet de réaliser les opérations suivantes :

- **Exécuter le client DHCP** – La commande `ifconfig` *interface* `[inet6] dhcp start` lance l'interaction entre `dhcpagent` et le serveur DHCP en vue d'obtenir l'adresse IP et un nouveau jeu d'options de configuration. L'intérêt de cette commande est évident lorsque vous modifiez des informations que vous souhaitez appliquer immédiatement à un client, par exemple lorsque vous ajoutez des adresses IP ou changer le masque de sous-réseau.
- **Demander uniquement des informations de configuration réseau** – La commande `ifconfig` *interface* `[inet6] dhcp inform` fait en sorte que `dhcpagent` émette une demande en vue d'obtenir les paramètres de configuration réseau, adresse IP mise à part. Cette

commande est pratique lorsque l'interface réseau possède une adresse IP statique, mais que le système client exige la mise à jour des options réseau. Vous ferez appel à cette commande si vous n'avez pas besoin de DHCP pour gérer les adresses IP, mais que vous l'utilisez pour configurer les hôtes sur le réseau.

- **Demander une extension de bail** – La commande `ifconfig` *interface* `[inet6] dhcp extendipadm refresh-addr` *dhcp-addrobj* provoque l'émission d'une demande de renouvellement du bail par `dhcpagent`. Le client requiert automatiquement le renouvellement des baux. Cependant, vous pouvez faire appel à cette commande si vous modifiez la durée du bail et souhaiter qu'elle soit appliquée aux clients sans attendre le renouvellement de bail suivant.
- **Libérer l'adresse IP** – La commande `ifconfig` *interface* `[inet6] dhcp release` demande à `dhcpagent` d'abandonner l'adresse IP utilisée par l'interface réseau. La libération de l'adresse IP a automatiquement lieu à l'expiration du bail. Il est possible d'émettre cette commande depuis un ordinateur portable, par exemple, lorsque vous quittez un réseau et comptez lancer le système sur un nouveau réseau. Voir aussi la propriété `RELEASE_ON_SIGTERM` du fichier de configuration `/etc/default/dhcpagent`.
- **Abandonner l'adresse IP** – La commande `ifconfig` *interface* `[inet6] dhcp drop` demande à `dhcpagent` d'arrêter l'interface réseau sans informer le serveur DHCP et de mettre en cache le bail dans le système de fichiers. Cette commande permet au client d'utiliser la même adresse IP sans devoir redémarrer.
- **Effectuer un test ping de l'interface réseau** – La commande `ifconfig` *interface* `[inet6] dhcp ping` vous permet de vérifier si l'interface est sous le contrôle de DHCP.
- **Afficher l'état de configuration DHCP de l'interface réseau** – La commande `ifconfig` *interface* `[inet6] dhcp status` affiche l'état actuel du client DHCP. L'affichage indique :
  - si une adresse IP est liée au client ;
  - le nombre de requêtes envoyées, reçues et refusées ;
  - si cette interface est l'interface principale ;
  - la date d'obtention des baux, leur date d'expiration et la date à laquelle leur renouvellement est programmé.

  Exemple :

```
# ifconfig hme0 dhcp status
Interface  State         Sent  Recv  Declined  Flags
hme0       BOUND            1     1         0   [PRIMARY]
(Began,Expires,Renew)=(08/16/2005 15:27, 08/18/2005 13:31, 08/17/2005 15:24)

# ifconfig hme0 inet6 dhcp status
Interface  State         Sent  Recv  Declined  Flags
hme0       BOUND            1     0         0   [PRIMARY]
(Began,Expires,Renew)=(11/22/2006 20:39, 11/22/2006 20:41, 11/22/2006 20:40)
```

Définition des paramètres de configuration du client DHCP

Le fichier `/etc/default/dhcpagent` qui se trouve sur le système client contient des paramètres ajustables pour `dhcpagent`. Vous pouvez utiliser un éditeur de texte pour modifier plusieurs paramètres ayant une incidence sur le fonctionnement du client. Le fichier `/etc/default/dhcpagent` est bien documenté, aussi pour plus d'informations, reportez-vous au fichier ainsi qu'à la page du manuel `dhcpagent(1M)`.

Le fichier `/etc/dhcp.`*interface* constitue un autre emplacement dans lequel les paramètres affectant le client DHCP sont définis. Les paramètres spécifiés dans ce fichier sont utilisés par les scripts de démarrage du système avec la commande `ifconfig`. Cette opération a seulement un impact sur DHCPv4, car il n'existe pas d'équivalent pour DHCPv6.

Par défaut, le client DHCP est configuré comme suit :

Pour DHCPv4

- Le système client ne nécessite aucun nom d'hôte particulier.

  Si vous voulez qu'un client porte un nom d'hôte spécifique, reportez-vous à la section "Noms d'hôtes du client DHCPv4" à la page 449.

- Des requêtes par défaut pour le client sont attribuées dans `/etc/default/dhcpagent` et portent sur le serveur DNS, le domaine DNS et l'adresse de diffusion.

  Le fichier des paramètres du client DHCP peut être configuré pour obtenir des options supplémentaires avec le mot-clé `PARAM_REQUEST_LIST` figurant dans le fichier `/etc/default/dhcpagent`. Le serveur DHCP peut être configuré afin de fournir des options qui n'ont pas été demandées de manière spécifique. Pour plus d'informations sur l'utilisation des macros du serveur DHCP afin d'envoyer des informations aux clients, reportez-vous aux sections "À propos des macros DHCP" à la page 318 et "Utilisation des macros DHCP (liste des tâches)" à la page 401.

Pour DHCPv4 et DHCPv6

- Le système client utilise DHCP sur une interface réseau physique.

  Si vous voulez exploiter DHCP sur plusieurs interfaces réseau physiques, reportez-vous à la section "Systèmes clients DHCP avec plusieurs interfaces réseau" à la page 448.

- Le client n'est pas automatiquement configuré en tant que client de service de noms si le client DHCP a été configuré après l'installation d'Oracle Solaris.

  Pour plus d'informations sur l'utilisation des services de noms avec les clients DHCP, reportez-vous à la section "Systèmes clients DHCP et services de noms" à la page 450.

Systèmes clients DHCP avec plusieurs interfaces réseau

Le client DHCP peut gérer simultanément plusieurs interfaces sur un même système. Il peut s'agit d'interfaces physiques comme d'interfaces logiques. Chaque interface possède sa propre adresse IP et sa propre durée de bail. Si plusieurs interfaces réseau sont configurées pour DHCP, le client émet des demandes distinctes pour les configurer. Le client conserve alors un jeu de paramètres de configuration réseau pour chaque interface. Bien que les paramètres soient stockés indépendamment les uns des autres, certains d'entre eux ont un caractère général. Les paramètres globaux s'appliquent à l'ensemble du système plutôt qu'à une interface réseau particulière.

Le nom d'hôte, le nom de domaine NIS et le fuseau horaire sont des exemples de paramètres globaux. Les paramètres globaux ont, en principe, des valeurs différentes pour chaque interface. Cependant, une seule valeur peut être utilisée pour chaque paramètre global associé à chaque système. Pour éviter qu'une requête portant sur un paramètre global ne génère plusieurs réponses, seuls les paramètres de l'interface réseau principale sont pris en compte. Vous avez la possibilité d'insérer le mot `primary` dans le fichier `/etc/dhcp.` *interface* pour l'interface que vous souhaitez traiter comme interface principale. Si vous omettez de spécifier le mot-clé `primary`, c'est la première interface dans l'ordre alphabétique qui est considérée comme interface principale.

Le client DHCP procède de la même manière pour gérer les baux des interfaces logiques et des interfaces physiques, à l'exception de la limitation suivante pour les interfaces logiques :

- Le client DHCP ne gère pas les routes par défaut associées aux interfaces logiques.

  Le noyau Oracle Solaris associe les routes aux interfaces physiques, et non pas aux interfaces logiques. Lors de l'établissement de l'adresse IP d'une interface physique, il est essentiel que les routes par défaut appropriées soient placées dans la table de routage. Si vous avez recours par la suite à DHCP pour configurer une interface logique associée à cette interface physique, les routes nécessaires doivent déjà être en place. L'interface logique utilise les mêmes routes.

  Lors de l'expiration d'un bail sur une interface physique, le client DHCP supprime les routes par défaut associées à l'interface. Lors de l'expiration d'un bail sur une interface logique, le client DHCP n'efface pas les routes par défaut associées à l'interface. L'interface physique associée et les autres interfaces logiques devront éventuellement utiliser les mêmes routes.

  Si vous avez besoin d'ajouter ou de supprimer les routes par défaut associées à une interface sous le contrôle de DHCP, vous pouvez faire appel au mécanisme de script d'événement du client DHCP. Voir "Scripts d'événement client DHCP" à la page 455.

Noms d'hôtes du client DHCPv4

Par défaut, le client DHCPv4 ne fournit pas son propre nom d'hôte, car il s'attend à ce qu'il soit proposé par le serveur DHCP. Le serveur DHCPv4 est configuré par défaut de manière à fournir des noms d'hôtes aux clients DHCPv4. Lorsque vous utilisez le serveur et le client DHCPv4 ensemble, ces comportements par défaut ne posent pas de problème. En revanche, lorsque vous utilisez le client DHCPv4 avec des serveurs DHCP tiers, il est possible que le client ne reçoive pas de nom d'hôte du serveur. Si le client DHCP n'obtient pas de nom d'hôte via DHCP, le système client vérifie s'il n'existe pas un nom pouvant servir de nom d'hôte dans le fichier `/etc/nodename`. Si le fichier est vide, le nom d'hôte prend la valeur `unknown`.

Si le serveur DHCP propose un nom dans l'option DHCP `Hostname`, le client utilise ce nom d'hôte, même si une autre valeur figure dans le fichier `/etc/nodename`. Si vous souhaitez que le client utilise un nom d'hôte spécifique, vous pouvez activer le client de façon à ce qu'il réclame ce nom, comme cela est décrit dans la procédure suivante.

Remarque – La procédure présentée ci-après ne s'applique pas à tous les serveurs DHCP. Elle implique l'envoi d'un nom d'hôte spécifique au serveur DHCP par le client, lequel s'attend en retour à recevoir le même nom.

Le serveur DHCP n'est pas tenu, cependant, de respecter cette demande. C'est d'ailleurs ce qui se produit dans de nombreux cas. Il se contente souvent de renvoyer un autre nom.

▼ Activation d'un client DHCPv4 pour qu'il demande un nom d'hôte spécifique

1. **Sur le système client, modifiez le fichier `/etc/default/dhcpagent` en tant que superutilisateur.**

2. **Recherchez le mot-clé `REQUEST_HOSTNAME` dans le fichier `/etc/default/dhcpagent` et modifiez-le de la façon suivante :**

   ```
   REQUEST_HOSTNAME=yes
   ```

   Si `REQUEST_HOSTNAME` est précédé d'un symbole de commentaire (#), supprimez le symbole #. Si le mot-clé `REQUEST_HOSTNAME` ne figure pas dans le fichier, insérez-le.

3. **Éditez le fichier `/etc/hostname.`*interface* sur le système client en ajoutant la ligne suivante :**

   `inet` *nom-hôte*

   nom-hôte est le nom que le client doit utiliser.

4 **Entrez les commandes suivantes pour que le client effectue une négociation DHCP complète à l'issue du redémarrage :**

```
# ifconfig interface dhcp release
# reboot
```

Les données DHCP mises en mémoire cache sur le client sont supprimées. Le client relance le protocole pour demander de nouvelles données de configuration, ainsi qu'un nouveau nom d'hôte. Le serveur DHCP commence par s'assurer que le nom d'hôte n'est pas utilisé par un autre système sur le réseau. Il attribue ensuite le nom d'hôte au client. S'il est configuré à cet effet, le serveur DHCP peut se charger de mettre à jour les services de noms en fonction du nom d'hôte du client.

Si vous préférez changer le nom d'hôte ultérieurement, répétez l'Étape 3 et l'Étape 4.

Systèmes clients DHCP et services de noms

Les systèmes Oracle Solaris prennent en charge les services de noms suivants : DNS, NIS, NIS+ et un magasin de fichiers local (`/etc/inet/hosts`). Pour être exploitable, chaque service de noms exige un certain niveau de configuration. Le fichier de configuration du commutateur du service de noms (voir `nsswitch.conf(4)`) doit également être configuré correctement pour indiquer les services de noms à utiliser.

Pour qu'un système client DHCP utilise un service de noms, il est indispensable de configurer le système en tant que client du service de noms. Par défaut, sauf si vous en avez décidé autrement lors de l'installation du système, seuls les fichiers locaux sont pris en compte.

Le tableau suivant récapitule les problèmes ayant trait à chaque service de noms et à DHCP. Il propose des liens vers de la documentation de référence contenant des informations utiles sur la configuration des clients pour chaque service de noms.

TABLEAU 16–1 Informations sur la configuration des services de noms pour les systèmes clients DHCP

Service de noms	Informations relatives à la configuration du client

NIS	Si vous utilisez un service DHCP pour envoyer des informations concernant l'installation d'un réseau Oracle Solaris à un système client, vous pouvez utiliser une macro de configuration contenant les options `NISservs` et `NISdmain`. Ces options ont pour effet de transmettre les adresses IP des serveurs NIS et du nom de domaine NIS au client. Le client devient ensuite automatiquement un client NIS.
	
	Si un système client DHCP exécute déjà Oracle Solaris, le client NIS n'est pas automatiquement configuré sur ce système lorsque le serveur DHCP envoie les informations NIS au client.
	
	Si le serveur DHCP est configuré pour communiquer des informations NIS au système client DHCP, vous pouvez connaître les valeurs transmises au client si vous utilisez la commande `dhcpinfo` sur le client de la façon suivante :
	
	`# /sbin/dhcpinfo NISdmain`
	
	`# /sbin/dhcpinfo NISservs`
	
	Remarque – Pour DHCPv6, veillez à inclure `-v6` ainsi que divers mots-clés de protocole dans la commande.
	
	`# /sbin/dhcpinfo -v6 NISDomain`
	
	`# /sbin/dhcpinfo -v6 NISServers`
	
	Utilisez les valeurs renvoyées pour le nom de domaine NIS et les serveurs NIS lorsque vous configurez le système en tant que client NIS.
	
	Pour configurer un client NIS pour un système client DHCP, procédez de manière habituelle comme indiqué au Chapitre 5, “Paramétrage et configuration du service NIS” du *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.
	
	Astuce – Vous pouvez créer un script en y faisant figurer les commandes `dhcpinfo` et `ypinit` afin d'automatiser la configuration du client NIS sur des systèmes clients DHCP.

NIS+	Si le client NIS+ d'un système client DHCP est configuré de façon conventionnelle, le serveur DHCP risque parfois de communiquer au client des adresses différentes. Cela pose un problème en terme de sécurité dans la mesure où la fonction de sécurité NIS+ intègre l'adresse IP dans la configuration. Pour s'assurer que votre client possède toujours la même adresse, configurez le client NIS+ pour un système client DHCP de façon non standard, comme cela est décrit dans la section “Configuration des clients DHCP en tant que clients NIS+” à la page 452. Si une adresse IP a été assignée de façon manuelle au système client DHCP, l'adresse du client est systématiquement la même. Vous pouvez configurer le client NIS+ de façon conventionnelle, comme indiqué à la section “Setting Up NIS+ Client Machines” du *System Administration Guide: Naming and Directory Services (NIS+)*.

TABLEAU 16–1 Informations sur la configuration des services de noms pour les systèmes clients DHCP *(Suite)*

Service de noms	Informations relatives à la configuration du client
`/etc/inet/hosts`	Vous devez configurer le fichier `/etc/inet/hosts` d'un système client DHCP devant utiliser `/etc/inet/hosts` pour son service de noms. Le nom d'hôte du système client DHCP est ajouté à son propre fichier `/etc/inet/hosts` par les outils DHCP. Il convient, cependant, d'ajouter manuellement le nom d'hôte aux fichiers `/etc/inet/hosts` des autres systèmes dans le réseau. Si le système serveur DHCP utilise `/etc/inet/hosts` pour la résolution de nom, vous devez également insérer manuellement le nom d'hôte du client sur le système.
DNS	Si le système client DHCP reçoit le nom de domaine DNS via DHCP, le fichier `/etc/resolv.conf` du système client est configuré automatiquement. Le fichier `/etc/nsswitch.conf` est également mis à jour automatiquement afin d'ajouter `dns` à la ligne `hosts` après tout autre service de noms dans l'ordre de recherche. Pour plus d'informations au sujet de DNS, reportez-vous au manuel *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

Configuration des clients DHCP en tant que clients NIS+

Vous pouvez utiliser le service de noms NIS+ sur des systèmes Oracle Solaris faisant office de clients DHCP. Toutefois, si votre serveur DHCP est capable de fournir des adresses différentes à différents moments, cela permet de contourner l'une des fonctions de sécurité de NIS+, à savoir la création d'informations d'identification DES (Data Encryption Standard). Pour travailler dans des conditions de sécurité optimales, configurez le serveur DHCP de façon à ce qu'il propose systématiquement la même adresse. Lorsque vous configurez un client NIS+ qui n'a *pas* recours à DHCP, vous ajoutez au serveur NIS+ des informations d'identification DES uniques pour le client. Il y a différentes façons de créer des informations d'identification. Vous pouvez, par exemple, utiliser le script `nisclient` ou la commande `nisaddcred`.

Pour pouvoir générer des informations d'identification NIS+, le client doit avoir un nom d'hôte statique qui permette de créer et de stocker ce type d'information. Si vous avez l'intention d'utiliser NIS+ et DHCP, il est impératif de définir des informations d'identification réservées à tous les noms d'hôtes des clients DHCP. Quels que soit l'adresse IP et le nom d'hôte associé reçus par un client DHCP, le client peut utiliser les mêmes informations d'identification DES.

La procédure suivante montre comment générer des informations d'identification pour l'ensemble des noms d'hôtes DHCP. Elle n'a d'intérêt que si vous connaissez les noms d'hôtes utilisés par les clients DHCP. Lorsque le serveur DHCP génère les noms d'hôtes, par exemple, vous avez une idée précise des noms d'hôtes susceptibles d'être reçus par un client.

Configuration des clients DHCP en tant que clients NIS+

Un système client DHCP censé devenir un client NIS+ doit exploiter les informations d'identification appartenant à un autre système client NIS+ dans le domaine NIS+. Cette procédure permet de produire uniquement des informations d'identification pour le système, lesquelles s'appliquent exclusivement au superutilisateur connecté au système. Tout autre utilisateur se connectant au système client DHCP doit posséder ses propres informations d'identification au niveau du serveur NIS+. Ces informations d'identification sont définies conformément à la procédure décrite dans le manuel *System Administration Guide: Naming and Directory Services (NIS+)*.

1. **Créez les informations d'identification pour un client en entrant la commande suivante sur le serveur NIS+ :**

   ```
   # nisgrep nisplus-client-name cred.org_dir > /tmp/file
   ```

   Cette commande inscrit l'entrée de table `cred.org_dir` pour le client NIS+ dans un fichier temporaire.

2. **Servez-vous de la commande `cat` pour afficher le contenu du fichier temporaire.**

   Vous pouvez également utiliser un éditeur de texte.

3. **Copiez les informations d'identification réservées aux clients DHCP.**

   Vous devez copier la clé publique et la clé privée (longues chaînes de chiffres et de lettres séparés par le signe deux-points). Les informations d'identification sont destinées à être collées dans la commande exécutée à l'étape suivante.

4. **Ajoutez les informations d'identification pour un client DHCP en tapant la commande suivante :**

   ```
   # nistbladm -a cname=" dhcp-client-name@nisplus-domain" auth_type=DES \
   auth_name="unix.dhcp-client-name@nisplus-domain" \
   public_data=copied-public-key \
   private_data=copied-private-key
   ```

   Pour la *clé-publique-copiée*, collez les informations relatives à la clé publique à partir du fichier temporaire. Pour la *clé-privée-copiée*, collez les informations relatives à la clé privée à partir du fichier temporaire.

5. **Copiez à distance les fichiers à partir du système client NIS+ vers le système client DHCP en tapant les commandes suivantes sur le système client DHCP :**

   ```
   # rcp nisplus-client-name:/var/nis/NIS_COLD_START /var/nis
   # rcp nisplus-client-name:/etc/.rootkey /etc
   # rcp nisplus-client-name:/etc/defaultdomain /etc
   ```

   Si vous obtenez un message signalant un problème de permission, il est possible que les systèmes ne soient pas configurés pour autoriser la copie à distance. Dans ce cas, il suffit de copier les fichiers en tant qu'utilisateur normal vers un emplacement intermédiaire. En tant que superutilisateur, copiez les fichiers depuis l'emplacement intermédiaire vers l'emplacement approprié sur le système client DHCP.

6 **Copiez le fichier du commutateur du service de noms qui convient pour NIS+ en entrant la commande suivante sur le système client DHCP :**

```
# cp /etc/nsswitch.nisplus /etc/nsswitch.conf
```

7 **Redémarrez le système client DHCP.**

Le système client DHCP doit désormais être en mesure d'utiliser les services NIS+.

Exemple 16–1 Configuration d'un système client DHCP en tant que client NIS+

L'exemple suivant suppose que vous disposez d'un système `nisei`, considéré comme un client NIS+ dans le domaine NIS+ `dev.example.net` . Vous disposez également d'un système client DHCP (`dhow`) et souhaitez que `dhow` devienne un client NIS+.

```
     (First log in as superuser on the NIS+ server)
# nisgrep nisei cred.org_dir > /tmp/nisei-cred
# cat /tmp/nisei-cred
nisei.dev.example.net.:DES:unix.nisei@dev.example.net:46199279911a84045b8e0
c76822179138173a20edbd8eab4:90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830
c05bc1c724b
# nistbladm -a cname="dhow@dev.example.net." \
auth_type=DES auth_name="unix.dhow@dev.example.net" \
public_data=46199279911a84045b8e0c76822179138173a20edbd8eab4 \
private_data=90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830\
c05bc1c724b
# rlogin dhow
     (Log in as superuser on dhow)
# rcp nisei:/var/nis/NIS_COLD_START /var/nis
# rcp nisei:/etc/.rootkey /etc
# rcp nisei:/etc/defaultdomain /etc
# cp /etc/nsswitch.nisplus /etc/nsswitch.conf
# reboot
```

Le système client DHCP `dhow` doit désormais être capable d'exploiter les services NIS+.

Exemple 16–2 Ajout d'informations d'identification à l'aide d'un script

Si vous souhaitez configurer un grand nombre de systèmes clients DHCP en tant que clients NIS+, le mieux est d'écrire un script. Un script est très pratique pour ajouter les entrées dans la table NIS+ `cred.org_dir`. Voici un exemple de script caractéristique.

```
#! /usr/bin/ksh
#
# Copyright (c) by Sun Microsystems, Inc. All rights reserved.
#
# Sample script for cloning a credential. Hosts file is already populated
# with entries of the form dhcp-[0-9][0-9][0-9]. The entry we're cloning
# is dhcp-001.
```

```
#
#
PUBLIC_DATA=6e72878d8dc095a8b5aea951733d6ea91b4ec59e136bd3b3
PRIVATE_DATA=3a86729b685e2b2320cd7e26d4f1519ee070a60620a93e48a8682c5031058df4
HOST="dhcp-"
DOMAIN="mydomain.example.com"

for
i in 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019
do
     print - ${HOST}${i}
     #nistbladm -r [cname="${HOST}${i}.${DOMAIN}."]cred.org_dir
     nistbladm -a cname="${HOST}${i}.${DOMAIN}." \
         auth_type=DES auth_name="unix.${HOST}${i}@${DOMAIN}" \
         public_data=${PUBLIC_DATA} private_data=${PRIVATE_DTA} cred.org_Dir
done

exit 0
```

Scripts d'événement client DHCP

Il est possible de configurer le client DHCP de façon à l'utiliser comme un programme exécutable ou un script en vue d'effectuer des actions appropriées pour le système client. Le programme ou le script, appelé *script d'événement*, est exécuté automatiquement dès que certains événements liés au bail DHCP se produisent. Vous pouvez vous servir du script d'événement pour exécuter d'autres commandes, programmes ou scripts en réponse à des événements de bail spécifiques. Pour ce faire, vous devez fournir votre propre script d'événement.

Les mots-clés d'événement suivants sont utilisés par `dhcpagent` pour signifier des événements de bail DHCP :

Mot-clé d'événement	**Description**
`BOUND` et `BOUND6`	L'interface est configurée pour DHCP. Le client reçoit l'accusé de réception (DHCPv4 `ACK`) ou (DHCPv6 `Reply`) du serveur DHCP, qui lui accorde la demande de bail pour une adresse IP. Le script d'événement est appelé immédiatement après la configuration de l'interface.
`EXTEND` et `EXTEND6`	Le client prolonge le bail de la ligne spécialisée. Le script d'événement est appelé dès que le client reçoit l'accusé de réception du serveur DHCP ayant trait à la demande de renouvellement.
`EXPIRE` et `EXPIRE6`	Le bail expire à la date butoir fixée. Pour DHCPv4, le script d'événement est appelé avant la suppression de l'adresse louée de l'interface et l'interface est signalée comme arrêtée. Pour DHCPv6, le script d'événement est appelé avant la suppression des dernières adresses louées de l'interface.

`DROP` et `DROP6`	Le client abandonne la ligne spécialisée pour retirer l'interface du contrôle de DHCP. Le script d'événement est appelé juste avant que l'interface n'échappe au contrôle de DHCP.
`RELEASE` et `RELEASE6`	Le client libère l'adresse IP. Le script d'événement est appelé juste avant que le client ne libère l'adresse sur l'interface et n'envoie le paquet DHCPv4 `RELEASE` ou DHCPv6 `Release` au serveur DHCP.
`INFORM` et `INFORM6`	Une interface se procure des données de configuration nouvelles ou mises à jour à partir d'un serveur DHCP par l'intermédiaire du paquet DHCPv4 `INFORM` ou du message DHCPv6 `Information-Request.` Ces événements se produisent si le client DHCP obtient uniquement les paramètres de configuration du serveur, mais pas le bail d'une adresse IP.
`LOSS6`	Pendant la phase d'expiration, lorsqu'il reste un ou plusieurs baux valides, le script d'événement est appelé juste avant la suppression des adresses expirées. Les adresses effacées sont signalées par l'indicateur `IFF_DEPRECATED`.

Pour chacun de ces événements, `dhcpagent` exécute la commande suivante :

```
/etc/dhcp/eventhook interface event
```

où *interface* représente l'interface faisant appel à DHCP et *événement* correspond à un des mots-clés d'événement décrits précédemment. Par exemple, la première fois que vous configurez l'interface `ce0` pour DHCP, `dhcpagent` appelle le script d'événement de la façon suivante :

```
/etc/dhcp/eventhook ce0 BOUND
```

Pour utiliser la fonction de script d'événement, vous devez effectuer les opérations suivantes :

- Donner le nom `/etc/dhcp/eventhook` au fichier exécutable.
- Définir `root` comme propriétaire du fichier.
- Configurer les permissions sur `755` (`rwxr-xr-x`).
- Écrire le script ou le programme afin de réaliser une série d'actions en réponse à un des événements documentés. Comme Sun est susceptible d'ajouter de nouveaux événements, le programme doit ignorer, en silence, les événements qui ne sont pas reconnus ou qui n'exigent aucune action. Le programme ou le script peut, par exemple, inscrire des informations dans un fichier journal en présence de l'événement `RELEASE`, et ignorer tous les autres événements.
- Rendre le script ou le programme non interactif. Avant de recourir au script d'événement, `stdin`, `stdout` et `stderr` se connectent à `/dev/null`. Pour afficher la sortie ou les erreurs, vous devez la/les rediriger vers un fichier.

Le script d'événement hérite son environnement de programme de `dhcpagent` et s'exécute avec les privilèges `root`. Il peut faire appel à l'utilitaire `dhcpinfo` pour obtenir des informations supplémentaires au sujet de l'interface, si cela est nécessaire. Pour plus d'informations, reportez-vous à la page de manuel `dhcpinfo(1)`.

Le démon `dhcpagent` attend que le script d'événement prenne fin pour tous les événements. Si le script d'événement ne se termine au bout de 55 secondes, `dhcpagent` envoie un signal `SIGTERM` au processus du script. Si le processus ne se termine par au bout de trois secondes supplémentaires, le démon envoie un signal `SIGKILL` pour interrompre le processus.

Vous trouverez un exemple de script d'événement dans la page de manuel `dhcpagent(1M)`.

L'Exemple 16–3 illustre l'utilisation d'un script d'événement DHCP pour maintenir le contenu du fichier `/etc/resolv.conf` à jour. Lorsque les événements `BOUND` et `EXTEND` se produisent, le script remplace les noms du serveur de domaine et du serveur de noms. Lorsque les événements `EXPIRE`, `DROP` et `RELEASE` se produisent, le script supprime les noms du serveur de domaine et du serveur de noms du fichier.

Remarque – Le script proposé en exemple considère que DHCP est la source qui fait autorité pour les noms du serveur de domaine et le serveur de noms. Il suppose également que toutes les interfaces sous le contrôle de DHCP renvoient des informations cohérentes et à jour. Il est possible que ces conditions ne soient pas réunies sur votre système.

EXEMPLE 16–3 Script d'événement pour la mise à jour du fichier `/etc/resolv.conf`

```
#!/bin/ksh -p

PATH=/bin:/sbin export PATH
umask 0222

# Refresh the domain and name servers on /etc/resolv.conf

insert ()
{
    dnsservers=‘dhcpinfo -i $1 DNSserv‘
    if [ -n "$dnsservers" ]; then
        # remove the old domain and name servers
        if [ -f /etc/resolv.conf ]; then
            rm -f /tmp/resolv.conf.$$
            sed -e ’/^domain/d’ -e ’/^nameserver/d’ \
                /etc/resolv.conf > /tmp/resolv.conf.$$
        fi

        # add the new domain
        dnsdomain=‘dhcpinfo -i $1 DNSdmain‘
        if [ -n "$dnsdomain" ]; then
            echo "domain $dnsdomain" >> /tmp/resolv.conf.$$
        fi

        # add new name servers
```

EXEMPLE 16–3 Script d'événement pour la mise à jour du fichier `/etc/resolv.conf` *(Suite)*

```
        for name in $dnsservers; do
            echo nameserver $name >> /tmp/resolv.conf.$$
        done
        mv -f /tmp/resolv.conf.$$ /etc/resolv.conf
    fi
}

# Remove the domain and name servers from /etc/resolv.conf

remove ()
{
    if [ -f /etc/resolv.conf ]; then
        rm -f /tmp/resolv.conf.$$
        sed -e '/^domain/d' -e '/^nameserver/d' \
            /etc/resolv.conf > /tmp/resolv.conf.$$
        mv -f /tmp/resolv.conf.$$ /etc/resolv.conf
    fi
}

case $2 in
BOUND | EXTEND)
    insert $1
    exit 0
    ;;
EXPIRE | DROP | RELEASE)
    remove
    exit 0
    ;;
*)
    exit 0
    ;;
esac
```

◆ ◆ ◆ CHAPITRE 17

Résolution des problèmes DHCP (référence)

Ce chapitre vous aide à résoudre les problèmes que vous êtes susceptible de rencontrer lors de la configuration d'un serveur ou d'un client DHCP. Il propose également différentes solutions possibles aux problèmes d'utilisation de DHCP une fois la configuration terminée.

Il contient les informations suivantes :

Reportez-vous au Chapitre 14, "Configuration du service DHCP (tâches)" pour plus d'informations sur la configuration de votre serveur DHCP. Pour plus d'informations au sujet de la configuration de votre client DHCP, reportez-vous à la section "Activation et désactivation d'un client DHCP " à la page 443.

Résolution des problèmes de serveur DHCP

Il existe deux grandes catégories de problèmes en matière de configuration du serveur :

Problèmes liés à NIS+ et au magasin de données DHCP

Si vous utilisez NIS+ en guise de magasin de données DHCP, voici les trois grands types de problème que vous êtes susceptible de rencontrer :

Impossible de sélectionner NIS+ comme magasin de données DHCP

Si vous essayez d'utiliser NIS+ comme magasin de données, il est possible que le gestionnaire DHCP ne vous propose pas ce choix. Si vous exécutez la commande `dhcpconfig`, vous risquez d'obtenir un message précisant que NIS+ ne semble ni être installé, ni en service. Ces deux symptômes signifient simplement que NIS+ n'a pas été configuré pour ce serveur, même si ce système d'information est pourtant utilisé sur le réseau. Pour pouvoir sélectionner NIS+ comme magasin de données, il convient de configurer le système serveur en tant que client NIS+.

Avant de définir le système serveur DHCP en tant que client NIS+, assurez-vous que les conditions suivantes sont réunies :

- Le domaine a déjà été configuré.
- Le serveur maître du domaine NIS+ est en en cours d'exécution.
- Les tables du serveur maître ont été renseignées.
- La table des hôtes possède une entrée pour le nouveau système client, à savoir le système serveur DHCP.

La section "Setting Up NIS+ Client Machines" du *System Administration Guide: Naming and Directory Services (NIS+)* explique de façon détaillée comment configurer un client NIS+.

NIS+ n'est pas configuré correctement pour le magasin de données DHCP

Lorsque vous utilisez le système d'information NIS+ avec DHCP, des erreurs risquent de produire si des modifications ont été apportées à NIS+. En effet, les changements peuvent provoquer des problèmes de configuration. Les explications suivantes vous aideront à déterminer l'origine de ces problèmes et d'y apporter des solutions.

Problème : L'objet root n'existe pas dans le domaine NIS+.

Solution : Tapez la commande suivante\~:

```
/usr/lib/nis/nisstat
```

Cette commande affiche des statistiques pour le domaine. Si l'objet root n'existe pas, aucune statistique n'est établie.

Configurez le domaine NIS+ à l'aide du *System Administration Guide: Naming and Directory Services (NIS+)* .

Problème : NIS+ n'est pas pris en compte avec les informations `passwd` et `publickey` .

Solution : Tapez la commande suivante pour afficher le fichier de configuration correspondant au commutateur du service de noms :

```
cat /etc/nsswitch.conf
```

Vérifiez les entrées `passwd` et `publickey` pour le mot-clé “nisplus”. Pour plus d'informations sur le commutateur du service de noms, reportez-vous au *System Administration Guide: Naming and Directory Services (NIS+)*.

Problème : Le nom de domaine est vide.

Solution : Tapez la commande suivante\~:

```
domainname
```

Si la commande renvoie une chaîne vide, cela signifie qu'aucun nom de domaine n'a été défini pour le domaine. Utilisez des fichiers locaux pour votre magasin de données ou configurez un domaine NIS+ pour votre réseau. Reportez-vous au *System Administration Guide: Naming and Directory Services (NIS+)* .

Problème : Le fichier `NIS_COLD_START` n'existe pas.

Solution : Tapez la commande suivante sur le système serveur pour vérifier si le fichier existe :

```
cat /var/nis/NIS_COLD_START
```

Utilisez des fichiers locaux pour votre magasin de données ou créez un client NIS+. Reportez-vous au *System Administration Guide: Naming and Directory Services (NIS+)* .

Problèmes d'accès à NIS+ pour le magasin de données DHCP

Des problèmes d'accès à NIS+ risquent de générer des messages d'erreur relatifs à des informations d'identification DES incorrectes ou des autorisations de mise à jour de tables ou d'objets NIS+ non appropriées. Aidez-vous des explications suivantes pour déterminer la cause des erreurs d'accès NIS+ obtenues.

Problème : Le système serveur DHCP ne dispose pas d'un droit de création sur l'objet `org_dir` dans le domaine NIS+.

Solution : Tapez la commande suivante\~:

```
nisls -ld org_dir
```

Les droits d'accès sont présentés sous la forme `r---rmcdrmcdr---`. Les autorisations s'appliquent respectivement à personne, au propriétaire, au groupe et à tous. Le propriétaire de l'objet est indiqué à la suite.

En principe, l'objet répertoire `org_dir` garantit des droits complets à la fois au propriétaire et au groupe. Les droits complets offrent les possibilités suivantes : lecture, modification, création et destruction. L'objet répertoire `org_dir` accorde uniquement un accès en lecture aux classes world et nobody.

Le nom du serveur DHCP doit correspondre au propriétaire de l'objet `org_dir` ou à l'entité principale du groupe. Le groupe doit bénéficier d'un droit de création. Répertoriez les informations du groupe à l'aide de la commande :

`nisls -ldg org_dir`
Servez-vous de la commande `nischmod` pour changer les autorisations de `org_dir`, si cela est nécessaire. Pour accorder un droit de création au groupe, par exemple, tapez la commande suivante :

`nischmod g+c org_dir`
Pour plus d'informations, reportez-vous à la page de manuel `nischmod(1)`.

Problème : Le serveur DHCP ne dispose pas des droits d'accès lui permettant de créer une table sous l'objet `org_dir`.

Ce problème signifie généralement que le nom principal du système serveur n'est pas un membre du groupe propriétaire pour l'objet `org_dir` ou qu'aucun groupe propriétaire n'existe.

Solution : Tapez la commande suivante pour identifier le nom du groupe propriétaire :

`niscat -o org_dir`
Recherchez une ligne similaire à la ligne suivante :

```
Group : "admin.example.com."
```

Affichez la liste des noms principaux dans le groupe à l'aide de la commande suivante :

`nisgrpadm -l` *groupname*
La commande suivante établit, par exemple, la liste des noms principaux du groupe `admin.example.com` :

```
nisgrpadm -l admin.example.com
```

Le nom du système serveur doit être répertorié comme un membre explicite du groupe ou faire partie des membres implicites du groupe. Si besoin est, ajoutez le nom du système serveur au groupe à l'aide de la commande `nisgrpadm`.

Pour inclure, par exemple, le nom du serveur `pacific` au groupe `admin.example.com`, tapez la commande suivante :

```
nisgrpadm -a admin.example.com pacific.example.com
```

Pour plus d'informations, reportez-vous à la page de manuel `nisgrpadm(1)`.

Problème : Le serveur DHCP ne dispose pas d'informations d'identification DES (Data Encryption Standard) valides dans la table NIS+ `cred`.

Solution : En cas de problème d'identification, un message d'erreur indique que l'utilisateur ne possède pas d'informations d'identification DES dans le service de noms NIS+.

Servez-vous de la commande `nisaddcred` pour ajouter des informations d'identification de sécurité pour le système serveur DHCP.

L'exemple suivant montre comment ajouter des informations d'identification DES pour le système `mercury` dans le domaine `example.com` :

```
nisaddcred -p unix.mercury@example.com \
-P mercury.example.com. DES example.com.
```

La commande invite l'utilisateur à spécifier le mot de passe root nécessaire à la création d'une clé secrète chiffrée.

Pour plus d'informations, reportez-vous à la page de manuel `nisaddcred(1M)`.

Erreurs d'allocation d'adresses IP dans DHCP

Lorsqu'un client essaie d'obtenir ou de valider une adresse IP, il est possible que des erreurs soient consignées dans `syslog` ou dans la sortie du mode de débogage du serveur. Vous trouverez les causes et solutions possibles de ces problèmes dans la liste de messages d'erreur suivante.

`There is no` *n.n.n.n* `dhcp-network table for DHCP client's network`

Origine : Un client demande une adresse IP spécifique ou cherche à prolonger le bail de son adresse IP actuelle. Le serveur DHCP ne parvient pas à trouver la table de réseau DHCP pour cette adresse.

Solution : Il est possible que la table de réseau DHCP ait été supprimée par accident. Vous pouvez reconstituer la table de réseau en ajoutant à nouveau le réseau à l'aide du gestionnaire DHCP ou de la commande `dhcpconfig`.

`ICMP ECHO reply to OFFER candidate:` *n.n.n.n*`, disabling`

Origine : L'adresse IP proposée à un client DHCP est déjà utilisée. Ce problème risque de se produire lorsque plusieurs serveurs DHCP sont propriétaires de l'adresse ou si l'adresse a été configurée manuellement pour un client réseau non DHCP.

Solution : Identifiez le véritable propriétaire de l'adresse. Corrigez la base de données du serveur DHCP ou la configuration réseau de l'hôte.

`ICMP ECHO reply to OFFER candidate:` *n.n.n.n*`. No corresponding dhcp network record.`

Origine : L'adresse IP proposée à un client DHCP ne possède pas d'enregistrement dans une table du réseau. Cette erreur indique que l'enregistrement de l'adresse IP a été supprimé de la table du réseau DHCP après la sélection de l'adresse. Elle peut survenir uniquement pendant la brève période qui précède la vérification des adresses en double.

Solution : Servez-vous du gestionnaire DHCP ou de la commande `pntadm` pour afficher la table du réseau DHCP. Si l'adresse IP n'y figure pas, créez-la à l'aide du gestionnaire DHCP en choisissant la commande Create dans le menu Edit de l'onglet Addresse. Vous pouvez également générer l'adresse IP au moyen de la commande `pntadm`.

`DHCP network record for` *n.n.n.n*`is unavailable, ignoring request.`

Origine : Comme l'enregistrement correspondant à l'adresse IP demandée ne figure pas dans la table de réseau DHCP, le serveur abandonne la requête.

Solution : Servez-vous du gestionnaire DHCP ou de la commande `pntadm` pour afficher la table du réseau DHCP. Si l'adresse IP n'y figure pas, créez-la à l'aide du gestionnaire DHCP en choisissant la commande Create dans le menu Edit de l'onglet Addresse. Vous pouvez également générer l'adresse au moyen de la commande `pntadm`.

n.n.n.n `currently marked as unusable.`

Origine : Il est impossible d'offrir l'adresse IP demandée, car elle est marquée comme inutilisable dans la table du réseau.

Solution : Vous pouvez utiliser le gestionnaire DHCP ou la commande `pntadm` afin de rendre l'adresse utilisable.

n.n.n.n `was manually allocated. No dynamic address will be allocated.`

Origine : Une adresse allouée de façon manuelle a été assignée à l'ID de client. Or, cette adresse est marquée comme inutilisable. Le serveur ne peut pas allouer une autre adresse à ce client.

Solution : Vous pouvez utiliser le gestionnaire DHCP ou de la commande `pntadm` pour rendre l'adresse utilisable ou allouer manuellement une autre adresse au client.

`Manual allocation (`*n.n.n.n, client ID*`) has` *n* `other records. Should have 0.`

Origine : Plusieurs adresses IP ont été assignées manuellement au client possédant l'ID de client spécifié. Une seule adresse doit être attribuée au client. Le serveur sélectionne la dernière adresse assignée manuellement qu'il trouve dans la table de réseau.

Solution : Servez-vous du gestionnaire DHCP ou de la commande `pntadm` pour modifier les adresses IP en vue de supprimer les allocations manuelles supplémentaires.

`No more IP addresses on` *n.n.n.n*`network.`

Origine : Toutes les adresses IP gérées actuellement par DHCP sur le réseau spécifié ont été allouées.

Solution : Servez-vous du gestionnaire DHCP ou de la commande `pntadm` pour définir de nouvelles adresses IP pour ce réseau.

`Client:` *clientid* `lease on` *n.n.n.n* `expired.`

Origine : Le bail n'était pas négociable et a expiré.

Solution : Le client doit redémarrer automatiquement le protocole pour obtenir un nouveau bail.

`Offer expired for client:` *n.n.n.n*

Origine : Le serveur propose une adresse IP au client, mais comme le client n'a pas répondu assez vite, l'offre a expiré.

Solution : Le client doit émettre automatiquement un nouveau message de découverte. Si ce message n'aboutit pas non plus, augmentez le délai d'expiration des offres dans la mémoire cache du serveur DHCP. Choisissez Modify dans le menu Service du gestionnaire DHCP.

`Client:` *clientid* `REQUEST is missing requested IP option.`
Origine : Comme la requête du client ne correspondait pas à l'adresse IP proposée, le serveur DHCP a ignoré la demande. Cela peut se produire lorsque vous utilisez un client DHCP tiers non conforme au protocole DHCP mis à jour (RFC 2131).

Solution : Mettez à jour le logiciel client.

`Client:` *clientid* `is trying to renew` *n.n.n.n*`, an IP address it has not leased.`
Origine : L'adresse IP pour ce client dans la table de réseau DHCP ne correspond pas à l'adresse IP que le client a spécifiée dans sa demande de renouvellement. Le serveur DHCP ne peut donc pas renouveler le bail de l'adresse IP. Ce problème peut se produire lorsque vous supprimez l'enregistrement d'un client alors que ce dernier fait encore usage de l'adresse IP.

Solution : Servez-vous du gestionnaire DHCP ou de la commande `pntadm` pour examiner la table de réseau et corriger l'enregistrement du client, si besoin est. L'ID de client doit être lié à l'adresse IP indiquée. Si ce n'est pas le cas, modifiez les propriétés de l'adresse pour ajouter l'ID de client.

`Client:` *clientid* `is trying to verify unrecorded address:` *n.n.n.n*`, ignored.`
Origine : Le client spécifié n'a pas été enregistré dans la table de réseau DHCP avec cette adresse. La requête est donc ignorée par ce serveur DHCP.

Il est possible qu'un autre serveur DHCP sur le réseau ait assigné l'adresse à ce client ou que vous ayez supprimé l'enregistrement du client alors qu'il continuait à utiliser l'adresse IP.

Solution : Servez-vous du gestionnaire DHCP ou de la commande `pntadm` pour examiner la table de réseau sur ce serveur et sur tous les autres serveurs DHCP du réseau. Apportez les corrections nécessaires.

Vous pouvez également laisser le bail expirer. Le client effectue automatiquement une demande de renouvellement.

Pour que le client obtienne immédiatement un nouveau bail, redémarrez le protocole DHCP sur le client en tapant les commandes suivantes :

```
ifconfig interface dhcp release
ifconfig interface dhcp start
```

Résolution des problèmes de configuration d'un client DHCP

Il existe deux grandes catégories de problèmes avec un client DHCP :

- “Problèmes de communication avec le serveur DHCP” à la page 466
- “Problèmes liés à des données de configuration DHCP inexactes” à la page 474

Problèmes de communication avec le serveur DHCP

Cette section décrit les problèmes que vous risquez de rencontrer lors de l'ajout de clients DHCP au réseau.

Après avoir activé le logiciel client et redémarré le système, le client essaie d'établir une liaison avec le serveur DHCP afin de connaître sa configuration réseau. S'il n'y parvient pas, voici les messages d'erreur que vous êtes susceptible d'obtenir :

```
DHCP or BOOTP server not responding
```

Pour déterminer l'origine du problème, vous devez réunir les éléments de diagnostic nécessaires à partir du client et du serveur. Les tâches suivantes vous seront très utiles à ce titre :

1. “Exécution du client DHCP en mode de débogage” à la page 466
2. “Exécution du serveur DHCP en mode de débogage” à la page 467
3. “Contrôle du trafic sur le réseau DHCP à l'aide de `snoop`” à la page 467

Vous pouvez réaliser ces tâches ensemble ou indépendamment les unes des autres.

Les informations que vous collectez permettent de savoir si le problème est lié au client, au serveur ou à un agent de relais. Une fois l'origine du problème identifiée, vous pourrez appliquer la solution qui convient.

▼ Exécution du client DHCP en mode de débogage

Si le client n'est pas un client DHCP, reportez-vous à la documentation du client pour savoir comment exécuter le client en mode de débogage.

Si vous disposez d'un client DHCP, procédez de la façon suivante.

1 Connectez-vous au système client DHCP en tant que superutilisateur.

2 Détruisez le démon client DHCP.

```
# pkill -x dhcpagent
```

3 Redémarrez le démon en mode de débogage.

```
# /sbin/dhcpagent -d1 -f &
```

Le commutateur `-d` fait passer le client DHCP en mode de débogage avec un détail de niveau 1. Le commutateur `-f` permet de diriger la sortie vers la console au lieu de `syslog`.

4. **Configurez l'interface en vue de lancer la négociation DHCP.**

   ```
   # ifconfig interface dhcp start
   ```

   Remplacez *interface* par le nom de l'interface réseau du client, tel que `ge0`.

   En mode de débogage, le démon du client affiche les messages à l'écran pendant l'exécution des requêtes DHCP. Pour plus d'informations sur la sortie du mode de débogage client, reportez-vous à la section "Sortie du client DHCP en mode de débogage" à la page 468.

▼ Exécution du serveur DHCP en mode de débogage

1. **Connectez-vous au système serveur en tant que superutilisateur.**

2. **Arrêtez temporairement le serveur DHCP.**

   ```
   # svcadm disable -t svc:/network/dhcp-server
   ```

   Vous pouvez également arrêter le serveur à l'aide du gestionnaire DHCP ou de la commande `dhcpconfig`.

3. **Redémarrez le démon en mode de débogage.**

   ```
   # /usr/lib/inet/in.dhcpd -d -v
   ```

   N'oubliez pas d'insérer les options de ligne de commande `in.dhcpd` que vous utilisez normalement lors de l'exécution du démon. Si vous lancez, par exemple, le démon en tant qu'agent de relais BOOTP, pensez à associer l'option `-r` à la commande `in.dhcpd -d -v`.

   En mode de débogage, le démon affiche les messages à l'écran pendant le traitement des requêtes DHCP ou BOOTP. Pour plus d'informations sur la sortie du mode de débogage serveur, reportez-vous à la section "Sortie du serveur DHCP en mode de débogage" à la page 469.

▼ Contrôle du trafic sur le réseau DHCP à l'aide de `snoop`

1. **Connectez-vous au système serveur DHCP en tant que superutilisateur.**

2. **Lancez la commande `snoop` pour commencer le suivi du trafic sur le réseau via l'interface réseau du serveur.**

   ```
   # /usr/sbin/snoop -d interface -o snoop-output-filename udp port 67 or udp port 68
   ```

   Par exemple, vous entrez la commande suivante :

   ```
   #  /usr/sbin/snoop -d hme0 -o /tmp/snoop.output udp port 67 or udp port 68
   ```

   `snoop` continue à contrôler l'interface tant que vous n'arrêtez pas `snoop` en appuyant sur Contrôle-C une fois que vous avez collecté les informations requises.

3 **Initialisez le système client ou relancez `dhcpagent` sur le système client.**

La section "Exécution du client DHCP en mode de débogage" à la page 466 explique comment redémarrer `dhcpagent`.

4 **Exécutez `snoop` sur le système serveur pour afficher les paquets du réseau consignés dans le fichier de sortie :**

```
# /usr/sbin/snoop -i snoop-output-filename -x0 -v
```

Par exemple, vous entrez la commande suivante :

```
# /usr/sbin/snoop -i /tmp/snoop.output -x0 -v
```

Voir aussi Pour savoir comment interpréter la sortie, reportez-vous à la section "Sortie snoop DHCP" à la page 472.

Sortie du client DHCP en mode de débogage

L'exemple suivant présente une sortie normale correspondant à la situation suivante : un client DHCP en mode de débogage envoie sa requête DHCP et reçoit ses données de configuration à partir d'un serveur DHCP.

EXEMPLE 17–1 Sortie normale du client DHCP en mode de débogage

```
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhcpagent: debug: init_ifs: initted interface hme0
/sbin/dhcpagent: debug: insert_ifs: hme0: sdumax 1500, optmax 1260, hwtype 1, hwlen 6
/sbin/dhcpagent: debug: insert_ifs: inserted interface hme0
/sbin/dhcpagent: debug: register_acknak: registered acknak id 5
/sbin/dhcpagent: debug: unregister_acknak: unregistered acknak id 5
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x26018 (ARP reply filter)
/sbin/dhcpagent: info: setting IP netmask on hme0 to 255.255.192.0
/sbin/dhcpagent: info: setting IP address on hme0 to 10.23.3.233
/sbin/dhcpagent: info: setting broadcast address on hme0 to 10.23.63.255
/sbin/dhcpagent: info: added default router 10.23.0.1 on hme0
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x28054 (blackhole filter)
/sbin/dhcpagent: debug: configure_if: bound ifsp->if_sock_ip_fd
/sbin/dhcpagent: info: hme0 acquired lease, expires Tue Aug 10 16:18:33 2006
/sbin/dhcpagent: info: hme0 begins renewal at Tue Aug 10 15:49:44 2006
/sbin/dhcpagent: info: hme0 begins rebinding at Tue Aug 10 16:11:03 2006
```

Si le client ne parvient pas à joindre le serveur DHCP, il est possible que la sortie du mode de débogage affichée à l'écran soit similaire à la sortie illustrée dans l'exemple qui suit.

EXEMPLE 17–2 Sortie signalant un problème du client DHCP en mode de débogage

```
/sbin/dhcpagent: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhcpagent: debug: init_ifs: initted interface hme0
/sbin/dhcpagent: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhcpagent: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhcpagent: debug: select_best: no valid OFFER/BOOTP reply
```

EXEMPLE 17–2 Sortie signalant un problème du client DHCP en mode de débogage *(Suite)*

Si vous voyez ce message, cela signifie que la requête du client n'a jamais atteint le serveur ou que le serveur n'est pas en mesure d'envoyer une réponse au client. Exécutez `snoop` sur le serveur comme indiqué à la section "Contrôle du trafic sur le réseau DHCP à l'aide de snoop" à la page 467 afin de déterminer si des paquets provenant du client sont parvenus au serveur.

Sortie du serveur DHCP en mode de débogage

La sortie normale du serveur en mode de débogage présente les informations de configuration du serveur suivies des données relatives à chaque interface réseau au démarrage du démon. À l'issue du démarrage du démon, la sortie du mode de débogage affiche les informations relatives aux requêtes traitées par le démon. L'Exemple 17–3 illustre la sortie du mode de débogage pour un serveur DHCP venant d'être démarré. Le serveur prolonge le bail pour un client utilisant une adresse appartenant à un autre serveur DHCP qui ne répond pas.

EXEMPLE 17–3 Sortie normale pour le serveur DHCP en mode de débogage

```
Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
Run mode is: DHCP Server Mode.
Datastore: nisplus
Path: org_dir.dhcp.test..:dhcp.test..:$
DHCP offer TTL: 10
Ethers compatibility enabled.
BOOTP compatibility enabled.
ICMP validation timeout: 1000 milliseconds, Attempts: 2.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.21.255.255
Netmask: 255.255.0.0
Address: 10.21.0.2
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 10.22.255.255
Netmask: 255.255.0.0
Address: 10.22.0.1
Monitor (0007/qfe0) started...
Thread Id: 0007 - Monitoring Interface: qfe0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.23.63.255
Netmask: 255.255.192.0
Address: 10.23.0.1
Read 33 entries from DHCP macro database on Tue Aug 10 15:10:27 2006
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
```

EXEMPLE 17–3 Sortie normale pour le serveur DHCP en mode de débogage *(Suite)*

```
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A maps to IP: 10.23.3.233
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
DHCP EXTEND 0934312543 0934316143 10.23.3.233 10.21.0.2
          0800201DBA3A SUNW.Ultra-5_10 0800201DBA3A
```

L'Exemple 17–4 illustre la sortie du mode de débogage d'un démon DHCP exécuté en tant qu'agent de relais BOOTP. L'agent transfère les requêtes d'un client vers un serveur DHCP et relaie les réponses du serveur au client.

EXEMPLE 17–4 Sortie normale d'un agent de relais BOOTP en mode de débogage

```
Relay destination: 10.21.0.4 (blue-servr2)     network: 10.21.0.0
Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
Run mode is: Relay Agent Mode.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.21.255.255
Netmask: 255.255.0.0
Address: 10.21.0.2
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 10.22.255.255
Netmask: 255.255.0.0
Address: 10.22.0.1
Monitor (0007/qfe0) started...
Thread Id: 0007 - Monitoring Interface: qfe0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.23.63.255
Netmask: 255.255.192.0
Address: 10.23.0.1
Relaying request 0800201DBA3A to 10.21.0.4, server port.
BOOTP RELAY-SRVR 0934297685 0000000000 0.0.0.0 10.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 10.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
BOOTP RELAY-CLNT 0934297688 0000000000 10.23.0.1 10.23.3.233 0800201DBA3A
N/A 0800201DBA3A
Relaying request 0800201DBA3A to 10.21.0.4, server port.
BOOTP RELAY-SRVR 0934297689 0000000000 0.0.0.0 10.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 10.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
```

EXEMPLE 17–4 Sortie normale d'un agent de relais BOOTP en mode de débogage *(Suite)*

Si vous constatez un problème avec DHCP, voici les avertissements ou messages d'erreur susceptibles d'être affichés dans la sortie du mode de débogage. Recherchez la solution appropriée dans la liste des messages d'erreur DHCP.

`ICMP ECHO reply to OFFER candidate:` *adresse_ip* `disabling`

Origine : Avant de proposer une adresse IP à un client, le serveur DHCP effectue un test ping lors de l'envoi de l'adresse pour s'assurer que l'adresse n'est pas déjà utilisée. Si un client répond, cela signifie que l'adresse est effectivement utilisée.

Solution : Vérifiez si l'adresse que vous avez configurée est libre. Vous pouvez, pour ce faire, exécuter la commande `ping`. Pour plus d'informations, reportez-vous à la page de manuel `ping`(1M).

`No more IP addresses on` *adresse-réseau* `network.`

Origine : Aucune adresse IP n'est disponible dans la table de réseau DHCP associée au réseau du client.

Solution : Créez d'autres d'adresses IP avec le gestionnaire DHCP ou à l'aide de la commande `pntadm`. Si le démon DHCP est chargé de contrôler plusieurs sous-réseaux, assurez-vous que les adresses supplémentaires s'appliquent au sous-réseau où figure le client. Pour plus d'informations, reportez-vous à la section "Ajout d'adresses IP au service DHCP" à la page 389.

`No more IP addresses for` *adresse-réseau* `network when you are running the DHCP daemon in BOOTP compatibility mode.`

Origine : BOOTP n'applique pas de durée de bail. Aussi, le serveur DHCP recherche des adresses libres dont l'indicateur BOOTP permet leur allocation aux clients BOOTP.

Solution : Servez-vous du gestionnaire DHCP pour allouer des adresses BOOTP. Voir "Prise en charge des clients BOOTP via le service DHCP (liste des tâches)" à la page 382.

`Demande d'accès à une base de données réseau inexistante :` *nom-base-de-données* `dans le magasin de données :` *magasin-de-données.*

Origine : Lors de la configuration du serveur DHCP, la table de réseau DHCP d'un sous-réseau n'a pas été créée.

Solution : Servez-vous du gestionnaire DHCP ou de la commande `pntadm` pour créer la table de réseau DHCP et définir de nouvelles adresses IP. Voir "Ajout de réseaux DHCP" à la page 374.

`There is no` *nom-table* `dhcp-network table for DHCP client's network.`
Origine : Lors de la configuration du serveur DHCP, la table de réseau DHCP d'un sous-réseau n'a pas été créée.

Solution : Servez-vous du gestionnaire DHCP ou de la commande `pntadm` pour créer la table de réseau DHCP et définir de nouvelles adresses IP. Voir "Ajout de réseaux DHCP" à la page 374.

`Client using non_RFC1048 BOOTP cookie.`
Origine : Un périphérique du réseau essaie d'accéder à une implémentation non prise en charge de BOOTP.

Solution : Ignorez ce message, sauf si vous avez besoin de configurer ce périphérique. Pour savoir comment prendre en charge ce périphérique, reportez-vous à la section "Prise en charge des clients BOOTP via le service DHCP (liste des tâches)" à la page 382.

Sortie `snoop` DHCP

Dans la sortie `snoop`, assurez-vous que les paquets sont échangés entre le système client DHCP et le système serveur DHCP. L'adresse IP pour chaque système est indiquée dans chaque paquet. Les adresses IP des routeurs ou des agents de relais dans le chemin du paquet sont également mentionnées. Si vous constatez que les systèmes n'échangent pas de paquets, il est probable que le système client ne soit pas en mesure d'établir le contact avec le système serveur. Le problème se produit donc à un niveau inférieur.

Pour évaluer la sortie `snoop`, vous devez connaître le comportement normal de la commande. Vous devez, par exemple, savoir si la requête transite par un agent de relais BOOTP. Il est essentiel, en outre, de connaître les adresses MAC et l'adresse IP des systèmes impliqués de façon à déterminer si ces valeurs sont celles que vous attendiez. S'il existe plusieurs interfaces réseau, vous devez également connaître leurs adresses.

L'exemple suivant présente une sortie `snoop` normale pour un accusé de réception DHCP transmis depuis le serveur DHCP sur `blue-servr2` à destination d'un client dont l'adresse MAC est `8:0:20:8e:f3:7e` . Dans l'accusé de réception, le serveur alloue au client l'adresse IP `192.168.252.6` et le nom d'hôte `white-6`. Y figurent également un certain nombre d'options de réseau standard et plusieurs options spécifiques au fournisseur pour le client.

EXEMPLE 17–5 Exemple de sortie `snoop` pour un paquet

```
ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 26 arrived at 14:43:19.14
ETHER:  Packet size = 540 bytes
ETHER:  Destination = 8:0:20:8e:f3:7e, Sun
ETHER:  Source      = 8:0:20:1e:31:c1, Sun
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
```

EXEMPLE 17–5 Exemple de sortie snoop pour un paquet *(Suite)*

```
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 526 bytes
IP:   Identification = 64667
IP:   Flags = 0x4 IP:         .1.. .... = do not fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 254 seconds/hops
IP:   Protocol = 17 (UDP)
IP:   Header checksum = 157a
IP:   Source address = 10.21.0.4, blue-servr2
IP:   Destination address = 192.168.252.6, white-6
IP:   No options
IP:   UDP:  ----- UDP Header -----
UDP:
UDP:  Source port = 67
UDP:  Destination port = 68 (BOOTPC)
UDP:  Length = 506
UDP:  Checksum = 5D4C
UDP:
DHCP: ----- Dynamic Host Configuration Protocol -----
DHCP:
DHCP: Hardware address type (htype) =  1 (Ethernet (10Mb))
DHCP: Hardware address length (hlen) = 6 octets
DHCP: Relay agent hops = 0
DHCP: Transaction ID = 0x2e210f17
DHCP: Time since boot = 0 seconds
DHCP: Flags = 0x0000
DHCP: Client address (ciaddr) = 0.0.0.0
DHCP: Your client address (yiaddr) = 192.168.252.6
DHCP: Next server address (siaddr) = 10.21.0.2
DHCP: Relay agent address (giaddr) = 0.0.0.0
DHCP: Client hardware address (chaddr) = 08:00:20:11:E0:1B
DHCP:
DHCP: ----- (Options) field options -----
DHCP:
DHCP: Message type = DHCPACK
DHCP: DHCP Server Identifier = 10.21.0.4
DHCP: Subnet Mask = 255.255.255.0
DHCP: Router at = 192.168.252.1
DHCP: Broadcast Address = 192.168.252.255
DHCP: NISPLUS Domainname = dhcp.test
DHCP: IP Address Lease Time = 3600 seconds
DHCP: UTC Time Offset = -14400 seconds
DHCP: RFC868 Time Servers at = 10.21.0.4
DHCP: DNS Domain Name = sem.example.com
DHCP: DNS Servers at = 10.21.0.1
DHCP: Client Hostname = white-6
DHCP: Vendor-specific Options (166 total octets):
DHCP:   (02) 04 octets  0x8194AE1B (unprintable)
```

EXEMPLE 17–5 Exemple de sortie snoop pour un paquet *(Suite)*

```
DHCP:   (03) 08 octets  "pacific"
DHCP:   (10) 04 octets  0x8194AE1B (unprintable)
DHCP:   (11) 08 octets  "pacific"
DHCP:   (15) 05 octets  "xterm"
DHCP:   (04) 53 octets  "/export/s2/base.s2s/latest/Solaris_8/Tools/Boot"
DHCP:   (12) 32 octets  "/export/s2/base.s2s/latest"
DHCP:   (07) 27 octets  "/platform/sun4u/kernel/unix"
DHCP:   (08) 07 octets  "EST5EDT"
  0: 0800 208e f37e 0800 201e 31c1 0800 4500    .. .ó~.. .1...E.
 16: 020e fc9b 4000 fe11 157a ac15 0004 c0a8    ....@....z......
 32: fc06 0043 0044 01fa 5d4c 0201 0600 2e21    ...C.D..]L.....!
 48: 0f17 0000 0000 0000 0000 c0a8 fc06 ac15    ................
 64: 0002 0000 0000 0800 2011 e01b 0000 0000    ........ .......
 80: 0000 0000 0000 0000 0000 0000 0000 0000    ................
 96: 0000 0000 0000 0000 0000 0000 0000 0000    ................
112: 0000 0000 0000 0000 0000 0000 0000 0000    ................
128: 0000 0000 0000 0000 0000 0000 0000 0000    ................
144: 0000 0000 0000 0000 0000 0000 0000 0000    ................
160: 0000 0000 0000 0000 0000 0000 0000 0000    ................
176: 0000 0000 0000 0000 0000 0000 0000 0000    ................
192: 0000 0000 0000 0000 0000 0000 0000 0000    ................
208: 0000 0000 0000 0000 0000 0000 0000 0000    ................
224: 0000 0000 0000 0000 0000 0000 0000 0000    ................
240: 0000 0000 0000 0000 0000 0000 0000 0000    ................
256: 0000 0000 0000 0000 0000 0000 0000 0000    ................
272: 0000 0000 0000 6382 5363 3501 0536 04ac    ......c.Sc5..6..
288: 1500 0401 04ff ffff 0003 04c0 a8fc 011c    ................
304: 04c0 a8fc ff40 0964 6863 702e 7465 7374    .....@.dhcp.test
320: 3304 0000 0e10 0204 ffff c7c0 0404 ac15    3...............
336: 0004 0f10 736e 742e 6561 7374 2e73 756e    ....sem.example.
352: 2e63 6f6d 0604 ac15 0001 0c07 7768 6974    com.........whit
368: 652d 362b a602 0481 94ae 1b03 0861 746c    e-6+.........pac
384: 616e 7469 630a 0481 94ae 1b0b 0861 746c    ific.........pac
400: 616e 7469 630f 0578 7465 726d 0435 2f65    ific...xterm.5/e
416: 7870 6f72 742f 7332 382f 6261 7365 2e73    xport/sx2/bcvf.s
432: 3238 735f 776f 732f 6c61 7465 7374 2f53    2xs_btf/latest/S
448: 6f6c 6172 6973 5f38 2f54 6f6f 6c73 2f42    olaris_x/Tools/B
464: 6f6f 740c 202f 6578 706f 7274 2f73 3238    oot. /export/s2x
480: 2f62 6173 652e 7332 3873 5f77 6f73 2f6c    /bcvf.s2xs_btf/l
496: 6174 6573 7407 1b2f 706c 6174 666f 726d    atest../platform
512: 2f73 756e 346d 2f6b 6572 6e65 6c2f 756e    /sun4u/kernel/un
528: 6978 0807 4553 5435 4544 54ff              ix..EST5EDT.
```

Problèmes liés à des données de configuration DHCP inexactes

Si un client DHCP reçoit des informations de configuration de réseau inexactes, examinez les données du serveur DHCP. Vérifiez les valeurs des options dans les macros traitées par le serveur DHCP pour ce client. Il est possible, par exemple, que le nom du domaine NIS ou l'adresse IP du routeur soient incorrects.

Pour déterminer la source des erreurs, appliquez la procédure suivante :

- Etudiez les macros définies sur le serveur comme indiqué dans la section "Affichage des macros définies sur un serveur DHCP (gestionnaire DHCP)" à la page 403. Aidez-vous des informations de la section "Ordre de traitement des macros" à la page 319 pour déterminer les macros traitées automatiquement pour ce client.
- Vérifiez la table de réseau pour connaître la macro (le cas échéant) assignée à l'adresse IP du client en tant que macro de configuration. Pour plus d'informations, reportez-vous à la section "Traitement des adresses IP dans le service DHCP (liste des tâches)" à la page 385.
- Prenez note des options exécutées dans plusieurs macros. Assurez-vous que la valeur à attribuer à une option est définie dans la dernière macro traitée.
- Modifiez la ou les macros appropriée(s) pour être certain que la valeur transmise au client est celle qui convient. Voir "Modification des macros DHCP" à la page 404.

Problèmes liés aux noms d'hôtes fournis par les clients DHCP

Cette section décrit les problèmes posés parfois par les clients DHCP qui fournissent leurs propres noms d'hôtes en vue de les enregistrer auprès du DNS.

Le client DHCP ne demande par de nom d'hôte

Si votre client n'est pas un client DHCP, consultez la documentation du client pour savoir comment configurer le client afin de demander un nom d'hôte. S'il s'agit d'un client DHCP, reportez-vous à la section "Activation d'un client DHCPv4 pour qu'il demande un nom d'hôte spécifique" à la page 449.

Le client DHCP n'obtient pas le nom d'hôte demandé

La liste suivante récapitule les différents problèmes qu'un client risque d'avoir pour obtenir le nom d'hôte demandé et suggère les solutions appropriées.

Problème : Le client a accepté une offre d'un serveur DHCP qui n'émet pas de mises à jour DNS.

Solution : Si le client a accès à deux serveurs DHCP, ils doivent tous les deux être configurés pour fournir des mises à jour DNS. Pour plus d'informations sur la configuration du serveur DHCP et du serveur DNS, reportez-vous à la section "Activation des mises à jour DNS dynamiques par un serveur DHCP" à la page 365.

Pour savoir si le serveur DHCP est configuré pour fournir des mises à jour DNS :

1. Déterminez l'adresse IP du serveur DHCP du client. Sur le système client, utilisez `snoop` ou une autre application afin de capturer les paquets du réseau. Pour ce faire, reportez-vous à la section "Contrôle du trafic sur le réseau DHCP à l'aide de snoop" à la page 467 et effectuez la

procédure sur le client au lieu du serveur. Dans la sortie `snoop`, examinez l'identificateur du serveur DHCP pour connaître l'adresse IP du serveur.

2. Connectez-vous au système serveur DHCP pour vérifier si système est configuré pour assurer des mises à jour DNS. Tapez la commande suivante en tant que superutilisateur :

   `dhcpconfig -P`

   Si `UPDATE_TIMEOUT` est répertorié comme un paramètre serveur, cela signifie que le serveur DHCP est configuré pour proposer des mises à jour DNS.

3. Sur le serveur DNS, ouvrez le fichier `/etc/named.conf`. Recherchez le mot-clé `allow-update` dans la section `zone` du domaine approprié. Si le serveur autorise des mises à jour DNS par le serveur DHCP, l'adresse IP du serveur DHCP est indiquée dans le mot-clé `allow-update`.

Problème : Le client utilise l'option `FQDN` pour spécifier le nom d'hôte. DHCP ne prend actuellement pas en charge l'option `FQDN`, car elle ne fait pas partie officiellement du protocole DHCP.

Solution : Sur le serveur, utilisez `snoop` ou une autre application afin de capturer les paquets du réseau. Pour ce faire, reportez-vous à la section "Contrôle du trafic sur le réseau DHCP à l'aide de snoop" à la page 467. Dans la sortie `snoop`, recherchez l'option `FQDN` dans un des paquets provenant du client.

Configurez le client pour qu'il spécifie le nom d'hôte au moyen de l'option `Hostname`. `Hostname` a le code d'option 12. Reportez-vous à documentation du client pour obtenir des instructions.

Dans le cas d'un client Oracle Solaris, reportez-vous à la section "Activation d'un client DHCPv4 pour qu'il demande un nom d'hôte spécifique" à la page 449.

Problème : Le serveur DHCP qui propose une adresse au client ne connaît pas le domaine DNS du client.

Solution : Sur le serveur DHCP, recherchez l'option `DNSdmain` avec une valeur valide. Donnez à l'option `DNSdmain` un nom de domaine DNS correct au sein d'une macro traitée pour ce client. `DNSdmain` figure généralement dans la macro de réseau. Pour savoir comment changer les valeurs des options dans une macro, reportez-vous à la section "Modification des macros DHCP" à la page 404.

Problème : Le nom d'hôte demandé par le client correspond à une adresse IP non gérée par le serveur DHCP. Le serveur DHCP ne propose pas de mises à jour DNS pour les adresses IP non gérées par le serveur.

Solution : Vérifiez si `syslog` contient l'un des messages suivants émis par le serveur DHCP :

- `There is no` *n.n.n.n* `dhcp-network table for DHCP client's network.`
- `DHCP network record for` *n.n.n.n* `is unavailable, ignoring request.`

Configurez le client pour qu'il demande un autre nom. Reportez-vous à la section "Activation d'un client DHCPv4 pour qu'il demande un nom d'hôte spécifique" à la page 449. Choisissez un

nom mappé vers une adresse gérée par le serveur DHCP. Les mappages d'adresses sont répertoriés dans l'onglet Addresses du gestionnaire DHCP. Une autre solution consiste à choisir une adresse non mappée vers une adresse IP.

Problème : Le nom d'hôte demandé par le client correspond à une adresse IP qui n'est pas disponible actuellement. Il est possible que l'adresse soit en service, allouée à un autre client ou en cours de proposition à un autre client.

Solution : Vérifiez si `syslog` contient le message suivant émis par le serveur DHCP : `ICMP ECHO reply to OFFER candidate:` *n.n.n.n*.

Configurez le client pour qu'il choisisse un nom correspondant à une autre adresse IP. Vous pouvez également récupérer l'adresse à partir du client qui utilise l'adresse en question.

Problème : Le serveur DNS n'est pas configuré pour accepter les mises à jour à partir du serveur DHCP.

Solution : Examinez le contenu du fichier `/etc/named.conf` sur le serveur DNS. Recherchez l'adresse IP du serveur DHCP indiquée dans le mot-clé `allow-update` dans la section `zone` correspondant au domaine du serveur DHCP. Si l'adresse IP n'y figure pas, cela signifie que le serveur DNS n'est pas configuré pour accepter les mises à jour à partir du serveur DHCP.

Pour plus d'informations sur la configuration du serveur DNS, reportez-vous à la section "Activation de la mise à jour DNS dynamique pour les clients DHCP" à la page 367.

Si le serveur DHCP dispose de plusieurs interfaces, vous devrez éventuellement configurer le serveur DNS afin qu'il accepte les mises à jour provenant de toutes les adresses du serveur DHCP. Activez le débogage sur le serveur DNS pour vérifier si les mises à jour parviennent au serveur DNS. Si le serveur DNS reçoit des demandes de mise à jour, examinez la sortie du mode de débogage pour identifier l'origine du problème. Pour plus d'informations sur le mode de débogage DNS, reportez-vous à la page de manuel `in.named`.1M.

Problème : Les mises à jour DNS n'ont peut-être pas été réalisées dans le temps imparti. Les serveurs DHCP ne renvoient pas les noms d'hôtes aux clients si les mises à jour DNS n'ont pas été effectuées dans les délais prévus. Les tentatives de mise à jour DNS continuent néanmoins.

Solution : Servez-vous de la commande `nslookup` pour déterminer si les mises à jour ont été accomplies correctement. Voir la page de manuel `nslookup(1M)`.

Supposons, par exemple, que le domaine DNS soit `hills.example.org` et que l'adresse IP du serveur DNS soit `10.76.178.11`. Le nom d'hôte que le client souhaite enregistrer est `cathedral`. Voici la commande qui permettrait de savoir si `cathedral` a été enregistré auprès de ce serveur DNS :

```
nslookup cathedral.hills.example.org 10.76.178.11
```

Si les mises à jour ont été menées à terme, mais pas dans le temps imparti, il convient d'augmenter le délai fixé. Voir "Activation de la mise à jour DNS dynamique pour les clients DHCP" à la page 367. Lors de cette procédure, augmentez le délai d'attente (en secondes) des réponses provenant du serveur DNS avant expiration.

◆ ◆ ◆ CHAPITRE 18

Commandes et fichiers DHCP (référence)

Ce chapitre décrit les relations entre les commandes DHCP et les fichiers DHCP. Il n'explique pas, cependant, comment utiliser les commandes.

Ce chapitre contient les informations suivantes :

Commandes DHCP

Le tableau suivant présente les commandes prévues pour gérer le protocole DHCP sur votre réseau.

TABLEAU 18–1 Commandes utilisées dans DHCP

Commande	Description	Page de manuel
`dhtadm`	Permet d'apporter des modifications aux options et macros dans le fichier `dhcptab`. Cette commande est particulièrement utile dans les scripts que vous créez pour automatiser les changements de vos informations DHCP. Associez la commande `dhtadm` à l'option `-P` et traitez la sortie avec la commande `grep` de manière à rechercher des valeurs d'option particulières dans la table `dhcptab`.	`dhtadm`(1M)
`pntadm`	Permet d'apporter des modifications aux tables de réseau DHCP établissant la correspondance entre ID de client et adresses IP et éventuellement d'associer les données de configuration aux adresses IP.	`pntadm`(1M)

TABLEAU 18–1 Commandes utilisées dans DHCP *(Suite)*

Commande	Description	Page de manuel
`dhcpconfig`	Permet de configurer des serveurs DHCP et les agents de relais BOOTP et d'annuler la configuration lorsque cela est nécessaire. Cette commande sert également à effectuer une conversion vers un autre format de magasin de données et à importer/exporter les données de configuration DHCP.	`dhcpconfig`(1M)
`in.dhcpd`	Correspond au démon du serveur DHCP exécuté au démarrage du système. Il est déconseillé de lancer directement le démon du serveur. Pour démarrer ou arrêter le démon, vous pouvez au choix utiliser le gestionnaire DHCP, la commande `svcadm` ou la commande `dhcpconfig`. Faites appel directement au démon uniquement lorsque vous souhaitez exécuter le serveur en mode de débogage en vue de résoudre des problèmes.	`in.dhcpd`(1M)
`dhcpmgr`	Correspond au gestionnaire DHCP, interface graphique (IG) utilisée spécialement pour configurer et gérer le service DHCP. Le gestionnaire DHCP est l'outil d'administration DHCP recommandé.	`dhcpmgr`(1M)
`ifconfig`	Permet d'attribuer des adresses IP aux interfaces réseau et/ou de configurer les paramètres d'interface réseau au démarrage du système. Sur un client DHCP, la commande `ifconfig` permet de démarrer le service DHCP pour obtenir les paramètres nécessaires (y compris l'adresse IP) à la configuration d'une interface réseau.	`ifconfig`(1M)
`dhcpinfo`	Permet aux scripts de démarrage système des systèmes clients Oracle Solaris d'obtenir un certain nombre d'informations (comme le nom de l'hôte) à partir du démon du client DHCP `dhcpagent`. Vous pouvez également utiliser la commande `dhcpinfo` dans des scripts ou depuis la ligne de commande afin d'obtenir les valeurs des paramètres qui vous intéressent.	`dhcpinfo`(1)
`snoop`	Permet de capturer et d'afficher le contenu des paquets transmis sur le réseau. `snoop` est très pratique pour résoudre les problèmes liés au service DHCP.	`snoop`(1M)
`dhcpagent`	Correspond au démon client DHCP prévu pour implémenter le côté client du protocole DHCP.	`dhcpagent`(1M)

Exécution des commandes DHCP au sein de scripts

Les commandes `dhcpconfig`, `dhtadm` et `pntadm` sont optimisées pour les scripts. La commande `pntadm` est notamment utile pour créer un grand nombre d'entrées d'adresses IP dans une table de réseau DHCP. L'exemple de script suivant utilise la commande `pntadm` en mode de traitement par lots pour générer des adresses IP.

EXEMPLE 18–1 Script `addclient.ksh` avec la commande `pntadm`

```
#! /usr/bin/ksh
#
# This script utilizes the pntadm batch facility to add client entries
# to a DHCP network table. It assumes that the user has the rights to
# run pntadm to add entries to DHCP network tables.

#
# Based on the nsswitch setting, query the netmasks table for a netmask.
# Accepts one argument, a dotted IP address.
#
get_netmask()
{
    MTMP=‘getent netmasks ${1} | awk ’{ print $2 }’‘
    if [ ! -z "${MTMP}" ]
    then
        print - ${MTMP}
    fi
}

#
# Based on the network specification, determine whether or not network is
# subnetted or supernetted.
# Given a dotted IP network number, convert it to the default class
# network.(used to detect subnetting). Requires one argument, the
# network number. (e.g. 10.0.0.0) Echos the default network and default
# mask for success, null if error.
#
get_default_class()
{
    NN01=${1%%.*}
    tmp=${1#*.}
    NN02=${tmp%%.*}
    tmp=${tmp#*.}
    NN03=${tmp%%.*}
    tmp=${tmp#*.}
    NN04=${tmp%%.*}
    RETNET=""
    RETMASK=""

    typeset -i16 ONE=10#${1%%.*}
    typeset -i10 X=$((${ONE}&16#f0))
    if [ ${X} -eq 224 ]
    then
        # Multicast
        typeset -i10 TMP=$((${ONE}&16#f0))
        RETNET="${TMP}.0.0.0"
        RETMASK="240.0.0.0"
    fi
    typeset -i10 X=$((${ONE}&16#80))
    if [ -z "${RETNET}" -a ${X} -eq 0 ]
    then
        # Class A
        RETNET="${NN01}.0.0.0"
        RETMASK="255.0.0.0"
    fi
    typeset -i10 X=$((${ONE}&16#c0))
    if [ -z "${RETNET}" -a ${X} -eq 128 ]
```

EXEMPLE 18–1 Script `addclient.ksh` avec la commande `pntadm` *(Suite)*

```
    then
        # Class B
        RETNET="${NN01}.${NN02}.0.0"
        RETMASK="255.255.0.0"
    fi
    typeset -i10 X=$((${ONE}&16#e0))
    if [ -z "${RETNET}" -a ${X} -eq 192 ]
    then
        # Class C
        RETNET="${NN01}.${NN02}.${NN03}.0"
        RETMASK="255.255.255.0"
    fi
    print - ${RETNET} ${RETMASK}
    unset NNO1 NNO2 NNO3 NNO4 RETNET RETMASK X ONE
}

#
# Given a dotted form of an IP address, convert it to its hex equivalent.
#
convert_dotted_to_hex()
{
    typeset -i10 one=${1%%.*}
    typeset -i16 one=${one}
    typeset -Z2 one=${one}
    tmp=${1#*.}

    typeset -i10 two=${tmp%%.*}
    typeset -i16 two=${two}
    typeset -Z2 two=${two}
    tmp=${tmp#*.}

    typeset -i10 three=${tmp%%.*}
    typeset -i16 three=${three}
    typeset -Z2 three=${three}
    tmp=${tmp#*.}

    typeset -i10 four=${tmp%%.*}
    typeset -i16 four=${four}
    typeset -Z2 four=${four}

     hex=‘print - ${one}${two}${three}${four} | sed -e ’s/#/0/g’‘
     print - 16#${hex}
     unset one two three four tmp
}

#
# Generate an IP address given the network address, mask, increment.
#
get_addr()
{
    typeset -i16 net=‘convert_dotted_to_hex ${1}‘
    typeset -i16 mask=‘convert_dotted_to_hex ${2}‘
    typeset -i16 incr=10#${3}

    # Maximum legal value - invert the mask, add to net.
    typeset -i16 mhosts=~${mask}
```

EXEMPLE 18–1 Script `addclient.ksh` avec la commande `pntadm` *(Suite)*

```
    typeset -i16 maxnet=${net}+${mhosts}

    # Add the incr value.
    let net=${net}+${incr}

    if [ $((${net} < ${maxnet})) -eq 1 ]
    then
        typeset -i16 a=${net}\&16#ff000000
        typeset -i10 a="${a}>>24"

        typeset -i16 b=${net}\&16#ff0000
        typeset -i10 b="${b}>>16"

        typeset -i16 c=${net}\&16#ff00
        typeset -i10 c="${c}>>8"

        typeset -i10 d=${net}\&16#ff
        print - "${a}.${b}.${c}.${d}"
    fi
    unset net mask incr mhosts maxnet a b c d
}

# Given a network address and client address, return the index.
client_index()
{
    typeset -i NNO1=${1%%.*}
    tmp=${1#*.}
    typeset -i NNO2=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO3=${tmp%%.*}
    tmp=${tmp#*.}
    typeset -i NNO4=${tmp%%.*}

    typeset -i16 NNF1
    let NNF1=${NNO1}
    typeset -i16 NNF2
    let NNF2=${NNO2}
    typeset -i16 NNF3
    let NNF3=${NNO3}
    typeset -i16 NNF4
    let NNF4=${NNO4}
    typeset +i16 NNF1
    typeset +i16 NNF2
    typeset +i16 NNF3
    typeset +i16 NNF4
    NNF1=${NNF1#16\#}
    NNF2=${NNF2#16\#}
    NNF3=${NNF3#16\#}
    NNF4=${NNF4#16\#}
    if [ ${#NNF1} -eq 1 ]
    then
        NNF1="0${NNF1}"
    fi
    if [ ${#NNF2} -eq 1 ]
    then
        NNF2="0${NNF2}"
```

EXEMPLE 18–1 Script `addclient.ksh` avec la commande `pntadm` *(Suite)*

```
fi
if [ ${#NNF3} -eq 1 ]
then
    NNF3="0${NNF3}"
fi
if [ ${#NNF4} -eq 1 ]
then
    NNF4="0${NNF4}"
fi
typeset -i16 NN
let NN=16#${NNF1}${NNF2}${NNF3}${NNF4}
unset NNF1 NNF2 NNF3 NNF4

typeset -i NNO1=${2%%.*}
tmp=${2#*.}
typeset -i NNO2=${tmp%%.*}
tmp=${tmp#*.}
typeset -i NNO3=${tmp%%.*}
tmp=${tmp#*.}
typeset -i NNO4=${tmp%%.*}
typeset -i16 NNF1
let NNF1=${NNO1}
typeset -i16 NNF2
let NNF2=${NNO2}
typeset -i16 NNF3
let NNF3=${NNO3}
typeset -i16 NNF4
let NNF4=${NNO4}
typeset +i16 NNF1
typeset +i16 NNF2
typeset +i16 NNF3
typeset +i16 NNF4
NNF1=${NNF1#16\#}
NNF2=${NNF2#16\#}
NNF3=${NNF3#16\#}
NNF4=${NNF4#16\#}
if [ ${#NNF1} -eq 1 ]
then
    NNF1="0${NNF1}"
fi
if [ ${#NNF2} -eq 1 ]
then
    NNF2="0${NNF2}"
fi
if [ ${#NNF3} -eq 1 ]
then
    NNF3="0${NNF3}"
fi
if [ ${#NNF4} -eq 1 ]
then
    NNF4="0${NNF4}"
fi
typeset -i16 NC
let NC=16#${NNF1}${NNF2}${NNF3}${NNF4}
typeset -i10 ANS
let ANS=${NC}-${NN}
```

EXEMPLE 18–1 Script addclient.ksh avec la commande pntadm *(Suite)*

```
    print - $ANS
}

#
# Check usage.
#
if [ "$#" != 3 ]
then
    print "This script is used to add client entries to a DHCP network"
    print "table by utilizing the pntadm batch facilty.\n"
    print "usage: $0 network start_ip entries\n"
    print "where: network is the IP address of the network"
        print "       start_ip is the starting IP address \n"
        print "       entries is the number of the entries to add\n"
    print "example: $0 10.148.174.0 10.148.174.1 254\n"
    return
fi

#
# Use input arguments to set script variables.
#
NETWORK=$1
START_IP=$2
typeset -i STRTNUM=‘client_index ${NETWORK} ${START_IP}‘
let ENDNUM=${STRTNUM}+$3
let ENTRYNUM=${STRTNUM}
BATCHFILE=/tmp/batchfile.$$
MACRO=‘uname -n‘

#
# Check if mask in netmasks table. First try
# for network address as given, in case VLSM
# is in use.
#
NETMASK=‘get_netmask ${NETWORK}‘
if [ -z "${NETMASK}" ]
then
    get_default_class ${NETWORK} | read DEFNET DEFMASK
    # use the default.
    if [ "${DEFNET}" != "${NETWORK}" ]
    then
        # likely subnetted/supernetted.
        print - "\n\n###\tWarning\t###\n"
        print - "Network ${NETWORK} is netmasked, but no entry was found  \n
              in the 'netmasks' table; please update the 'netmasks'  \n
              table in the appropriate nameservice before continuing. \n
              (See /etc/nsswitch.conf.) \n" >&2
        return 1
    else
        # use the default.
        NETMASK="${DEFMASK}"
    fi
fi

#
# Create a batch file.
```

EXEMPLE 18–1 Script `addclient.ksh` avec la commande `pntadm` *(Suite)*

```
#
print -n "Creating batch file "
while [ ${ENTRYNUM} -lt ${ENDNUM} ]
do
    if [ $((${ENTRYNUM}-${STRTNUM}))%50 -eq 0 ]
    then
        print -n "."
    fi

    CLIENTIP=‘get_addr ${NETWORK} ${NETMASK} ${ENTRYNUM}‘
    print "pntadm -A ${CLIENTIP} -m ${MACRO} ${NETWORK}" >> ${BATCHFILE}
    let ENTRYNUM=${ENTRYNUM}+1
done
print " done.\n"

#
# Run pntadm in batch mode and redirect output to a temporary file.
# Progress can be monitored by using the output file.
#
print "Batch processing output redirected to ${BATCHFILE}"
print "Batch processing started."

pntadm -B ${BATCHFILE} -v > /tmp/batch.out 2 >&1

print "Batch processing completed."
```

Fichiers utilisés par le service DHCP

Le tableau suivant présente les différents fichiers associés à DHCP.

TABLEAU 18–2 Fichiers et tables utilisés par les démons et les commandes DHCP

Nom du fichier ou de la table	Description	Page de manuel
`dhcptab`	Terme générique désignant la table des données de configuration DHCP stockées sous forme d'options avec des valeurs attribuées, lesquelles sont ensuite regroupées dans des macros. Le nom de la table `dhcptab` et son emplacement sont déterminés par le magasin de données réservé aux informations DHCP.	`dhcptab(4)`
Table de réseau DHCP	Établit la correspondance entre les adresses IP et les ID de client et les options de configuration. Les tables de réseau DHCP sont nommées d'après l'adresse IP du réseau (`10.21.32.0`, par exemple). Il n'existe aucun fichier appelé `dhcp_network`. Le nom et l'emplacement des tables de réseau DHCP sont fonction du magasin de données utilisé pour les informations DHCP.	`dhcp_network(4)`

TABLEAU 18–2 Fichiers et tables utilisés par les démons et les commandes DHCP *(Suite)*

Nom du fichier ou de la table	Description	Page de manuel
`dhcpsvc.conf`	Stocke les options de démarrage du démon DHCP et les informations du magasin de données. Il est interdit d'éditer ce fichier de façon manuelle. Servez-vous de la commande `dhcpconfig` pour changer les options de démarrage.	`dhcpsvc.conf`(4)
`nsswitch.conf`	Indique l'emplacement des bases de données de services de noms et l'ordre de recherche des services de noms pour différents types d'information. Le fichier `nsswitch.conf` est consulté lors de la configuration d'un serveur DHCP dans le but d'obtenir des informations de configuration précises. Il figure dans le répertoire `/etc`.	`nsswitch.conf`(4)
`resolv.conf`	Contient les informations permettant la résolution des requêtes DNS. Ce fichier est consulté lors de la configuration du serveur DHCP pour vérifier le domaine DNS et le serveur DNS. Il figure dans le répertoire `/etc`.	`resolv.conf`(4)
`dhcp.`*interface*	Implique l'utilisation du service DHCP sur l'interface réseau du client spécifiée dans le nom du fichier `dhcp.`*interface*. La présence d'un fichier appelé `dhcp.qe0` indique, par exemple, que le service DHCP doit être utilisé sur l'interface `qe0`. Le fichier `dhcp.` *interface* peut éventuellement contenir des commandes transmises en tant qu'options à la commande `ifconfig`, laquelle permet de démarrer DHCP sur le client. Le fichier figure dans le répertoire `/etc` sur les systèmes clients DHCP	Aucune page de manuel spécifique, voir `dhcp`(5)
interface`.dhc`	Contient les paramètres de configuration obtenus à partir de DHCP pour l'interface réseau indiquée. Le client met en mémoire cache les données de configuration actuelles dans le fichier `/etc/dhcp/`*interface*`.dhc` dès que cesse le bail de l'adresse IP de l'interface. En cas d'utilisation du service DHCP sur l'interface `qe0`, par exemple, `dhcpagent` met en mémoire cache les données de configuration dans `/etc/dhcp/qe0.dhc`. Lors du prochain démarrage du service DHCP sur l'interface, le client adresse une requête au serveur DHCP afin d'exploiter la configuration mise en mémoire cache (à condition que le bail n'ait pas expiré). Si le serveur DHCP rejette la requête, le client lance le processus standard de négociation du bail DHCP.	Aucune page de manuel spécifique, voir `dhcpagent`(1M)
`dhcpagent`	Définit les valeurs des paramètres pour le démon client `dhcpagent`. Le chemin d'accès au fichier est `/etc/default/dhcpagent`. Pour plus d'informations sur les paramètres, reportez-vous au fichier `/etc/default/dhcpagent` ou à la page de manuel `dhcpagent`(1M).	`dhcpagent`(1M)

TABLEAU 18–2 Fichiers et tables utilisés par les démons et les commandes DHCP *(Suite)*

Nom du fichier ou de la table	Description	Page de manuel
DHCP `inittab`	Définit des aspects des codes d'options DHCP, tels que le type de données, et assigne des étiquettes comme mnémoniques. Pour plus d'informations sur la syntaxe du fichier, voir la page de manuel `dhcp_inittab(4)`. Au niveau du client, les informations provenant du fichier `/etc/dhcp/inittab` sont utilisées par `dhcpinfo` pour aider les utilisateurs à mieux comprendre la signification des informations. Au niveau du système du serveur DHCP, c'est le démon DHCP et les outils de gestion qui utilisent ce fichier pour obtenir des informations relatives aux options DHCP. Le fichier `/etc/dhcp/inittab` remplace le fichier `/etc/dhcp/dhcptags` utilisé dans les versions précédentes. Pour en savoir plus à ce sujet, reportez-vous à la section "Informations relatives aux options DHCP" à la page 488.	`dhcp_inittab(4)`

Informations relatives aux options DHCP

Auparavant, les informations ayant trait aux options DHCP étaient stockées à différents endroits, y compris la table `dhcptab` du serveur, le fichier `dhcptags` des clients et les tables internes de divers programmes. À partir de la version Solaris 8, ces informations sont systématiquement consolidées dans le fichier `/etc/dhcp/inittab`. Pour plus d'informations sur ce fichier, reportez-vous à la page de manuel `dhcp_inittab(4)`.

Le client DHCP utilise le fichier DHCP `inittab` en guise de remplacement du fichier `dhcptags`. Il se sert de ce fichier pour obtenir des informations sur les codes d'options reçus dans un paquet DHCP. Les programmes `in.dhcpd`, `snoop` et `dhcpmgr` sur le serveur DHCP utilisent également le fichier `inittab`.

Vérification de l'impact éventuel du commutateur sur votre site

La plupart des sites ayant recours à DHCP ne sont *pas* concernés par le commutateur dans le fichier `/etc/dhcp/inittab`. Votre site est concerné si vous remplissez toutes les conditions suivantes :

- Vous avez l'intention d'effectuer une mise à niveau à partir d'une version Oracle Solaris antérieure à Solaris 8.
- Vous avez défini auparavant de nouvelles options DHCP.
- Vous avez modifié le fichier `/etc/dhcp/dhcptags` et souhaitez conserver les changements apportés.

Lors de la mise à niveau, le journal de mise à niveau vous signale que le fichier `dhcptags` avait subi des modifications et que vous devez, par conséquent, apporter des changements au fichier DHCP `inittab`.

Différences entre les fichiers `dhcptags` et `inittab`

Le fichier `inittab` contient plus d'informations que le fichier `dhcptags`. Le fichier `inittab` utilise également une syntaxe différente.

Voici à quoi ressemble une entrée dans le fichier `dhcptags` :

```
33 StaticRt - IPList Static_Routes
```

`33` est le code numérique transmis dans le paquet DHCP. `StaticRt` est le nom de l'option. `IPList` indique que le type de données pour `StaticRt` doit correspondre à une liste d'adresses IP. `Static_Routes` représente la version descriptive du nom.

Le fichier `inittab` se compose d'enregistrements d'une seule ligne décrivant chaque option. Le format est similaire à celui prévu pour définir les symboles dans `dhcptab`. Le tableau suivant décrit la syntaxe du fichier `inittab` .

Option	Description
nom-option	Nom de l'option. Le nom de l'option doit être unique dans sa catégorie et ne doit pas entrer en conflit avec les autres noms d'option dans les catégories Standard, Site et Fournisseur. Vous ne pouvez pas, par exemple, définir deux options Site ayant le même nom. Il n'est pas non plus permis de créer une option Site avec un nom identique à celui d'une option Standard.
catégorie	Identifie l'espace de noms auquel l'option appartient. Il existe cinq possibilités : Standard, Site, Vendor (Fournisseur), Field (Champ) ou Internal (Interne).
code	Identifie l'option lors de sa transmission sur le réseau. Dans la plupart des cas, le code identifie sans ambiguïté l'option, au sein d'une même catégorie. Cependant, dans le cas des catégories internes telles que Champ ou Interne, il peut avoir une autre signification. Le code ne doit pas nécessairement être unique au sens général du terme. Il lui suffit de remplir les conditions suivantes : être unique au sein de la catégorie de l'option et ne pas être en conflit avec les codes des catégories Standard et Site.
type	Décrit les données associées à cette option. Les types autorisés sont : IP, ASCII, Octet, Boolean, Unumber8, Unumber16, Unumber32, Unumber64, Snumber8, Snumber16, Snumber32 et Snumber64. Dans le cas de nombres, l'initiale U ou S indique respectivement qu'il s'agit d'un nombre non signé ou signé. Les chiffres de fin indiquent le nombre de bits de

codage du nombre. Unumber8 signale, par exemple, un nombre non signé à 8 bits. Le type ne respecte pas la casse.

granularité Décrit le nombre d'unités de données nécessaires pour représenter une valeur entière pour cette option.

maximum Décrit le nombre de valeurs entières autorisées pour cette option. 0 indique un nombre infini.

consommateurs Décrit les programmes susceptibles d'exploiter ces informations. Vous êtes tenu de configurer les consommateurs au format `sdmi`, où :

`s` `snoop`

`d` `in.dhcpd`

`m` `dhcpmgr`

`i` `dhcpinfo`

Voici à quoi ressemble une entrée `inittab` :

```
StaticRt - Standard, 33, IP, 2, 0, sdmi
```

Cette entrée décrit une option appelée `StaticRt`. L'option se trouve dans la catégorie Standard et son code est 33. Les données attendues correspondent à un nombre potentiellement infini de paires d'adresses IP car le type est `IP`, la granularité est `2` et le nombre maximum est infini (`0`). Les consommateurs de cette option sont `sdmi` : `snoop`, `in.dhcpd`, `dhcpmgr` et `dhcpinfo`.

Conversion d'entrées `dhcptags` au format `inittab`

Si vous aviez ajouté précédemment des entrées à votre fichier `dhcptags`, vous devez insérer les entrées correspondantes dans le nouveau fichier `inittab` pour continuer à utiliser les options ajoutées à votre site. L'exemple suivant montre la façon dont une entrée `dhcptags` peut être exprimée au format `inittab` .

Supposons que vous ayez ajouté l'entrée `dhcptags` suivante pour des télécopieurs reliés au réseau :

```
128 FaxMchn - IP Fax_Machine
```

Le code `128` signifie que l'option doit appartenir à la catégorie Site. Le nom de l'option est `FaxMchn` et le type de données est `IP`.

L'entrée `inittab` correspondante pourrait ressembler à la suivante :

```
FaxMchn SITE, 128, IP, 1, 1, sdmi
```

La granularité (1) et le maximum (1) indiquent qu'une adresse IP est attendue pour cette option.

PARTIE IV

IPsec

Cette section met l'accent sur la sécurité à l'échelle du réseau. L'architecture IPsec (IP security) protège le réseau au niveau du paquet. IKE (Internet Key Exchange, échange de clé Internet) gère les clés pour IPsec. IP Filter fournit un pare-feu.

◆ ◆ ◆ CHAPITRE 19

Architecture IPsec (présentation)

L'architecture IPsec (IP security) offre la protection cryptographique des datagrammes IP dans les paquets réseau IPv4 et IPv6.

Le présent chapitre contient les informations suivantes :

Pour implémenter IPsec sur votre réseau, reportez-vous au Chapitre 20, "Configuration d'IPsec (tâches)". Pour des informations de référence, reportez-vous au Chapitre 21, "Architecture IPsec (référence)".

Nouveautés IPsec

Solaris 10 4/09 : À partir de cette version, l'utilitaire de gestion des services (SMF) gère IPsec en tant qu'ensemble de services.

Par défaut, deux services IPsec sont activés lors de l'initialisation du système :

- `svc:/network/ipsec/policy:default`
- `svc:/network/ipsec/ipsecalgs:default`

Par défaut, les services de gestion des clés sont désactivés à l'initialisation du système :

- `svc:/network/ipsec/manual-key:default`
- `svc:/network/ipsec/ike:default`

Pour activer les stratégies IPsec sous SMF, effectuez les étapes suivantes :

1. Ajoutez des entrées de stratégie IPsec au fichier `ipsecinit.conf`.
2. Configurez le protocole IKE (Internet Key Exchange) ou configurez manuellement les clés.
3. Actualisez le service de stratégie IPsec.
4. Activez le service de gestion des clés.

Pour plus d'informations sur l'utilitaire SMF, reportez-vous au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base*. Voir aussi les pages de manuel `smf(5)` et `svcadm(1M)`.

À partir de cette version, les commandes `ipsecconf` et `ipseckey` ont une option `-c` permettant de vérifier la syntaxe de leurs fichiers de configuration respectifs. De plus, le profil de droits Network IPsec Management est fourni pour administrer IPsec et IKE.

Solaris 10 7/07 : À partir de cette version, IPsec implémente entièrement les tunnels en mode Tunnel et les utilitaires de prise en charge des tunnels sont modifiés.

- IPsec implémente les tunnels en mode Tunnel pour les réseaux privés virtuels (VPN, Virtual Private Network). En mode Tunnel, IPsec prend en charge plusieurs clients derrière un NAT unique. En mode Tunnel, IPsec est interopérable avec les implémentations des tunnels IP-in-IP d'autres constructeurs. IPsec prend toujours en charge les tunnels en mode Transport, ce qui garantit sa compatibilité avec les versions Oracle Solaris antérieures.
- La syntaxe de création d'un tunnel est simplifiée. La commande `ipsecconf` a été étendue à la gestion de la stratégie IPsec. La commande `ifconfig` ne permet plus la gestion de la stratégie IPsec.
- À partir de cette version, le fichier `/etc/ipnodes` est supprimé. Configurez les adresses de réseau IPv6 à l'aide du fichier `/etc/hosts`.

Solaris10 1/06 : à partir de cette version, IKE est entièrement compatible avec la prise en charge NAT-Traversal comme décrit dans le document RFC 3947 et RFC 3948. Les opérations IKE utilisent la bibliothèque PKCS #11 à partir de la structure cryptographique, ce qui améliore les performances.

La structure cryptographique fournit un fichier keystore de clés softtoken pour les applications qui utilisent le métaconnecteur. Lorsque IKE utilise le métaconnecteur, vous avez la possibilité de stocker les clés sur un disque, sur une carte connectée ou dans le fichier keystore de clés softtoken.

- Pour utiliser le fichier keystore de clés softtoken, reportez-vous à la page de manuel `cryptoadm(1M)`.
- Vous trouverez une liste complète des nouvelles fonctionnalités de Solaris et la description des différentes versions de Solaris dans le guide *Nouveautés apportées à Oracle Solaris 10 8/11*.

Introduction à IPsec

Pour protéger les paquets IP, IPsec les chiffre et/ou les authentifie. IPsec s'exécute au sein du module IP, bien en dessous de la couche d'application. Par conséquent, une application Internet peut tirer profit d'IPsec sans pour autant avoir à modifier sa configuration. Une utilisation à bon escient d'IPsec en fait un outil efficace de sécurisation du trafic réseau.

La protection IPsec implique cinq composants principaux :

- **Protocoles de sécurité :** les mécanismes de protection de datagramme IP. L'en-tête d'authentification (AH, Authentication Header) signe les paquets IP et garantit leur intégrité. Bien que le contenu du datagramme ne soit pas chiffré, le destinataire est sûr que le contenu du paquet n'a subi aucune modification et que l'expéditeur a envoyé les paquets. protocole ESP chiffre les données IP et obscurcit, par conséquent, le contenu des paquets lors de leur transmission. ESP garantit également l'intégrité des données par le biais d'une option d'algorithme d'authentification.
- **SADB (Security Associations Database, base de données des associations de sécurité) :** base de données qui associe un protocole de sécurité à une adresse IP de destination et un numéro d'indexation. Ce numéro d'indexation est appelé index du paramètre de sécurité. Ces trois éléments (protocole de sécurité, adresse de destination et SPI) identifient un seul paquet IPsec légitime. La base de données garantit que le paquet protégé est reconnu par le récepteur à son arrivée. Elle permet également au récepteur de déchiffrer la communication, de vérifier que les paquets n'ont pas été altérés, de rassembler les paquets et de livrer les paquets à leur destination finale.
- **Gestion des clés :** génération et distribution des clés des algorithmes cryptographiques et de SPI.
- **Mécanismes de sécurité :** algorithmes de chiffrement et d'authentification qui protègent les données des datagrammes IP.
- **SPD (Security Policy Database, base de données de stratégie de sécurité) :** base de données indiquant le niveau de protection à appliquer à un paquet. La base de données SPD filtre le trafic IP et identifie le mode de traitement des paquets. Un paquet peut être rejeté, passé au clair ou protégé à l'aide d'IPsec. En ce qui concerne les paquets sortants, les bases de

données SPD et SADB déterminent le niveau de protection à appliquer. Pour les paquets entrants, la base de données SPD permet de déterminer l'acceptabilité du niveau de protection. Si le paquet est protégé par IPsec, une consultation de la base de données SPD est effectuée après déchiffrement et vérification du paquet.

IPsec applique les mécanismes de sécurité aux datagrammes IP circulant en direction de l'adresse IP de destination. À l'aide des informations contenues dans la base de données SADB, le destinataire vérifie que les paquets entrants sont légitimes et les déchiffre. Les applications peuvent appeler IPsec pour appliquer les mécanismes aux datagrammes IP au niveau de chaque socket.

Notez que le comportement des sockets diffère en fonction des ports :

- Les SA par socket remplacent leur entrée de port correspondante dans la base de données SPD.
- Par ailleurs, lorsque la stratégie IPsec est appliquée à un port sur lequel un socket est déjà connecté, le trafic qui utilise ce socket ne bénéficie pas de la protection IPsec.

  En revanche, les sockets ouverts sur un port *après* l'application de la stratégie IPsec en bénéficient aussi.

RFC IPsec

Le groupe IETF (Internet Engineering Task Force) a publié un certain nombre de documents RFC (Request for Comments, demande de commentaires) décrivant l'architecture de sécurité de la couche IP. Tous les RFC constituent la propriété intellectuelle de l'Internet Society. Pour plus d'informations sur les RFC, reportez-vous au site Web `http://ietf.org/`. Les références de sécurité IP les plus générales sont couvertes par les RFC suivants :

- RFC 2411, "IP Security Document Roadmap", novembre 1998 ;
- RFC 2401, "Security Architecture for the Internet Protocol", novembre 1998 ;
- RFC 2402, "IP Authentication Header", novembre 1998 ;
- RFC 2406, "IP Encapsulating Security Payload (ESP)", novembre 1998 ;
- RFC 2408, "Internet Security Association and Key Management Protocol (ISAKMP)", novembre 1998 ;
- RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP", novembre 1998 ;
- RFC 2409, "The Internet Key Exchange (IKE)", novembre 1998 ;
- RFC 3554, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec", juillet 2003 [non implémenté dans la version Solaris10].

Terminologie IPsec

Les documents RFC IPsec définissent un certain nombre de termes qui s'avèrent utiles lors de l'implémentation d'IPsec sur des systèmes. Les tableaux suivants répertorient les termes IPsec, leur acronyme et leur définition. Le Tableau 22–1 dresse la liste des termes de négociation de clé.

TABLEAU 19–1 Termes IPsec, acronymes et usages

Terme IPsec	Acronymes	Définition
Association de sécurité	SA (Security Association)	Connexion unique entre deux nœuds sur un réseau. La connexion est définie par les trois éléments suivants : un protocole de sécurité, un index de paramètre de sécurité et une destination IP. La destination IP peut être une adresse IP ou un socket.
Base de données d'associations de sécurité	SADB (Security Associations Database)	Base de données contenant toutes les associations de sécurité actives.
Index de paramètre de sécurité	SPI (Security Parameter Index)	Valeur d'indexation d'une association de sécurité. Une SPI est une valeur 32 bits qui différencie les SA partageant une destination IP et un protocole de sécurité.
Base de données de stratégie de sécurité	SPD (Security Policy Database)	Base de données déterminant si les paquets entrants et sortants présentent le niveau de protection spécifié.
Échange de clés		Processus de génération de clés pour les algorithmes cryptographiques asymétriques. Les principales méthodes utilisées sont les protocoles RSA et Diffie-Hellman.
Protocole Diffie-Hellman	DH	Protocole d'échange de clés impliquant la génération et l'authentification de clés et souvent appelé *échange de clés authentifiées*.
Protocole RSA	RSA	Protocole d'échange de clés impliquant la génération et la distribution de clés, Ce protocole porte le nom de ses trois créateurs : Rivest, Shamir et Adleman.
Association de sécurité Internet et protocole de gestion des clés	ISAKMP (Internet Security Association and Key Management Protocol)	Structure courante d'établissement du format des attributs SA, et de négociation, modification et suppression des SA. ISAKMP est le standard IETF de gestion des SA IPsec.

Flux de paquets IPsec

La Figure 19–1 illustre la procédure suivie par un paquet adressé IP, en tant que partie intégrante d'un datagramme IP lors d'un appel IPsec sur un paquet sortant. Le diagramme du flux indique l'endroit auquel les en-têtes d'authentification AH et les associations de sécurité ESP sont susceptibles d'être appliqués au paquet. Les méthodes d'application de ces entités et de sélection des algorithmes sont décrites dans les sections suivantes.

La Figure 19–2 illustre le processus entrant IPsec.

FIGURE 19–1 Application d'IPsec au processus de paquet sortant

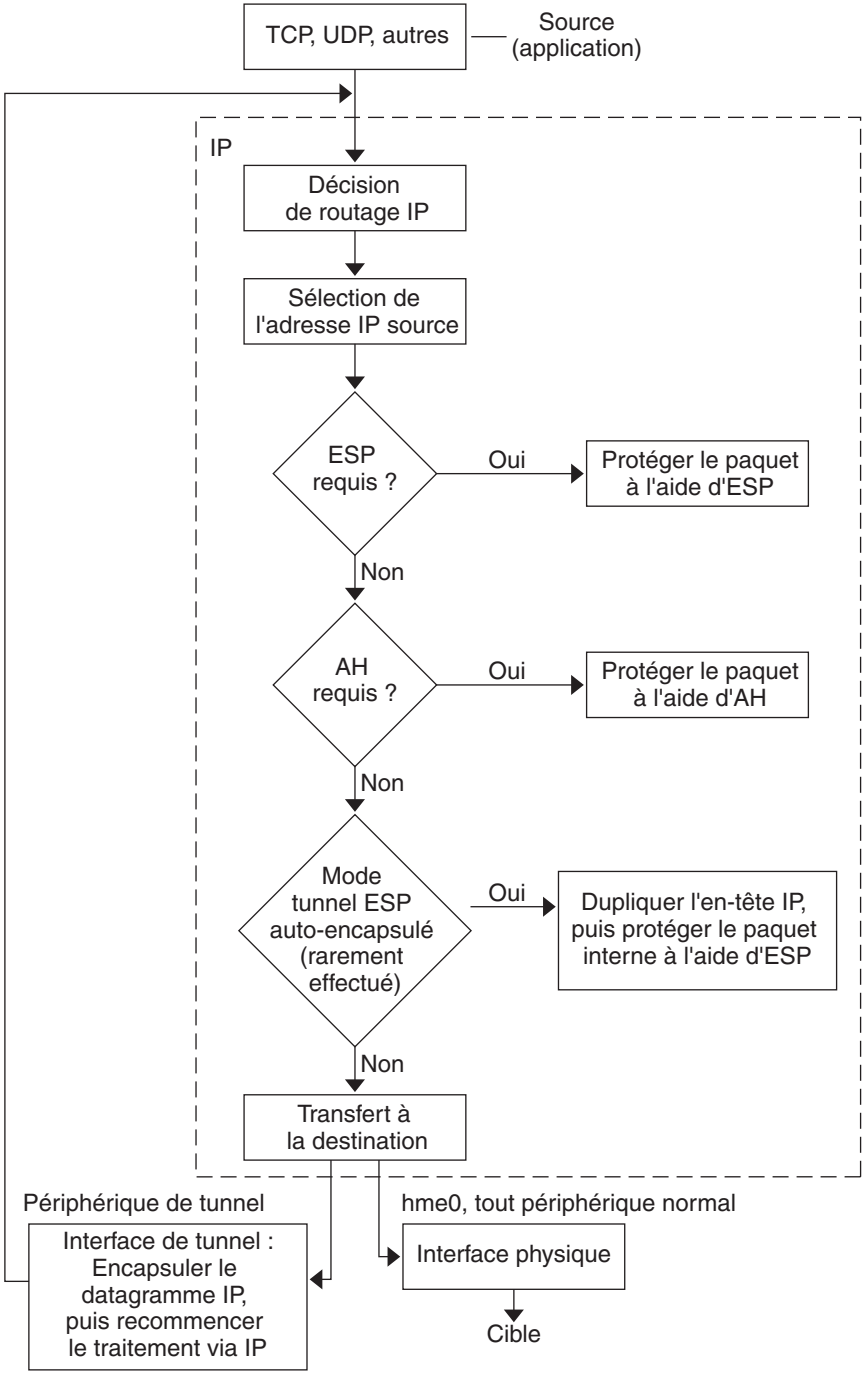
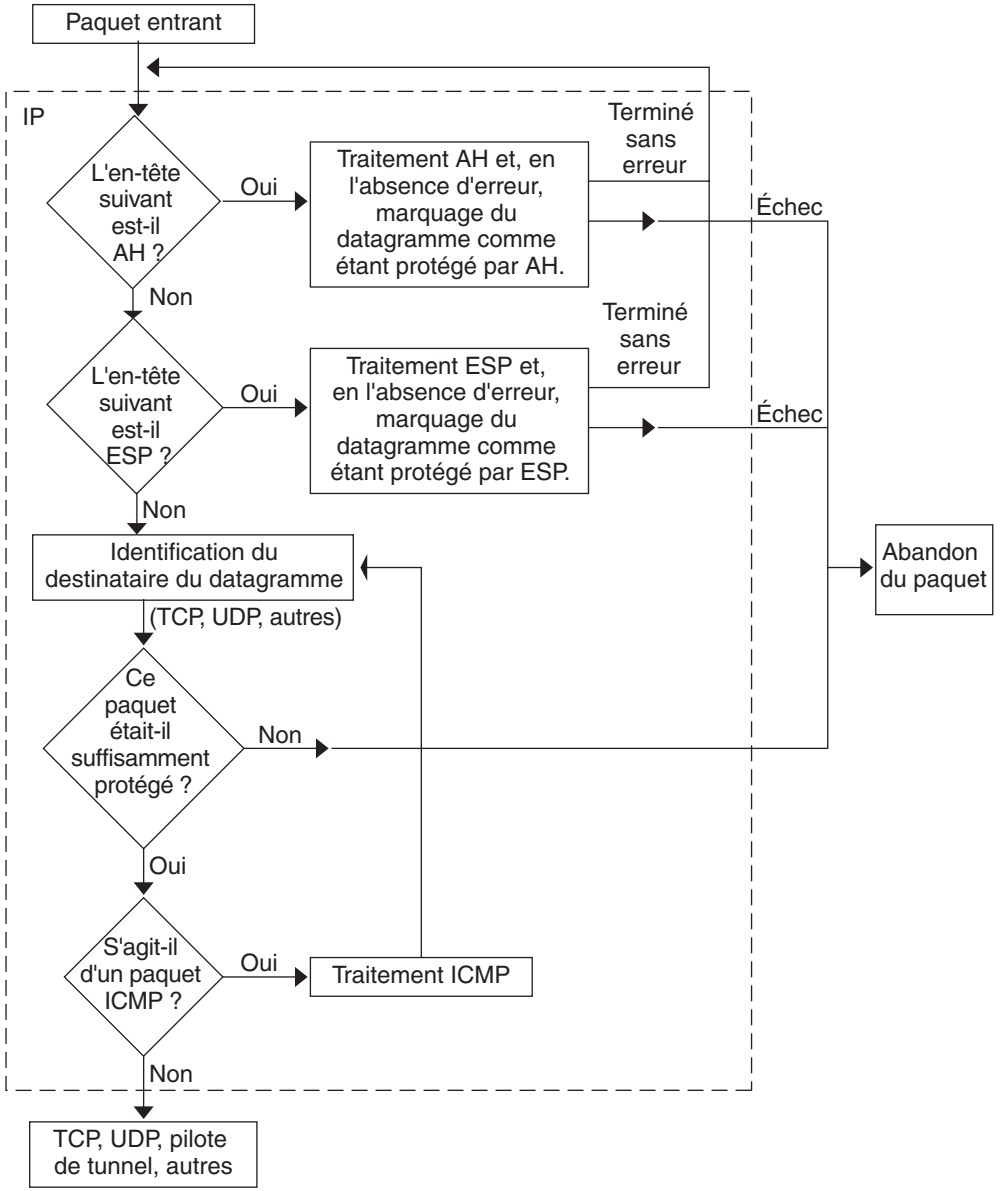


FIGURE 19–2 Application d'IPsec au processus de paquet entrant



Associations de sécurité IPsec

Une*association de sécurité* (SA, Security Association) IPsec spécifie les propriétés de sécurité que reconnaissent les hôtes lors de la communication. Une seule SA protège les données dans une direction. La protection s'applique à un seul hôte ou à une adresse de groupe (multidiffusion). La communication s'effectuant généralement entre homologues ou entre client et serveur, la sécurité du trafic dans les deux directions requiert la présence de deux SA.

Les trois éléments suivants identifient une SA IPsec de manière unique :

- le protocole de sécurité (AH ou ESP) ;
- l'adresse IP de destination ;
- le index du paramètre de sécurité.

Le SPI, valeur arbitraire 32 bits, est transmis avec un paquet AH ou ESP. Les pages de manuel `ipsecah`(7P) et `ipsecesp`(7P) expliquent l'étendue de la protection AH et ESP. Une somme de contrôle d'intégrité permet d'authentifier un paquet. En cas d'échec de l'authentification, le paquet est rejeté.

Les associations de sécurité sont stockées dans une *base de données d'associations de sécurité* (SADB). Un moteur d'administration socket, l'interface `PF_KEY`, autorise les applications privilégiées à gérer la base de données. Par exemple, l'application IKE et la commande `ipseckeys` font appel à l'interface socket `PF_KEY`.

- Pour une description détaillée de la SADB IPsec, reportez-vous à la section “Base de données des associations de sécurité IPsec” à la page 579.
- Pour plus d'informations sur la gestion de la SADB, consultez la page de manuel `pf_key`(7P).

Gestion des clés dans IPsec

Les associations de sécurité (SA) requièrent des numéros de clé pour l'authentification et le chiffrement. Le processus permettant de gérer ces *numéros de clés* est appelé la *gestion des clés*. Le protocole IKE (Internet Key Exchange, échange de clé Internet) gère les clés automatiquement. La commande `ipseckey` permet la gestion manuelle des clés, le cas échéant.

Les SA sur les paquets IPv4 et IPv6 peuvent recourir à chacune des méthodes. Il est recommandé d'utiliser la gestion automatique à moins d'avoir une bonne raison de préférer la gestion manuelle. Par exemple, la gestion manuelle de clés s'impose dans le cadre d'interopérations avec des systèmes autres que les systèmes Solaris.

Dans la version actuelle, l'utilitaire SMF fournit les services de gestion de clés pour IPsec :

- Le **service** `svc:/network/ipsec/ike:default` correspond au service SMF utilisé pour la gestion automatique des clés. Le service `ike` exécute le démon `in.iked` pour la gestion automatique des clés. Le Chapitre 22, "Protocole IKE (présentation)" propose une description du protocole IKE. Pour plus d'informations sur le démon `in.iked`, reportez-vous à la page de manuel `in.iked`(1M). Pour plus d'informations sur le service `ike`, reportez-vous à la section "Utilitaire de gestion du service IKE" à la page 639.
- Le **service** `svc:/network/ipsec/manual-key:default` correspond au service SMF utilisé pour la gestion manuelle des clés. Le service `manual-key` exécute la commande `ipseckey` avec de nombreuses options pour gérer les clés manuellement. La commande `ipseckey` est décrite à la section "Utilitaires de génération de clés IPsec" à la page 579. Pour obtenir une description détaillée des options de la commande `ipseckey`, reportez-vous à la page de manuel `ipseckey`(1M).

Dans les versions antérieures à la version Solaris 10 4/09, les commandes `in.iked` et `ipseckey` permettent de gérer les numéros de clé.

- Le démon `in.iked` permet la gestion automatique des clés. Le Chapitre 22, "Protocole IKE (présentation)" propose une description du protocole IKE. Pour plus d'informations sur le démon `in.iked`, reportez-vous à la page de manuel `in.iked`(1M).
- La commande `ipseckey` permet de gérer les clés manuellement. La section "Utilitaires de génération de clés IPsec" à la page 579 propose une description de cette commande. Pour obtenir une description détaillée des options de la commande `ipseckey`, reportez-vous à la page de manuel `ipseckey`(1M).

Mécanismes de protection IPsec

IPsec offre deux protocoles de sécurité dans le cadre de la protection des données :

- AH (Authentication Header, en-tête d'authentification)
- ESP (Encapsulating Security Payload, association de sécurité)

AH protège les données à l'aide d'un algorithme d'authentification. ESP protège les données à l'aide d'un algorithme de chiffrement, mais peut avoir recours à un algorithme d'authentification facultatif. On appelle *mécanisme* l'implémentation d'un algorithme.

En-tête Authentification

L'en-tête d'authentification offre l'authentification des données, un niveau élevé d'intégrité et la protection de rediffusion des datagrammes IP. AH protège la majeure partie du datagramme IP. Comme l'illustre la figure suivante, AH est inséré entre l'en-tête IP et l'en-tête de transport.

L'en-tête de transport peut être TCP, UDP, SCTP ou ICMP. Dans le cas de l'utilisation d'un tunnel, l'en-tête de transport peut être un autre en-tête IP.

ESP (Encapsulating Security Payload, association de sécurité)

Le module protocole ESP assure la confidentialité des encapsulations ESP. ESP propose également les services AH. Toutefois, ESP n'offre sa protection qu'à la partie des datagrammes d'encapsulation ESP. ESP fournit des services d'authentification facultatifs afin d'assurer l'intégrité du paquet protégé. Du fait qu'ESP utilise une technologie de chiffrement, un système fournissant ESP peut être soumis à des lois sur le contrôle des importations et exportations.

ESP encapsule ses données de sorte à protéger uniquement les données figurant à la suite de son commencement dans le datagramme, comme illustré ci-dessous.

Chiffré

Dans un paquet TCP, ESP encapsule uniquement l'en-tête TCP et ses données. Si le paquet est un datagramme IP-in-IP, ESP protège le datagramme IP interne. La stratégie par socket permet l'*auto-encapsulation*. Ainsi, ESP peut encapsuler les options IP, le cas échéant.

Lorsque l'auto-encapsulation est définie, l'en-tête IP est copié afin de créer un datagramme IP-in-IP. Par exemple, lorsque l'auto-encapsulation n'est pas définie sur un socket TCP, le datagramme est envoyé dans le format suivant :

```
[ IP(a -> b) options + TCP + data ]
```

Lorsque l'auto-encapsulation est définie sur ce socket TCP, le datagramme est envoyé dans le format suivant :

```
[ IP(a -> b) + ESP [ IP(a -> b) options + TCP + data ] ]
```

Pour de plus amples informations, reportez-vous à la section “Modes Transport et Tunnel dans IPsec” à la page 508.

Considérations de sécurité lors de l'utilisation de AH et ESP

Le tableau suivant permet de comparer les protections AH et ESP.

TABLEAU 19–2 Protections assurées par AH et ESP dans IPsec

Protocole	Paquets protégés	Protection	Attaques contrées
AH	Protection des paquets de l'en-tête IP jusqu'à l'en-tête de transport	Intégrité élevée, authentification des données : ■ réception garantie des données exactes envoyées par l'expéditeur ■ attaques par rejeu possibles lorsqu'un AH n'active pas la protection par rejeu	Rejeu, couper-coller
fournisseur de services aux entreprises	Protection des paquets figurant à la suite du début d'ESP dans le datagramme	Chiffrement du datagramme IP à l'aide de l'option de chiffrement Confidentialité garantie	Écoute électronique
		Protection identique à la protection AH à l'aide de l'option d'authentification	Rejeu, couper-coller
		Intégrité élevée, authentification des données et confidentialité à l'aide des deux options	Rejeu, couper-coller, écoute électronique

Authentification et chiffrement dans IPsec

Les protocoles de sécurité IPsec font appel à deux types d'algorithmes : les algorithmes d'authentification et les algorithmes de chiffrement. Le module AH recourt aux algorithmes d'authentification. Le module ESP peut utiliser aussi bien les algorithmes d'authentification que les algorithmes de chiffrement. La commande `ipsecalgs` affiche la liste des algorithmes présents sur le système, ainsi que leurs propriétés. Pour plus d'informations, reportez-vous à la page de manuel `ipsecalgs(1M)` Vous pouvez aussi utiliser les fonctions décrites dans la page de manuel `getipsecalgbyname(3NSL)`pour obtenir les propriétés des algorithmes.

Pour accéder aux algorithmes sur un système Solaris, IPsec fait appel à la structure cryptographique Solaris. Celle-ci offre un référentiel central d'algorithmes, en plus d'autres services. Elle permet à IPsec de tirer profit des accélérateurs cryptographiques hautes performances et offre des fonctions de contrôle de ressources. Par exemple, la structure permet de limiter le temps CPU consacré aux opérations cryptographiques dans le noyau.

Pour plus d'informations, reportez-vous aux références suivantes :

- Chapitre 13, “Oracle Solaris Cryptographic Framework (Overview)” du *System Administration Guide: Security Services*
- Chapitre 8, “Introduction to the Oracle Solaris Cryptographic Framework” du *Developer's Guide to Oracle Solaris Security*

Algorithmes d'authentification dans IPsec

Les algorithmes d'authentification génèrent une valeur de somme de contrôle d'intégrité, *digest*, à partir des données et d'une clé. Le module AH recourt aux algorithmes d'authentification. Le module ESP peut également y avoir recours.

Algorithmes de chiffrement dans IPsec

Les algorithmes de chiffrement chiffrent les données à l'aide d'une clé. Dans IPsec, le module ESP fait appel aux algorithmes de chiffrement. Les algorithmes agissent sur les données dans des unités d'une *taille de bloc*.

Les diverses versions du SE Solaris10 offrent différents algorithmes de chiffrement par défaut.

Attention – À partir de la version Solaris 10 7/07, n'ajoutez plus Solaris Encryption Kit à votre système. Le kit effectue une mise à niveau inférieure du patch de chiffrement de votre système. Le kit n'est pas compatible avec le chiffrement de votre système.

- À partir de la version Solaris 10 7/07, le contenu de Solaris Encryption Kit est installé par le support d'installation Solaris. Cette version intègre les algorithmes d'authentification SHA2 suivants : sha256, sha384 et sha512. Les implémentations SHA2 sont conformes à la spécification RFC 4868. Cette version ajoute également des groupes Diffie-Hellman plus grands : 2 048 bits (groupe 14), 3 072 bits (groupe 15) et 4 096 bits (groupe 16). Notez que les systèmes Sun alliés à la technologie CoolThreads permettent d'accélérer les groupes de 2 048 bits uniquement.
- Dans les versions antérieures à Solaris 10 7/07, le support d'installation Solaris n'offre que des algorithmes de base ; toutefois, Solaris Encryption Kit vous permet d'ajouter des algorithmes plus avancés.

  Par défaut, les algorithmes DES-CBC, 3DES-CBC, AES-CBC et Blowfish-CBC sont installés. Les tailles de clé prises en charge par les algorithmes AES-CBC et Blowfish-CBC ne peuvent excéder 128 bits.

  Les algorithmes AES-CBC et Blowfish-CBC prenant en charge les tailles de clé supérieures à 128 bits sont disponibles dans IPsec si vous installez le kit de chiffrement Solaris. Toutefois, certains algorithmes de chiffrement ne sont pas disponibles en dehors des États-Unis. Le kit est disponible sur un CD distinct qui ne fait *pas* partie du coffret d'installation Solaris10. Pour l'installer, consultez le document *Solaris 10 Encryption Kit Installation Guide*. Pour plus d'informations, reportez-vous au centre de téléchargement Sun (`http://www.oracle.com/technetwork/indexes/downloads/index.html`). Pour télécharger le kit, cliquez sur l'onglet Downloads A-Z, puis sur la lettre S. Solaris 10 Encryption Kit fait partie des 20 premières entrées.

Stratégies de protection IPsec

Les stratégies de protection IPsec peuvent recourir aux mécanismes de sécurité, quels qu'ils soient. Vous pouvez appliquer les stratégies IPsec aux niveaux suivants :

- à l'échelle du système ;
- par socket.

IPsec applique la stratégie à l'échelle du système aux datagrammes entrants et sortants. Les datagrammes sortants sont envoyés avec ou sans protection. Si la protection est appliquée, les algorithmes sont soit spécifiques, soit non spécifiques. Vous pouvez appliquer d'autres règles aux datagrammes sortants, en raison des données supplémentaires connues du système. Les datagrammes sortants peuvent être acceptés ou rejetés. La décision d'accepter ou de rejeter un datagramme sortant est fonction de plusieurs critères qui peuvent se chevaucher et être contradictoires. Pour résoudre les conflits éventuels, il faut identifier la règle à analyser en premier. Le trafic est accepté automatiquement, sauf si une entrée de stratégie indique qu'il doit ignorer toutes les autres stratégies.

La stratégie qui protège normalement un datagramme peut être ignorée. Vous pouvez spécifier une exception dans la stratégie à l'échelle du système ou demander un contournement dans la stratégie par socket. Au niveau du trafic système, les stratégies sont mises en œuvre, mais les mécanismes de sécurité à proprement parler ne sont pas appliqués. En revanche, la stratégie sortante sur un paquet interne au système se traduit par un paquet sortant auquel ces mécanismes ont été appliqués.

La configuration des stratégies IPsec s'effectue à l'aide du fichier `ipsecinit.conf` et de la commande `ipsecconf`. La page de manuel `ipsecconf(1M)` contient des exemples et des explications complémentaires.

Modes Transport et Tunnel dans IPsec

Les normes IPsec définissent deux modes distincts d'opération IPsec : le *mode Transport* et le *mode Tunnel*. Ces modes n'ont aucune incidence sur le codage des paquets. Les paquets sont protégés par AH, ESP ou ces deux protocoles dans chaque mode. L'application de la stratégie des modes est différente lorsque le paquet interne est un paquet IP :

- En mode Transport, l'en-tête extérieur détermine la stratégie IPsec qui protège le paquet IP interne.
- En mode Tunnel, le paquet IP interne détermine la stratégie IPsec qui protège son contenu.

En mode Transport, l'en-tête extérieur ainsi que l'en-tête suivant et tout port pris en charge par celui-ci permettent de déterminer la stratégie IPsec. En fait, IPsec peut mettre en œuvre différentes stratégies en mode Transport entre deux adresses IP au niveau d'un seul port. Par exemple, si l'en-tête suivant est un en-tête TCP, qui prend en charge les ports, la stratégie IPsec peut alors être définie pour un port TCP de l'adresse IP externe. De même, si l'en-tête suivant est IP, l'en-tête extérieur et l'en-tête IP intérieur permettent de déterminer la stratégie IPsec.

Le mode Tunnel ne fonctionne que pour les datagrammes IP-in-IP. La mise sous tunnel en mode Tunnel peut s'avérer utile lorsque des personnes travaillant à domicile se connectent à un emplacement central. En mode Tunnel, la stratégie IPsec est mise en œuvre sur le contenu du datagramme IP interne. Différentes stratégies IPsec peuvent être mises en œuvre pour différentes adresses IP internes. En d'autres termes, l'en-tête IP interne, ainsi que son en-tête

suivant et les ports que ce dernier prend en charge, peuvent mettre en œuvre une stratégie. Contrairement au mode Transport, le mode Tunnel ne permet pas à l'en-tête IP extérieur de dicter la stratégie de son datagramme IP interne.

Par conséquent, en mode Tunnel, la stratégie IPsec peut être spécifiée pour les sous-réseaux d'un LAN derrière un routeur et pour les ports de ces sous-réseaux. La stratégie IPsec peut également être spécifiée pour des adresses IP données (des hôtes) sur ces sous-réseaux. Les ports de ces hôtes peuvent aussi avoir une stratégie IPsec spécifique. Toutefois, si un protocole de routage dynamique est exécuté sur un tunnel, veillez à ne pas utiliser de sélection de sous-réseau ou d'adresse, car la vue de la topologie réseau sur le réseau homologue pourrait être modifiée. Les modifications annuleraient la stratégie IPsec statique. La section "Protection d'un VPN à l'aide d'IPsec" à la page 538 contient des exemples de mises en tunnel comprenant la configuration de routes statiques.

Dans le SE Solaris, le mode Tunnel ne peut être mis en œuvre que sur une interface réseau de mise en tunnel IP. La commande `ipsecconf` fournit un mot-clé `tunnel` pour sélectionner une interface réseau de mise en tunnel IP. Lorsque le mot-clé `tunnel` figure dans une règle, tous les sélecteurs spécifiés dans cette règle s'appliquent au paquet interne.

En mode Transport, ESP et/ou AH peuvent protéger le datagramme.

La figure suivante illustre un en-tête IP avec un paquet TCP non protégé.

FIGURE 19–3 Paquet IP non protégé transportant des informations TCP

En mode Transport, ESP protège les données, comme illustré ci-dessous. La zone ombrée indique la partie chiffrée du paquet.

FIGURE 19–4 Paquet IP protégé transportant des informations TCP

Chiffré

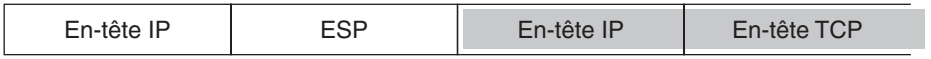
En mode Transport, AH protège les données comme illustré ci-dessous.

FIGURE 19–5 Paquet protégé par un en-tête d'authentification

AH couvre en fait les données avant leur apparition dans le datagramme. Par conséquent, la protection assurée par AH, même en mode Transport, couvre en partie l'en-tête IP.

En mode Tunnel, l'intégralité du datagramme figure *à l'intérieur* de la protection d'un en-tête IPsec. Le datagramme de la Figure 19–3 est protégé en mode Tunnel par un en-tête IPsec externe, ESP dans ce cas, comme indiqué sur l'illustration suivante.

FIGURE 19–6 Paquet IPsec protégé en mode Tunnel



La commande `ipsecconf` inclut des mots-clés permettant de définir des tunnels en mode Tunnel ou Transport.

- Pour plus d'informations sur la stratégie par socket, reportez-vous à la page de manuel `ipsec(7P)`.
- La section "Utilisation d'IPsec pour protéger un serveur Web du trafic non-web." à la page 523 comprend un exemple de stratégie par socket.
- Pour plus d'informations sur les tunnels, reportez-vous à la page de manuel `ipsecconf(1M)`.
- La section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544 contient un exemple de configuration de tunnel.

Réseaux privés virtuels et IPsec

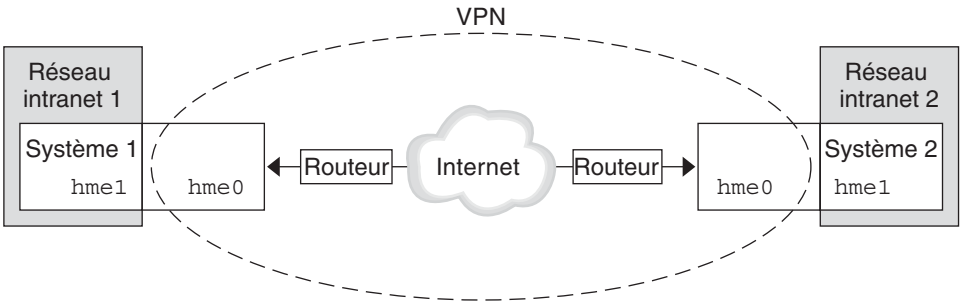
Un tunnel configuré est une interface point-à-point. Le tunnel permet l'encapsulation d'un paquet IP dans un autre paquet IP. Un tunnel correctement configuré requiert une source et une destination. Pour plus d'informations, reportez-vous à la page de manuel `tun(7M)` et à la section Configuration de tunnels pour la prise en charge d'IPv6.

Un tunnel crée une interface physique liée à IP. L'intégrité du lien physique est fonction des protocoles de sécurité sous-jacents. La configuration sécurisée des associations de sécurité (SA) rend le tunnel digne de confiance. Les paquets sortant du tunnel doivent provenir de l'homologue spécifié dans la destination de tunnel. Si la confiance est établie, vous pouvez avoir recours au transfert IP par interface pour créer un VPN.

Vous pouvez créer un VPN à l'aide d'IPsec. IPsec sécurise la connexion. Par exemple, une organisation ayant recours à la technologie VPN pour connecter deux bureaux de réseaux distincts peut déployer IPsec pour sécuriser le trafic entre ces deux bureaux.

Dans l'illustration suivante, deux bureaux utilisent Internet pour constituer leur VPN, avec IPsec déployé sur leurs systèmes réseau.

FIGURE 19–7 Réseau privé virtuel



La section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544 contient un exemple détaillé de configuration.

Un exemple similaire avec des adresses IPv6 est fourni à la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv6" à la page 554.

Passage de la translation d'adresses et IPsec

IKE peut négocier des SA IPsec dans une zone NAT Cela permet aux systèmes de se connecter en toute sécurité à partir d'un réseau distant, même lorsqu'ils résident derrière un périphérique NAT. Par exemple, les employés travaillant à domicile ou se connectant depuis un site de conférence peuvent protéger leur trafic à l'aide d'IPsec.

NAT est l'acronyme de Network Address Translation (translation d'adresse réseau). Un routeur NAT permet d'associer une adresse interne privée à une adresse Internet unique. Les routeurs NAT équipent de nombreux points d'accès publics à Internet, comme ceux qu'on trouve dans les hôtels. Pour de plus amples informations, reportez-vous à la section "Utilisation de la fonctionnalité NAT d'IP Filter" à la page 656.

La capacité à utiliser IKE lorsqu'un boîtier NAT est placé entre deux systèmes communiquant est appelé NAT Traversal ou NAT-T. Dans la version Solaris10, NAT-T présente les limitations suivantes :

- NAT-T ne peut pas tirer profit de l'accélération ESP IPsec que procure la carte Sun Crypto Accelerator 4000. Toutefois, l'accélération IKE avec la carte Sun Crypto Accelerator 4000 fonctionne.
- Le protocole AH dépend d'un en-tête IP qui ne change pas ; de ce fait, AH ne peut pas fonctionner avec NAT-T. Le protocole ESP est utilisé avec NAT-T.
- Le routeur NAT n'applique pas de règles de traitement particulières. Un routeur NAT obéissant à des règles de traitement IPsec pourrait intervenir dans l'implémentation de NAT-T.
- NAT-T fonctionne uniquement lorsque l'initiateur IKE est le système derrière le routeur NAT. Un répondeur IKE ne peut pas se trouver derrière un routeur NAT, à moins que celui-ci ne soit programmé pour transférer des paquets IKE au système adéquat figurant derrière lui.

Les RFC suivants décrivent la fonctionnalité NAT et les limites de NAT-T. Vous pouvez vous procurer des copies de ces RFC sur le site `http://www.rfc-editor.org`.

- RFC 3022, "Traditional IP Network Address Translator (Traditional NAT)", janvier 2001 ;
- RFC 3715, "IPsec-Network Address Translation (NAT) Compatibility Requirements", mars 2004 ;
- RFC 3947, "Negotiation of NAT-Traversal in the IKE", janvier 2005 ;
- RFC 3948, "UDP Encapsulation of IPsec Packets", janvier 2005.

Pour une utilisation conjointe d'IPsec et NAT, reportez-vous à la section “Configuration du protocole IKE pour les systèmes portables (liste des tâches)” à la page 624.

IPsec et SCTP

Le système d'exploitation Solaris prend en charge le protocole SCTP (Streams Control Transmission Protocol). Bien que prise en charge, l'utilisation du protocole SCTP et du numéro de port SCTP dans le cadre de la spécification de la stratégie IPsec n'est pas stable. Les extensions IPsec pour SCTP spécifiées dans le document RFC 3554 ne sont pas encore implémentées. Ces restrictions peuvent être source de complications lors de la création de la stratégie IPsec pour SCPT.

SCTP peut avoir recours à plusieurs adresses source et cible dans le cadre d'une association SCTP unique. Lorsque la stratégie IPsec est appliquée à une seule adresse source ou cible, la communication peut échouer si SCTP change l'adresse source ou cible de cette association. La stratégie IPsec reconnaît uniquement l'adresse d'origine. Pour plus d'informations sur le protocole SCTP, consultez les documents RFC et “Protocol SCTP” à la page 42.

IPsec et les zones Solaris

Pour les zones IP partagées, la stratégie IPsec est configurée à partir de la zone globale. Le fichier de configuration de la stratégie IPsec, `ipsecinit.conf`, existe uniquement dans la zone globale. Le fichier peut contenir des entrées s'appliquant aux zones non globales et des entrées s'appliquant à la zone globale.

Pour les zones IP exclusives, la stratégie IPsec est configurée dans la zone non globale.

Pour plus d'informations à propos de l'utilisation d'IPsec avec des zones, reportez-vous à la section "Protection du trafic à l'aide d'IPsec" à la page 518. Pour plus d'informations sur les zones, reportez-vous au Chapitre 16, "Introduction aux zones Solaris" du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

IPsec et domaines logiques

Le protocole IPsec fonctionne avec des domaines logiques. Le domaine logique doit être en cours d'exécution sur une version du système d'exploitation Solaris comprenant le protocole IPsec, comme la version Solaris 10.

Pour créer des domaines logiques, vous devez utiliser Oracle VM Server for SPARC. Cette application s'appelait auparavant Sun Logical Domains. Pour savoir comment configurer des domaines logiques, reportez-vous au *Logical Domains 1.2 Administration Guide* ou au *Oracle VM Server for SPARC 2.0 Administration Guide*.

Fichiers et utilitaires IPsec

Le Tableau 19–3 décrit les fichiers, commandes et identificateurs de service utilisés pour configurer et gérer IPsec. Exhaustif, ce tableau inclut les commandes et fichiers de gestion des clés.

À partir de la version Solaris 10 4/09, IPsec est géré par SMF. Pour plus d'informations sur les identificateurs de services, reportez-vous au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base*.

- Pour obtenir les instructions relatives à l'implémentation IPsec sur le réseau, reportez-vous à la section "Protection du trafic à l'aide d'IPsec (liste des tâches)" à la page 517.
- Pour plus d'informations sur les fichiers et utilitaires IPsec, reportez-vous au Chapitre 21, "Architecture IPsec (référence)".

TABLEAU 19–3 Liste des utilitaires et fichiers IPsec sélectionnés

Utilitaire IPsec, fichier ou service	Description	Page de manuel
`svc:/network/ipsec/ipsecalgs`	Dans la version actuelle, le service SMF qui gère les algorithmes IPsec.	`smf(5)`, `ipsecalgs(1M)`
`svc:/network/ipsec/manual-key`	Dans la version actuelle, le service SMF qui gère les associations de sécurité (SA) manuelles.	`smf(5)`, `ipseckey(1M)`
`svc:/network/ipsec/policy`	Dans la version actuelle, le service SMF qui gère la stratégie IPsec.	`smf(5)`, `ipsecconf(1M)`
`svc:/network/ipsec/ike`	Dans la version actuelle, le service SMF pour la gestion automatique des SA IPsec.	`smf(5)`, `in.iked(1M)`
Fichier `/etc/inet/ipsecinit.conf`	Fichier de stratégie IPsec. Dans les versions antérieures à la version Solaris 10 4/09, si ce fichier existe, IPsec est activé au démarrage. Dans la version actuelle, le service `policy` de SMF utilise ce fichier pour configurer la stratégie IPsec lors de l'initialisation du système.	`ipsecconf(1M)`
Commande `ipsecconf`	Commande de stratégie IPsec. Utile pour afficher et modifier la stratégie IPsec actuelle, ainsi que pour effectuer des tests. Dans les versions antérieures à la version Solaris 10 4/09, les scripts d'initialisation utilisent `ipsecconf` pour lire le fichier `/etc/inet/ipsecinit.conf` et activer IPsec. Dans la version actuelle, `ipsecconf` est utilisé par le service `policy` de SMF pour configurer la stratégie IPsec lors de l'initialisation du système.	`ipsecconf(1M)`
Interface socket `PF_KEY`	SADB (Interface for Security Associations Database, interface de la base de données des associations de sécurité). Responsable de la gestion manuelle et automatique des clés.	`pf_key(7P)`
Commande `ipseckey`	Commandes de génération de clés pour les SA IPsec `ipseckey` est un point d'entrée de commandes de l'interface `PF_KEY. ipseckey` permet de créer, supprimer ou modifier les SA.	`ipseckey(1M)`
Fichier `/etc/inet/secret/ipseckeys`	Clés pour SA IPsec. Dans les versions antérieures à la version Solaris 10 4/09, si le fichier `ipsecinit.conf` existe, le fichier `ipseckeys` est automatiquement lu au démarrage. Dans la version actuelle, `ipseckeys` est utilisé par le service `manual-key` de SMF pour configurer manuellement les SA à l'initialisation du système.	
Commande `ipsecalgs`	Commande d'algorithmes IPsec. Utile pour l'affichage et la modification de la liste d'algorithmes IPsec et de leurs propriétés. Dans la version actuelle, est utilisée par le service `ipsecalgs` de SMF pour synchroniser les algorithmes IPsec connus avec le noyau, à l'initialisation du système.	`ipsecalgs(1M)`

TABLEAU 19–3 Liste des utilitaires et fichiers IPsec sélectionnés *(Suite)*

Utilitaire IPsec, fichier ou service	Description	Page de manuel
Fichier `/etc/inet/ipsecalgs`	Contient les définitions d'algorithme et les protocoles IPsec configurés. Ce fichier est géré par la commande `ipsecalgs` et ne doit jamais être modifié manuellement.	
Fichier `/etc/inet/ike/config`	Fichier de configuration et de stratégie IKE. Par défaut, ce fichier n'existe pas. Dans les versions antérieures à la version Solaris 10 4/09, si ce fichier existe, le démon IKE, `in.iked`, permet la gestion automatique des clés. La gestion se base sur des règles et des paramètres généraux figurant dans le fichier `/etc/inet/ike/config`. Reportez-vous à la section "Utilitaires et fichiers IKE" à la page 590. Dans la version actuelle, si ce fichier existe, le service `svc:/network/ipsec/ike` lance le démon IKE, `in.iked` pour la gestion automatique des clés.	`ike.config(4)`

Modifications IPsec dans la version Solaris10

Vous trouverez une liste complète des nouvelles fonctionnalités de Solaris et la description des différentes versions de Solaris dans le guide *Nouveautés apportées à Oracle Solaris 10 8/11*. À partir de la version Solaris 9, IPsec inclut les fonctions suivantes :

- Lorsqu'une carte Sun Crypto Accelerator 4000 est connectée, elle met automatiquement en cache les SA IPsec des paquets faisant appel à son interface Ethernet. La carte accélère également le traitement des SA IPsec.
- IPsec peut tirer profit de la gestion automatique des clés avec IKE sur réseaux IPv6. Pour plus d'informations, reportez-vous au Chapitre 22, "Protocole IKE (présentation)".

  Pour connaître les nouvelles fonctions IKE, reportez-vous à la section "Modifications apportées à IKE dans Solaris10" à la page 591.
- L'analyseur de la commande `ipseckey` offre une aide plus claire. La commande `ipseckey monitor` indique la date et l'heure de chaque événement. Pour plus d'informations, reportez-vous à la page de manuel `ipseckey(1M)`.
- Les algorithmes IPsec proviennent désormais d'un espace de stockage central, la structure cryptographique Solaris. La page de manuel `ipsecalgs(1M)` décrit les caractéristiques des algorithmes disponibles. Les algorithmes sont optimisés pour l'architecture sur laquelle ils s'exécutent. Pour obtenir une description de la structure, reportez-vous au Chapitre 13, "Oracle Solaris Cryptographic Framework (Overview)" du *System Administration Guide: Security Services*.
- IPsec fonctionne dans la zone globale. La stratégie IPsec est gérée dans la zone globale pour une zone non globale. Les numéros de clé sont créés et gérés manuellement dans la zone globale pour une zone non globale. IKE ne permet pas de générer des clés pour une zone

non globale. Pour plus d'informations sur les zones, reportez-vous au Chapitre 16, “Introduction aux zones Solaris” du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

- La stratégie IPsec peut fonctionner avec le protocole SCTP (Streams Control Transmission Protocol) et le numéro de port SCTP. Toutefois, l'implémentation reste incomplète. Les extensions IPsec pour SCTP spécifiées dans le document RFC 3554 ne sont pas encore implémentées. Ces restrictions peuvent être source de complications lors de la création de la stratégie IPsec pour SCPT. Pour plus d'informations, reportez-vous aux RFC. Consultez également les documents “IPsec et SCTP” à la page 512 et “Protocol SCTP” à la page 42.
- IPsec et IKE peuvent protéger le trafic généré derrière un routeur NAT. Pour en savoir plus sur les restrictions, reportez-vous à la section “Passage de la translation d'adresses et IPsec” à la page 511. Pour plus d'informations sur les procédures, reportez-vous à la section “Configuration du protocole IKE pour les systèmes portables (liste des tâches)” à la page 624.

◆ ◆ ◆ CHAPITRE 20

Configuration d'IPsec (tâches)

Ce chapitre fournit les procédures d'implémentation d'IPsec sur votre réseau. Les procédures sont décrites dans la liste des tâches ci-dessous :

- “Protection du trafic à l'aide d'IPsec (liste des tâches)” à la page 517
- “Protection d'un VPN à l'aide d'IPsec (liste des tâches)” à la page 541

Vous trouverez une présentation d'IPsec au Chapitre 19, “Architecture IPsec (présentation)”. Des informations de référence sur IPsec sont fournies au Chapitre 21, “Architecture IPsec (référence)”.

Protection du trafic à l'aide d'IPsec (liste des tâches)

La liste des tâches ci-dessous répertorie les procédures de configuration d'IPsec sur un ou plusieurs systèmes. En outre, vous trouverez des procédures utiles dans les sections d'exemples des pages de manuel `ipsecconf`(1M), `ipseckey`(1M) et `ifconfig`(1M).

Tâche	Description	Voir
Sécurisation du trafic entre deux systèmes	Protège les paquets transmis d'un système à un autre.	“Sécurisation du trafic entre deux systèmes à l'aide d'IPsec” à la page 519
Sécurisation d'un serveur Web à l'aide de la stratégie IPsec	Requiert un trafic non-Web pour utiliser IPsec. Les clients Web sont identifiés par des ports particuliers : les vérifications IPsec sont ignorées.	“Utilisation d'IPsec pour protéger un serveur Web du trafic non-web.” à la page 523
Affichage des stratégies IPsec	Affiche les stratégies IPsec actuellement appliquées, dans l'ordre dans lequel elles sont mises en œuvre.	“Affichage des stratégies IPsec” à la page 526

Tâche	Description	Voir
Génération de numéros aléatoires	Génère des numéros aléatoires pour définir les numéros de clé afin de permettre la création manuelle d'associations de sécurité.	"Génération de numéros aléatoires sur un système Solaris" à la page 527 Section "How to Generate a Symmetric Key by Using the pktool Command" du *System Administration Guide: Security Services*
Création et remplacement manuels des associations de sécurité	Fournit les données brutes des associations de sécurité : ■ Nom d'algorithme IPsec et numéros de clé ; ■ Clé de l'index de paramètre de sécurité ; ■ Adresses IP source et de destination.	"Création manuelle d'associations de sécurité IPsec" à la page 528
Vérification de la protection des paquets par IPsec	Recherche des en-têtes spécifiques indiquant la méthode de protection des datagrammes IP dans la sortie de commande `snoop`.	"Vérification de la protection des paquets par IPsec" à la page 533
(Facultatif) Création d'un rôle de sécurité réseau	Crée un rôle pouvant configurer un réseau sécurisé, mais possédant moins de permissions que le superutilisateur.	"Configuration d'un rôle pour la sécurité réseau" à la page 535
Gestion d'IPsec et des numéros de clés en tant qu'ensemble de services SMF	Décrit quand et comment utiliser les commandes permettant d'activer, de désactiver, d'actualiser et de redémarrer les services. Décrit également les commandes permettant de modifier les valeurs de propriété des services.	"Procédure de gestion des services IKE et IPsec" à la page 536
Configuration d'un réseau privé virtuel (VPN, Virtual Private Network) sécurisé	Configure IPsec entre deux systèmes séparés par Internet.	"Protection d'un VPN à l'aide d'IPsec (liste des tâches)" à la page 541

Protection du trafic à l'aide d'IPsec

Cette section décrit les procédures permettant de sécuriser le trafic entre deux systèmes et de sécuriser un serveur Web. Pour protéger un VPN, reportez-vous à la section "Protection d'un VPN à l'aide d'IPsec (liste des tâches)" à la page 541. Des procédures supplémentaires fournissent des numéros de clé et des associations de sécurité et vérifient que IPsec fonctionne tel qu'il est configuré.

Les informations ci-dessous s'appliquent à toutes les tâches de configuration IPsec :

- **IPsec et zones :** pour gérer les clés et la stratégie IPsec dans le cas d'une zone non globale IP partagée, créez le fichier de stratégie IPsec dans la zone globale, puis exécutez les commandes de configuration IPsec à partir de la zone globale. Utilisez l'adresse source correspondant à la zone non globale à configurer. Vous pouvez également configurer les clés et la stratégie IPsec dans la zone globale pour la zone globale. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale. À partir de la version Solaris 10 7/07, vous pouvez gérer les clés dans une zone non globale à l'aide d'IKE.
- **IPsec et RBAC :** pour utiliser les rôles afin d'administrer IPsec, reportez-vous au Chapitre 9, "Using Role-Based Access Control (Tasks)" du *System Administration Guide: Security Services*. La section "Configuration d'un rôle pour la sécurité réseau" à la page 535 présente un exemple.
- **IPsec et SCTP :** vous pouvez utiliser IPsec pour protéger les associations SCTP (Streams Control Transmission Protocol, protocole de transmission de contrôle de flux), mais avec prudence. Pour de plus amples informations, reportez-vous à la section "IPsec et SCTP" à la page 512.

▼ Sécurisation du trafic entre deux systèmes à l'aide d'IPsec

Cette procédure correspond à la configuration suivante :

- Les systèmes s'appellent `enigma` et `partym`.
- Chaque système possède deux adresses, une adresse IPv4 et une adresse IPv6.
- Chaque système nécessite le chiffrement ESP avec l'algorithme AES, qui requiert une clé de 128 bits, ainsi que l'authentification ESP avec la synthèse des messages SHA1, qui requiert une clé de 160 bits.
- Chaque système utilise des associations de sécurité partagées (SA, Security Associations).

  Avec les SA partagées, une seule paire de SA est suffisante pour protéger les deux systèmes.

Avant de commencer Vous devez vous trouver dans la zone globale pour configurer la stratégie IPsec pour le système ou pour une zone IP partagée. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale.

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

Remarque – Les connexions à distance peuvent compromettre la sécurité du trafic de données critiques. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Exécutez la commande `ssh` pour assurer une connexion à distance sécurisée. Voir l' Exemple 20–1.

2 Sur chaque système, vérifiez les entrées d'hôte.

Dans la version actuelle, ajoutez les entrées d'hôte au fichier `/etc/inet/hosts`.

Sur un système exécutant une version antérieure à la version Solaris 10 7/07, insérez les entrées IPv4 et IPv6 dans le fichier `/etc/inet/ipnodes`. Les entrées d'un système doivent être contiguës dans le fichier. Pour de plus amples informations sur les fichiers de configuration système, reportez-vous à la section "Fichiers de configuration TCP/IP" à la page 237 et au Chapitre 11, "Présentation détaillée de IPv6 (référence)".

Si vous connectez des systèmes utilisant exclusivement des adresses IPv4, modifiez le fichier `/etc/inet/hosts`. Dans cet exemple, les systèmes à connecter s'exécutent dans une version Solaris antérieure et utilisent des adresses IPv6.

a. Sur un système appelé `enigma`, saisissez les lignes suivantes dans le fichier `hosts` ou `ipnodes` :

```
# Secure communication with partym
192.168.13.213 partym
2001::eeee:3333:3333 partym
```

b. Sur un système appelé `partym`, saisissez les lignes suivantes dans le fichier `hosts` ou `ipnodes` :

```
# Secure communication with enigma
192.168.116.16 enigma
2001::aaaa:6666:6666 enigma
```

L'utilisation de services d'assignation de noms pour des noms symboliques comporte des risques.

3 Sur chaque système, créez le fichier de stratégie IPsec.

Le nom de fichier est `/etc/inet/ipsecinit.conf`. Vous en trouverez un exemple dans le fichier `/etc/inet/ipsecinit.sample`.

4 Ajoutez une entrée de stratégie IPsec au fichier `ipsecinit.conf`.

a. Sur le système `enigma`, ajoutez la stratégie ci-dessous :

```
{laddr enigma raddr partym} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. Sur le système `partym`, ajoutez la même stratégie :

```
{laddr partym raddr enigma} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

La syntaxe des entrées de stratégie IPsec est décrite dans la page de manuel `ipsecconf(1M)`.

5 **Sur chaque système, ajoutez une paire de SA IPsec entre les deux systèmes.**

Vous pouvez configurer le protocole IKE (Internet Key Exchange, échange de clé Internet) afin de créer automatiquement les SA. Vous pouvez également ajouter les SA manuellement.

Remarque – Il est recommandé d'utiliser IKE, sauf si, pour des raisons spécifiques, vous devez générer les clés et les mettre à jour manuellement. La gestion des clés à l'aide d'IKE est plus sécurisée.

- Configurez IKE en suivant l'une des procédures de configuration décrites à la section "Configuration du protocole IKE (liste des tâches)" à la page 593. La syntaxe du fichier de configuration IKE est décrite à la page de manuel `ike.config(4)`.
- Pour ajouter des SA manuellement, reportez-vous à la section "Création manuelle d'associations de sécurité IPsec" à la page 528.

6 **Activez la stratégie IPsec.**

- **Si vous exécutez une version antérieure à la version Solaris 10 4/09, réinitialisez le système.**

  ```
  # init 6
  ```

  Reportez-vous ensuite à la section "Vérification de la protection des paquets par IPsec" à la page 533.

- **À partir de la version Solaris 10 4/09, actualisez le service IPsec et activez le service de gestion des clés.**

  Suivez les étapes Étape 7 à Étape 10.

7 **Vérifiez la syntaxe du fichier de stratégie IPsec.**

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

Corrigez les éventuelles erreurs, vérifiez la syntaxe du fichier, puis continuez.

8 **Actualisez la stratégie IPsec.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

La stratégie IPsec est activée par défaut. *Actualisez*-la. Si vous avez désactivé la stratégie IPsec, activez-la.

```
# svcadm enable svc:/network/ipsec/policy:default
```

9 **Activez les clés pour IPsec.**

- **Si vous avez configuré le service IKE lors l'Étape 5, effectuez l'une des opérations suivantes :**

  - **Si le service `ike` n'est pas activé, activez-le.**

    ```
    # svcadm enable svc:/network/ipsec/ike:default
    ```

- **Si le service `ike` est activé, redémarrez-le.**

  ```
  # svcadm restart svc:/network/ipsec/ike:default
  ```

- **Si vous avez configuré manuellement les clés lors de l'Étape 5, effectuez l'une des opérations suivantes :**

  - **Si le service `manual-key` n'est pas activé, activez-le.**

    ```
    # svcadm enable svc:/network/ipsec/manual-key:default
    ```

  - **Si le service `manual-key` est activé, actualisez-le.**

    ```
    # svcadm refresh svc:/network/ipsec/manual-key:default
    ```

10 **Assurez-vous que les paquets sont protégés.**

La procédure est décrite à la section "Vérification de la protection des paquets par IPsec" à la page 533.

Exemple 20–1 Ajout d'une stratégie IPsec lors de l'utilisation d'une connexion `ssh`

Dans cet exemple, l'administrateur en tant que superutilisateur configure la stratégie IPsec et des clés sur deux systèmes à l'aide de la commande `ssh` pour atteindre le second système. Pour plus d'informations, reportez-vous à la page de manuel `ssh(1)`.

- Tout d'abord, l'administrateur configure le premier système en effectuant les étapes Étape 2 à Étape 5 de la procédure précédente.
- Ensuite, dans une autre fenêtre de terminal, l'administrateur utilise la commande `ssh` pour se connecter au deuxième système.

  ```
  local-system # ssh other-system
  other-system #
  ```

- Dans la fenêtre de terminal de la session `ssh`, l'administrateur configure la stratégie IPsec et les clés du second système en effectuant les étapes Étape 2 à Étape 6.
- Ensuite, l'administrateur met fin à la session `ssh`.

  ```
  other-system # exit
  local-system #
  ```

- Enfin, l'administrateur active la stratégie IPsec sur le premier système en effectuant l'Étape 6.

La prochaine fois que les deux systèmes communiquent, y compris par le biais d'une connexion `ssh`, la communication est protégée par IPsec.

Exemple 20–2 Sécurisation du trafic à l'aide d'IPsec sans réinitialisation

L'exemple suivant est utile lorsque vous exécutez une version antérieure à la version Solaris 10 4/09. Dans votre version, IPsec n'est pas géré en tant que service. Cet exemple décrit l'implémentation d'IPsec dans un environnement de test. Dans un environnement de

production, il est plus sécurisé de réinitialiser que d'exécuter la commande `ipsecconf`. Les considérations de sécurité sont indiquées à la fin de cet exemple.

Au lieu de réinitialiser à l'Étape 6, choisissez l'une des options suivantes :

- Si vous utilisez IKE pour créer des numéros de clé, arrêtez le démon `in.iked`, puis relancez-le.

  ```
  # pkill in.iked
  # /usr/lib/inet/in.iked
  ```

- Si vous ajoutez des clés manuellement, exécutez la commande `ipseckey` afin d'ajouter les SA à la base de données.

  ```
  # ipseckey -c -f /etc/inet/secret/ipseckeys
  ```

  Ensuite, activez la stratégie IPsec à l'aide de la commande `ipsecconf`.

  ```
  # ipsecconf -a /etc/inet/ipsecinit.conf
  ```

Considérations de sécurité : lisez l'avertissement qui s'affiche lorsque vous exécutez la commande `ipsecconf`. Un socket déjà verrouillé, c'est-à-dire un socket déjà utilisé, constitue une porte dérobée non sécurisée sur le système. Pour plus d'informations, reportez-vous à la section "Considérations de sécurité à propos de `ipsecinit.conf` et `ipsecconf`" à la page 578.

▼ Utilisation d'IPsec pour protéger un serveur Web du trafic non-web.

Un serveur Web sécurisé permet aux clients Web de communiquer avec le service Web. Sur un serveur Web sécurisé, le trafic non Web *doit* passer des tests de sécurité. La procédure suivante inclut les contournements pour le trafic Web. En outre, ce serveur Web peut effectuer des requêtes client DNS non sécurisées. Tout autre trafic requiert ESP avec les algorithmes AES et SHA-1.

Avant de commencer

Vous devez configurer la stratégie IPsec dans la zone globale. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale. Vous avez effectué les étapes de la section "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 519 afin que les conditions suivantes soient remplies :

- La communication entre les deux systèmes est protégée par IPsec.
- Les numéros de clé sont en cours de création, soit manuellement, soit par le biais d'IKE.
- Vous avez vérifié que les paquets sont protégés.

1 **Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Exécutez la commande `ssh` pour assurer une connexion à distance sécurisée.

---

2 **Déterminez les services qui doivent ignorer les vérifications de stratégie de sécurité.**

Pour un serveur Web, ces services incluent les ports TCP 80 (HTTP) et 443 (HTTP sécurisé). Si le serveur Web assure la recherche de noms DNS, le serveur doit peut-être inclure également le port 53 pour TCP et UDP.

3 **Créez une stratégie IPsec pour le serveur Web et activez-la.**

- **À partir de la version Solaris 10 4/09, suivez les étapes Étape 4 à Étape 7.**
- **Si vous exécutez une version antérieure à la version Solaris 10 4/09, suivez les étapes Étape 8 à Étape 11.**

L'Étape 12 est facultative dans toutes les versions de Solaris.

4 **Ajoutez la stratégie du serveur Web au fichier de stratégie IPsec.**

Ajoutez les lignes suivantes dans le fichier `/etc/inet/ipsecinit.conf` :

```
# Web traffic that web server should bypass.
{lport  80 ulp tcp dir both} bypass {}
{lport 443 ulp tcp dir both} bypass {}

# Outbound DNS lookups should also be bypassed.
{rport 53 dir both} bypass {}

# Require all other traffic to use ESP with AES and SHA-1.
# Use a unique SA for outbound traffic from the port
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Cette configuration permet uniquement au trafic sécurisé d'accéder au système, avec les exceptions de contournement décrites à l'Étape 4.

5 **Vérifiez la syntaxe du fichier de stratégie IPsec.**

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 **Actualisez la stratégie IPsec.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

7 **Actualisez les clés pour IPsec.**

- **Si vous avez configuré le service IKE lors de l'Étape 5 de la section "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 519, relancez le service `IKE`.**

  ```
  # svcadm restart svc:/network/ipsec/ike
  ```

- **Si vous avez configuré manuellement des clés lors de l'Étape 5 de la section "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 519, actualisez le service `manual-key`.**

  ```
  # svcadm refresh svc:/network/ipsec/manual-key:default
  ```

Votre installation est terminée. Si vous le souhaitez, vous pouvez effectuer l'Étape 12.

8 **Créez un fichier dans le répertoire `/etc/inet` pour la stratégie de serveur Web.**

Remarque – Les étapes ci-dessous permettent de configurer un serveur Web exécutant une version antérieure à la version Solaris 10 4/09.

Attribuez au fichier un nom indiquant son objectif, par exemple `FichierInitWebIPsec`. Tapez les lignes suivantes dans ce fichier :

```
# Web traffic that web server should bypass.
{lport  80 ulp tcp dir both} bypass {}
{lport 443 ulp tcp dir both} bypass {}

# Outbound DNS lookups should also be bypassed.
{rport 53 dir both} bypass {}

# Require all other traffic to use ESP with AES and SHA-1.
# Use a unique SA for outbound traffic from the port
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Cette configuration permet uniquement au trafic sécurisé d'accéder au système, avec les exceptions de contournement décrites à l'Étape 4.

9 **Copiez le contenu du fichier créé lors de l'Étape 8 dans le fichier `/etc/inet/ipsecinit.conf`.**

10 **Protégez le fichier `FichierInitWebIPsec` à l'aide de permissions de lecture seule.**

```
# chmod 400 IPsecWebInitFile
```

11 **Sécurisez le serveur Web sans réinitialiser.**

Procédez de l'une des manières suivantes :

- Si vous effectuez la gestion des clés à l'aide d'IKE, arrêtez le démon `in.iked`, puis relancez-le.

  ```
  # pkill in.iked
  # /usr/lib/inet/in.iked
  ```

- Si vous gérez manuellement les clés, exécutez les commandes `ipseckey` et `ipsecconf`.

  Utilisez le fichier `FichierInitWebIPsec` en argument de la commande `ipsecconf`. Si vous utilisez le fichier `ipsecinit.conf` en argument, la commande `ipsecconf` génère des erreurs lorsque les stratégies du fichier sont déjà implémentées sur le système.

  ```
  # ipseckey -c -f /etc/inet/secret/ipseckeys
  # ipsecconf -a /etc/inet/IPsecWebInitFile
  ```

Attention – Lisez l'avertissement qui s'affiche lorsque vous exécutez la commande `ipsecconf`. Un socket déjà verrouillé, c'est-à-dire un socket déjà utilisé, constitue une porte dérobée non sécurisée sur le système. Pour plus d'informations, reportez-vous à la section "Considérations de sécurité à propos de `ipsecinit.conf` et `ipsecconf`" à la page 578. Le même avertissement s'applique au redémarrage du démon `in.iked`.

Vous pouvez également réinitialiser. La réinitialisation assure la mise en œuvre de la stratégie IPsec sur toutes les connexions TCP. À la réinitialisation, les connexions TCP utilisent la stratégie du fichier de stratégie IPsec.

12 (Facultatif) Autorisez un système distant à communiquer avec le serveur Web pour le trafic non-Web.

Tapez la stratégie ci-dessous dans le fichier `ipsecinit.conf` d'un système distant :

```
# Communicate with web server about nonweb stuff
#
{laddr webserver} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Un système distant peut communiquer de manière sécurisée avec le serveur Web pour le trafic non-Web uniquement lorsque les stratégies IPsec des systèmes sont identiques.

▼ Affichage des stratégies IPsec

Vous pouvez afficher les stratégies configurées dans le système lorsque vous exécutez la commande `ipsecconf` sans argument.

Avant de commencer Vous devez exécuter la commande `ipsecconf` dans la zone globale. Dans une zone IP exclusive, vous devez exécuter la commande `ipsecconf` dans la zone non globale.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil Network IPsec Management (gestion IPsec du réseau).

Si vous exécutez une version antérieure à la version Solaris 10 4/09, le profil Network IPsec Management n'est pas disponible. Utilisez le profil Network Security.

Pour créer un rôle incluant un profil de sécurité réseau et attribuer ce rôle à un utilisateur, reportez-vous à la section "Configuration d'un rôle pour la sécurité réseau" à la page 535.

2 Affichage des stratégies IPsec

a. Affichez les entrées de stratégie IPsec globales dans l'ordre dans lequel les entrées ont été insérées.

```
$ ipsecconf
```

La commande affiche chaque entrée avec un *index* suivi d'un numéro.

b. Affichez les entrées de stratégie IPsec dans l'ordre dans lequel les correspondances sont repérées.

```
$ ipsecconf -l
```

c. Affichez les entrées de stratégie IPsec, y compris les entrées définies par tunnel, dans l'ordre dans lequel les correspondances sont repérées.

```
$ ipsecconf -L
```

▼ Génération de numéros aléatoires sur un système Solaris

Si vous spécifiez les clés manuellement, leurs numéros doivent être aléatoires. Dans un système Solaris, les numéros de clé sont au format hexadécimal. D'autres systèmes d'exploitation peuvent nécessiter des numéros de clé au format ASCII. Si vous souhaitez générer des numéros de clé pour un système Solaris qui communique avec un système d'exploitation requérant le format ASCII, reportez-vous à l'Exemple 23–1.

Si votre site possède un générateur de nombres aléatoires, utilisez-le. Dans le cas contraire, vous pouvez utiliser la commande `od` avec le périphérique Solaris `/dev/random` en entrée. Pour de plus amples informations, reportez-vous à la page de manuel `od(1)`.

Dans la version Solaris 10 4/09, vous pouvez également utiliser la commande `pktool`. La syntaxe de cette commande est plus simple que la syntaxe de la commande `od`. Pour plus de détails, reportez-vous à la section "How to Generate a Symmetric Key by Using the pktool Command" du *System Administration Guide: Security Services*.

1 Générez des numéros aléatoires au format hexadécimal.

```
% od -x|-X -A n file | head -n
```

`-x` Affiche le vidage octal au format hexadécimal. Le format hexadécimal s'avère utile pour les numéros de clé. Le numéro hexadécimal obtenu s'imprime par blocs de 4 caractères.

`-X` Affiche le vidage octal au format hexadécimal. Le numéro hexadécimal obtenu s'imprime par blocs de 8 caractères.

`-A n` Supprime la base de décalage d'entrée de l'affichage.

fichier Constitue la source des numéros aléatoires.

`head -`*n* Limite l'affichage aux *n* premières lignes de la sortie de commande.

2 Combinez la sortie afin de créer une clé de longueur adéquate.

Supprime les espaces entre les numéros sur une ligne afin de créer des clés de 32 caractères. Une clé de 32 caractères correspond à 128 bits. Tout index de paramètre de sécurité (SPI, Security Parameter Index) doit être défini à l'aide d'une clé de 8 caractères. La clé doit utiliser le préfixe `0x`.

Exemple 20–3 Génération de numéros de clé pour IPsec

Dans l'exemple suivant, deux lignes de clés s'affichent par groupes de huit caractères hexadécimaux chacun.

```
% od -X -A n /dev/random | head -2
         d54d1536 4a3e0352 0faf93bd 24fd6cad
         8ecc2670 f3447465 20db0b0c c83f5a4b
```

En combinant les quatre numéros de la première ligne, vous pouvez créer une clé de 32 caractères. Un numéro de 8 caractères précédé de `0x` (`0xf3447465`, par exemple) définit une valeur de SPI adéquate.

Dans l'exemple suivant, deux lignes de clés s'affichent par groupes de quatre caractères hexadécimaux chacun.

```
% od -x -A n /dev/random | head -2
         34ce 56b2 8b1b 3677 9231 42e9 80b0 c673
         2f74 2817 8026 df68 12f4 905a db3d ef27
```

En combinant les huit numéros de la première ligne, vous pouvez créer une clé de 32 caractères.

▼ Création manuelle d'associations de sécurité IPsec

La procédure suivante fournit les numéros de clé de la procédure : "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 519. Vous générez des clés pour deux systèmes, `partym` et `enigma`. Vous générez des clés sur un système, puis utilisez les clés du premier système sur les deux systèmes.

Avant de commencer La gestion manuelle des numéros de clé pour une zone IP partagée s'effectue dans la zone globale.

1 **Générez les numéros de clé pour les SA.**

Il vous faut trois numéros aléatoires hexadécimaux pour le trafic sortant et trois autres numéros aléatoires hexadécimaux pour le trafic entrant.

Un système doit donc générer les numéros suivants :

- deux numéros aléatoires hexadécimaux comme valeur du mot-clé `spi` : un numéro pour le trafic sortant et un numéro pour le trafic entrant. Chaque numéro peut comporter huit caractères maximum.
- Deux numéros aléatoires hexadécimaux pour l'algorithme SHA1 pour authentification. Pour une clé de 160 bits, chaque numéro doit comporter 40 caractères. L'un d'eux est dédié à `dst enigma`, l'autre à `dst partym`.
- Deux numéros aléatoires hexadécimaux pour l'algorithme AES pour chiffrement. Pour une clé de 256 bits, chaque numéro doit comporter 64 caractères. L'un d'eux est dédié à `dst enigma`, l'autre à `dst partym`.

Si un générateur de nombres aléatoires est disponible sur votre site, utilisez-le. Vous pouvez également exécuter la commande `od`. La procédure est décrite à la section "Génération de numéros aléatoires sur un système Solaris" à la page 527.

2 **Connectez-vous à la console système de l'un des systèmes en tant qu'administrateur principal ou en tant que superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Exécutez la commande `ssh` pour assurer une connexion à distance sécurisée.

---

3 **Créez les SA.**

- **À partir de la version Solaris 10 4/09, suivez les étapes Étape 8 à Étape 10.**
- **Si vous exécutez une version antérieure à la version Solaris 10 4/09, suivez les étapes Étape 4 à Étape 9.**

4 **Activez le mode de la commande `ipseckey`.**

```
# ipseckey

>
```

L'invite > indique que le mode de la commande `ipseckey` est activé.

5 Lors du remplacement de SA existantes, videz les SA actuelles.

```
> flush
>
```

Pour éviter qu'un concurrent ait le temps de déceler vos SA, remplacez les numéros de clé.

Remarque – Vous devez coordonner les remplacements des clés sur les systèmes en communication. Lorsque vous remplacez les SA sur un système, vous devez également les remplacer sur le système distant.

---

6 Pour créer des SA, tapez la commande ci-dessous.

```
> add protocol spi random-hex-string \
src addr dst addr2 \
protocol-prefix_alg protocol-algorithm   \
protocol-prefixkey random-hex-string-of-algorithm-specified-length
```

Cette syntaxe permet également de remplacer les SA après les avoir vidées.

protocole
Défini sur `esp` ou `ah`.

chaîne-hex-aléatoire
Spécifie un numéro aléatoire de huit caractères maximum au format hexadécimal. Les caractères sont précédés de `0x`. Si les numéros saisis dépassent la limite définie par le SPI, le système ignore les numéros en trop. Si le nombre de numéros n'atteint pas la limite du SPI, le système complète l'entrée.

adr
Spécifie l'adresse IP d'un système.

adr2
Spécifie l'adresse IP du système homologue de *adr*.

préfixe-protocole
Défini sur `encr` ou `auth`. Le préfixe `encr` est utilisé avec le protocole `esp`. Le préfixe `auth` est utilisé avec le protocole `ah`, ainsi que pour l'authentification du protocole `esp`.

algorithme-protocole
Spécifie un algorithme pour ESP ou AH. Chaque algorithme requiert une clé d'une longueur spécifique.

MD5 et SHA1 sont des algorithmes d'authentification. SHA256 et SHA512 sont pris en charge depuis version la Solaris 10 4/09. DES, 3DES, AES et Blowfish sont des algorithmes de chiffrement.

chaîne-hex-aléatoire-longueur-requise-par-algorithme
Définit un numéro hexadécimal aléatoire de la longueur requise par l'algorithme. Par exemple, l'algorithme MD5 requiert une chaîne de 32 caractères pour sa clé de 128 bits. L'algorithme 3DES requiert une chaîne de 48 caractères pour sa clé de 192 bits.

a. Protégez les paquets sortants sur le système `enigma`, par exemple.

Utilisez les numéros aléatoires générés à l'Étape 1.

Pour Solaris 10 1/06 :

```
> add esp spi 0x8bcd1407 \
src 192.168.116.16 dst 192.168.13.213 \
encr_alg aes \
auth_alg sha1 \
encrkey c0c65b888c2ee301c84245c3da63127e92b2676105d5330e85327c1442f37d49 \
authkey 6fab07fec4f2895445500ed992ab48835b9286ff
>
```

Remarque – Le système homologue doit utiliser le même numéro et le même SPI.

b. Toujours dans le mode de la commande `ipseckey` sur le système `enigma`, protégez les paquets sortants.

Tapez les commandes suivantes pour protéger les paquets :

```
> add esp spi 0x122a43e4 \
src 192.168.13.213 dst 192.168.116.16 \
encr_alg aes \
auth_alg sha1 \
encrkey a2ea934cd62ca7fa14907cb2ad189b68e4d18c976c14f22b30829e4b1ea4d2ae \
authkey c80984bc4733cc0b7c228b9b74b988d2b7467745
>
```

Remarque – Les clés et SPI peuvent être différents pour chaque SA. Vous *devez* attribuer différentes clés et un SPI différent à chaque SA.

7 Pour quitter le mode de la commande `ipseckey`, appuyez sur Ctrl-D ou tapez `quit`.

8 Ajoutez les numéros de clé requis au fichier `/etc/inet/secret/ipseckeys`.

Dans les versions antérieures à la version Solaris 10 4/09, cette étape permet de s'assurer que les numéros de clé requis sont disponibles pour IPsec au moment de la réinitialisation.

Les lignes du fichier `/etc/inet/secret/ipseckeys` sont identiques à celles de la ligne de commande `ipseckey`.

a. Par exemple, le fichier `/etc/inet/secret/ipseckeys` du système `enigma` serait similaire à l'exemple ci-dessous :

```
# ipseckeys - This file takes the file format documented in
#   ipseckey(1m).
#   Note that naming services might not be available when this file
```

```
#   loads, just like ipsecinit.conf.
#
# for outbound packets on enigma
add esp spi 0x8bcd1407 \
   src 192.168.116.16 dst 192.168.13.213  \
   encr_alg aes \
   auth_alg sha1  \
   encrkey  c0c65b888c2ee301c84245c3da63127e92b2676105d5330e85327c1442f37d49 \
   authkey  6fab07fec4f2895445500ed992ab48835b9286ff
#
# for inbound packets
add esp spi 0x122a43e4 \
   src 192.168.13.213 dst 192.168.116.16 \
   encr_alg aes \
   auth_alg sha1  \
   encrkey a2ea934cd62ca7fa14907cb2ad189b68e4d18c976c14f22b30829e4b1ea4d2ae \
   authkey c80984bc4733cc0b7c228b9b74b988d2b7467745
```

b. Protégez le fichier à l'aide de permissions de lecture seule.

```
# chmod 400 /etc/inet/secret/ipseckeys
```

9 Répétez la procédure sur le système `partym`.

Utilisez les mêmes numéros de clé que sur `enigma`.

Les numéros de clés utilisés sur chacun des systèmes *doivent* être identiques. Comme illustré dans l'exemple ci-dessous, les commentaires du fichier `ipseckeys` constituent la seule différente. Les commentaires sont différents parce que `dst enigma` correspond à du trafic entrant sur le système `enigma` et à du trafic sortant sur le système `partym`.

```
# partym ipseckeys file
#
# for inbound packets
add esp spi 0x8bcd1407 \
   src 192.168.116.16 dst 192.168.13.213  \
   encr_alg aes \
   auth_alg sha1  \
   encrkey  c0c65b888c2ee301c84245c3da63127e92b2676105d5330e85327c1442f37d49 \
   authkey  6fab07fec4f2895445500ed992ab48835b9286ff
#
# for outbound packets
add esp spi 0x122a43e4 \
   src 192.168.13.213 dst 192.168.116.16 \
   encr_alg aes \
   auth_alg sha1  \
   encrkey a2ea934cd62ca7fa14907cb2ad189b68e4d18c976c14f22b30829e4b1ea4d2ae \
   authkey c80984bc4733cc0b7c228b9b74b988d2b7467745
```

10 Activez le service `manual-key`.

```
# svcadm enable svc:/network/ipsec/manual-key
```

Pour remplacer des clés dans la version actuelle, reportez-vous à l'Exemple 20–4.

Exemple 20–4 Remplacement des SA IPsec

Dans cet exemple, l'administrateur configure un système exécutant la version actuelle Solaris 10. L'administrateur crée de nouvelles clés, modifie les informations de clé dans le fichier `ipseckeys`, puis redémarre le service.

- Tout d'abord, l'administrateur génère les clés en effectuant la procédure de la section "Génération de numéros aléatoires sur un système Solaris" à la page 527.
- Ensuite, l'administrateur utilise les clés générées dans le fichier `/etc/inet/secret/ipseckeys`.

  L'administrateur a utilisé les mêmes algorithmes. Par conséquent, l'administrateur change les valeurs de `SPI`, `encrkey` et `authkey` uniquement :

```
add esp spi 0x8xzy1492 \
   src 192.168.116.16 dst 192.168.13.213  \
   encr_alg aes \
   auth_alg sha1  \
   encrkey 0a1f3886b06ebd7d39f6f89e4c29c93f2741c6fa598a38af969907a29ab1b42a \
   authkey a7230aabf513f35785da73e33b064608be41f69a
#
# add esp spi 0x177xce34\
   src 192.168.13.213 dst 192.168.116.16 \
   encr_alg aes \
   auth_alg sha1  \
   encrkey 4ef5be40bf93498017b2151d788bb37e372f091add9b11149fba42435fefe328 \
   authkey 0e1875d9ff8e42ab652766a5cad49f38c9152821
```

- Enfin, l'administrateur redémarre le service `manual-key`. La commande remet à zéro les anciennes clés avant l'ajout de nouvelles clés.

```
# svcadm restart manual-key
```

▼ Vérification de la protection des paquets par IPsec

Pour vérifier que les paquets sont protégés, testez la connexion à l'aide de la commande `snoop`. Les préfixes suivants peuvent apparaître dans la sortie `snoop` :

- Le préfixe `AH:` indique que AH protège les en-têtes. `AH:` s'affiche si le trafic est protégé à l'aide d'`auth_alg`.
- Le préfixe `ESP:` indique le transfert de données chiffrées. `ESP:` s'affiche si le trafic est protégé à l'aide d'`encr_auth_alg` ou d'`encr_alg`.

Avant de commencer Pour créer la sortie `snoop`, vous devez être superutilisateur ou prendre un rôle équivalent. Vous devez avoir accès aux deux systèmes afin de tester la connexion.

1 Sur un système, par exemple `partym`, connectez-vous en tant que superutilisateur.

```
% su -
Password:       Type root password
#
```

2 À partir du système `partym`, préparez l'analyse des paquets à l'aide de la commande snoop à partir d'un système distant.

Dans une fenêtre de terminal sur `partym`, analysez les paquets du système `enigma`.

```
# snoop -v enigma
Using device /dev/hme (promiscuous mode)
```

3 Envoyez un paquet à partir du système distant.

Dans une autre fenêtre de terminal, connectez-vous à distance au système `enigma`. Tapez le mot de passe. Ensuite, connectez-vous en tant que superutilisateur et envoyez un paquet du système `enigma` vers le système `partym`. Le paquet doit être capturé à l'aide de la commande `snoop -v enigma`.

```
% ssh enigma
Password:       Type your password
% su -
Password:       Type root password
# ping partym
```

4 Examinez la sortie de la commande `snoop`.

Sur le système `partym`, la sortie devrait contenir les informations `AH` et `ESP` après les informations d'en-tête `IP` initiales. Les informations `AH` et `ESP` semblables à l'exemple ci-dessous indiquent que les paquets sont protégés :

```
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 -----
...
```

▼ Configuration d'un rôle pour la sécurité réseau

Si vous administrez vos systèmes selon le modèle RBAC (Role-Based Access Control, contrôle d'accès à base de rôles), suivez cette procédure pour générer un rôle de gestion ou de sécurité du réseau.

1 Recherchez les profils de droit réseau dans la base de données `prof_attr`.

Dans la version actuelle, le résultat est semblable à ce qui suit :

```
% cd /etc/security
% grep Network prof_attr
Network IPsec Management:::Manage IPsec and IKE...
Network Link Security:::Manage network link security...
Network Management:::Manage the host and network configuration...
Network Security:::Manage network and host security...
Network Wifi Management:::Manage wifi network configuration...
Network Wifi Security:::Manage wifi network security...
```

Si vous exécutez une version antérieure à la version Solaris 10 4/09, la sortie est semblable à ce qui suit :

```
% cd /etc/security
% grep Network prof_attr
Network Management:::Manage the host and network configuration
Network Security:::Manage network and host security
System Administrator::: Network Management
```

Le profil de gestion du réseau est un profil supplémentaire inclus dans le profil d'administrateur système. Si vous avez attribué le profil de droits d'administrateur système à un rôle, alors ce dernier permet d'exécuter les commandes définies dans le profil de gestion du réseau.

2 Déterminez les commandes incluses dans le profil de droits de gestion du réseau.

```
% grep "Network Management" /etc/security/exec_attr
Network Management:solaris:cmd:::/usr/sbin/ifconfig:privs=sys_net_config
...
Network Management:suser:cmd:::/usr/sbin/snoop:uid=0
```

Les commandes de stratégie `solaris` s'exécutent avec un privilège (`privs=sys_net_config`). Les commandes de stratégie `suser` s'exécutent en tant que superutilisateur (`uid=0`).

3 Choisissez l'étendue des rôles de sécurité réseau sur votre site.

Basez votre choix sur les profils de droits définis lors de l'Étape 1.

- **Pour créer un rôle qui gère l'ensemble de la sécurité du réseau, utilisez le profil de droits Network Security.**
- **Dans la version actuelle, pour créer un rôle qui gère IPsec et IKE uniquement, utilisez le profil de droits Network IPsec Management.**

4 Créez un rôle de sécurité réseau incluant le profil de droits Network Management.

Un rôle auquel est appliqué le profil de droits Network Security ou Network IPsec Management, en plus du profil Network Management, peut exécuter les commandes `ifconfig`, `snoop`, `ipsecconf` et `ipseckey`, entre autres, avec les privilèges appropriés.

Pour créer un rôle et l'attribuer à un utilisateur, ainsi que pour enregistrer les modifications avec le service de noms, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services* .

Exemple 20–5 Répartition des responsabilités de sécurité réseau entre les rôles

Dans cet exemple, l'administrateur répartit les responsabilités de sécurité réseau entre deux rôles. Un rôle peut administrer la sécurité des connexions Wi-Fi et des liens et un autre rôle administrer IPsec et IKE. Chaque rôle est assigné à trois personnes, une personne par période de travail.

Ces rôles sont créés par l'administrateur comme suit :

- L'administrateur nomme le premier rôle LinkWifi.
  - L'administrateur attribue au rôle les profils de droits Network Wifi, Network Link Security et Network Management.
  - Ensuite, l'administrateur attribue le rôle LinkWifi aux utilisateurs appropriés.
- L'administrateur nomme le deuxième rôle Administrateur IPsec.
  - L'administrateur attribue au rôle les profils de droits Network IPsec Management et Network Management.
  - Ensuite, l'administrateur attribue le rôle d'administrateur IPsec aux utilisateurs appropriés.

▼ Procédure de gestion des services IKE et IPsec

Les étapes suivantes présentent les utilisations les plus probables des services SMF pour IPsec, IKE et la gestion manuelle des clés. Par défaut, les services `policy` et `ipsecalgs` sont activés. Également par défaut, les services `ike` et `manual-key` sont désactivés.

1 Pour gérer la stratégie IPsec, effectuez l'une des opérations suivantes :

- **Après l'ajout de nouvelles stratégies au fichier `.conf`, actualisez le service `policy`.**

```
# svcadm refresh svc:/network/ipsec/policy
```

- **Après la modification de la valeur d'une propriété du service, affichez la valeur de la propriété, puis actualisez et redémarrez le service `policy`.**

```
# svccfg -s policy setprop config/config_file=/etc/inet/MyIpsecinit.conf
# svcprop -p config/config_file policy
```

```
/etc/inet/MyIpsecinit.conf
# svcadm refresh svc:/network/ipsec/policy
# svcadm restart svc:/network/ipsec/policy
```

2. **Pour gérer automatiquement les clés, effectuez l'une des opérations suivantes :**

   - **Après l'ajout d'entrées dans le fichier `/etc/inet/ike/config`, activez le service `ike`.**

     ```
     # svcadm enable svc:/network/ipsec/ike
     ```

   - **Après modification des entrées dans le fichier `/etc/inet/ike/config`, actualisez le service `ike`.**

     ```
     # svcadm refresh svc:/network/ipsec/ike
     ```

   - **Après la modification de la valeur d'une propriété du service, affichez la valeur de la propriété, puis actualisez et redémarrez le service.**

     ```
     # svccfg -s ike setprop config/admin_privilege=modkeys
     # svcprop -p config/admin_privilege ike
     modkeys
     # svcadm refresh svc:/network/ipsec/ike
     # svcadm restart svc:/network/ipsec/ike
     ```

   - **Pour arrêter le service `ike`, désactivez-le.**

     ```
     # svcadm disable svc:/network/ipsec/ike
     ```

3. **Pour gérer manuellement les clés, effectuez l'une des opérations suivantes :**

   - **Après l'ajout d'entrées pour le fichier `/etc/inet/secret/ipseckeys`, activez le service `manual-key`.**

     ```
     # svcadm enable svc:/network/ipsec/manual-key
     ```

   - **Une fois que vous avez modifié le fichier `ipseckeys`, actualisez le service.**

     ```
     # svcadm refresh manual-key
     ```

   - **Après la modification de la valeur d'une propriété du service, affichez la valeur de la propriété, puis actualisez et redémarrez le service.**

     ```
     # svccfg -s manual-key setprop config/config_file=/etc/inet/secret/MyIpseckeyfile
     # svcprop -p config/config_file manual-key
     /etc/inet/secret/MyIpseckeyfile
     # svcadm refresh svc:/network/ipsec/manual-key
     # svcadm restart svc:/network/ipsec/manual-key
     ```

   - **Pour empêcher la gestion manuelle des clés, désactivez le service `manual-key`.**

     ```
     # svcadm disable svc:/network/ipsec/manual-key
     ```

4. **Si vous modifiez le tableau des protocoles IPsec et des algorithmes, actualisez le service `ipsecalgs`.**

   ```
   # svcadm refresh svc:/network/ipsec/ipsecalgs
   ```

Erreurs fréquentes Pour connaître l'état d'un service, utilisez la commande de *service* `svcs`. Si le service est en mode `maintenance`, suivez les suggestions de débogage dans la sortie de la commande de *service* `svcs -x`.

Protection d'un VPN à l'aide d'IPsec

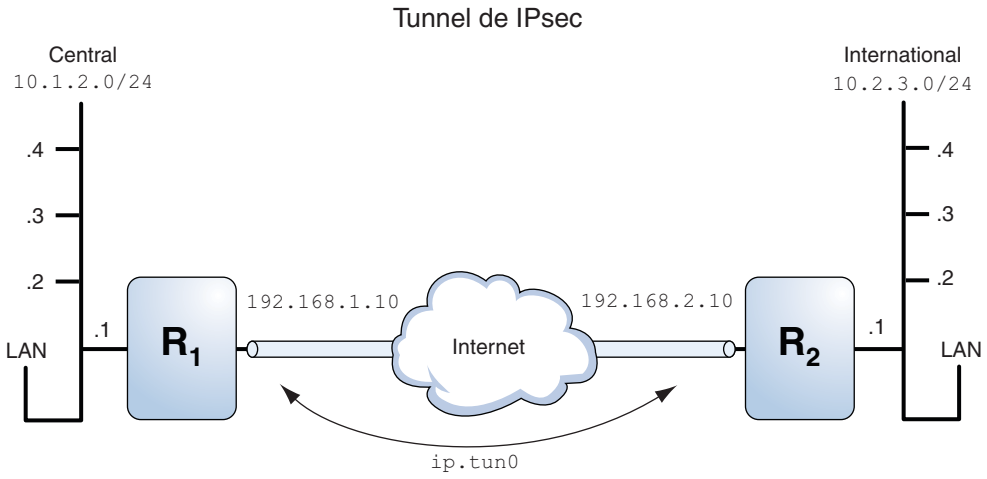
Les tunnels IPsec peuvent protéger un VPN. Dans la version Solaris 10 7/07, un tunnel peut être en mode Tunnel ou en mode Transport. Le *mode Tunnel* est compatible avec l'implémentation d'IPsec par d'autres fournisseurs. Le *mode Transport* est compatible avec les versions précédentes du SE Solaris. Les modes de tunnel sont expliqués à la section "Modes Transport et Tunnel dans IPsec" à la page 508.

Les tunnels en mode Tunnel permettent un contrôle plus détaillé du trafic. En mode Tunnel, vous pouvez spécifier la protection particulière à appliquer pour une adresse IP interne, selon un niveau de détail allant jusqu'au port.

- Des exemples de stratégies IPsec pour les tunnels en mode Tunnel sont fournis à la section "Protection d'un VPN à l'aide d'IPsec via des tunnels en mode Tunnel (exemple)" à la page 538.
- Les procédures de protection d'un VPN sont décrites à la section "Protection d'un VPN à l'aide d'IPsec (liste des tâches)" à la page 541.

Protection d'un VPN à l'aide d'IPsec via des tunnels en mode Tunnel (exemple)

FIGURE 20–1 Diagramme de tunnel IPsec



Les exemples ci-dessous considèrent que le tunnel est configuré pour tous les sous-réseaux des LAN :

```
## Tunnel configuration ##
# Tunnel name is ip.tun0
# Intranet point for the source is 10.1.2.1
# Intranet point for the destination is 10.2.3.1
# Tunnel source is 192.168.1.10
# Tunnel destination is 192.168.2.10
```

EXEMPLE 20–6 Création d'un tunnel utilisable par tous les sous-réseaux

Dans cet exemple, l'intégralité du trafic issu des LAN locaux du LAN Central de la Figure 20–1 peut être mis en tunnel du routeur 1 au routeur 2, puis fourni à tous les LAN locaux du LAN Overseas. Le trafic est chiffré à l'aide d'AES.

```
## IPsec policy ##
{tunnel ip.tun0 negotiate tunnel}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

EXEMPLE 20–7 Création d'un tunnel connectant deux sous-réseaux

Dans cet exemple, seul le trafic entre le sous-réseau `10.1.2.0/24` du LAN Central et le sous-réseau `10.2.3.0/24` du LAN Overseas est mis en tunnel et chiffré. En l'absence d'autres stratégies IPsec pour Central, si le LAN Central tente de transmettre des données pour d'autres LAN via ce tunnel, le trafic est abandonné au niveau du routeur 1.

```
## IPsec policy ##
{tunnel ip.tun0 negotiate tunnel laddr 10.1.2.0/24 raddr 10.2.3.0/24}
 ipsec {encr_algs aes encr_auth_algs md5 sha1 shared}
```

EXEMPLE 20–8 Création d'un tunnel pour le trafic d'e-mail entre deux sous-réseaux

Dans cet exemple, un tunnel est créé pour les échanges d'e-mail exclusivement. Le trafic est fourni à partir du sous-réseau `10.1.2.0/24` du LAN Central vers le serveur de courrier sur le sous-réseau `10.2.3.0/24` du LAN Overseas. L'e-mail est chiffré à l'aide de Blowfish. Les stratégies s'appliquent aux ports de courrier locaux et distants. La stratégie `rport` protège l'e-mail envoyé par Central au port de courrier distant d'Overseas. La stratégie `lport` protège l'e-mail reçu par Central en provenance d'Overseas sur le port local 25.

```
## IPsec policy for email from Central to Overseas ##
{tunnel ip.tun0 negotiate tunnel ulp tcp rport 25
 laddr 10.1.2.0/24 raddr 10.2.3.0/24}
 ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}

## IPsec policy for email from Overseas to Central ##
{tunnel ip.tun0 negotiate tunnel ulp tcp lport 25
 laddr 10.1.2.0/24 raddr 10.2.3.0/24}
 ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}
```

EXEMPLE 20–9 Création d'un tunnel pour le trafic FTP pour tous les sous-réseaux

Dans cet exemple, la stratégie IPsec protège les ports FTP de la Figure 20–1 à l'aide d'AES pour tous les sous-réseaux du LAN Central vers tous les sous-réseaux du LAN Overseas. Cette configuration fonctionne pour le mode actif de FTP.

```
## IPsec policy for outbound FTP from Central to Overseas ##
{tunnel ip.tun0 negotiate tunnel ulp tcp rport 21}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
{tunnel ip.tun0 negotiate tunnel ulp tcp lport 20}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## IPsec policy for inbound FTP from Central to Overseas ##
{tunnel ip.tun0 negotiate tunnel ulp tcp lport 21}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
{tunnel ip.tun0 negotiate tunnel ulp tcp rport 20}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Protection d'un VPN à l'aide d'IPsec (liste des tâches)

La liste des tâches suivante fait référence aux procédures de configuration d'IPsec dans le cadre de la protection du trafic sur Internet. Ces procédures permettent de configurer un VPN (Virtual Private Network, réseau privé virtuel) sécurisé entre deux systèmes séparés par Internet. Grâce à cette technologie, vous pouvez notamment protéger le trafic de données entre les employés travaillant à domicile et le site de la société.

Tâche	Description	Voir
Protection du trafic de tunnel en mode Tunnel sur IPv4	Protège le trafic en mode Tunnel entre deux systèmes Solaris 10, deux systèmes Oracle Solaris ou entre un système Solaris 10 et un système Oracle Solaris Express. Le système Solaris 10 doit exécuter au moins la version Solaris 10 7/07. Protège également le trafic en mode Tunnel entre un système Solaris 10 ou un système Oracle Solaris Express et un système exécuté sur une autre plate-forme. Le système Solaris 10 doit exécuter au moins la version Solaris 10 7/07.	"Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544
Protection du trafic de tunnel en mode Tunnel sur IPv6	Protège le trafic en mode Tunnel entre deux systèmes Oracle Solaris utilisant le protocole IPv6.	"Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv6" à la page 554
Protection du trafic de tunnel en mode Transport sur IPv4	Protège le trafic en mode Transport entre deux systèmes Solaris 10, deux systèmes Solaris ou entre un système Solaris 10 et un système Oracle Solaris. Le système Solaris 10 doit exécuter au moins la version Solaris 10 7/07. Protège également le trafic en mode Transport entre un système exécutant une version antérieure de SE Solaris et un système Solaris 10 ou Oracle Solaris. Le système Solaris 10 doit exécuter au moins la version Solaris 10 7/07.	"Protection d'un VPN à l'aide d'un tunnel IPsec en mode Transport sur IPv4" à la page 559
	Protège le trafic à l'aide d'une syntaxe plus ancienne et désapprouvée Cette méthode s'avère particulièrement utile pour communiquer avec un système exécutant une version antérieure du SE Solaris. Elle simplifie la comparaison des fichiers de configuration sur les deux systèmes.	Exemple 20–11 Exemple 20–16
Protection du trafic de tunnel en mode Transport sur IPv6	Protège le trafic en mode Tunnel entre deux systèmes Oracle Solaris utilisant le protocole IPv6.	"Protection d'un VPN à l'aide d'un tunnel IPsec en mode Transport sur IPv6" à la page 566

Tâche	Description	Voir
Protection contre l'usurpation d'adresse IP	Crée un service SMF afin d'empêcher le système de transmettre des paquets sur un réseau VPN sans que ceux-ci soient déchiffrés.	"Protection contre l'usurpation d'adresse IP" à la page 572

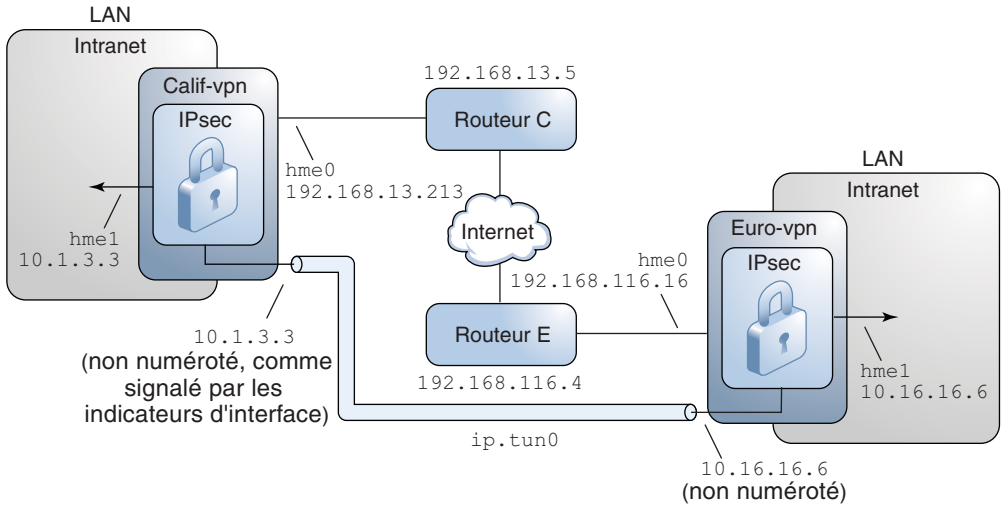
Description de la topologie réseau requise par les tâches IPsec afin de protéger un VPN

Les procédures suivant cette section sont définies pour la configuration ci-dessous. Le réseau est illustré sur la Figure 20–2.

- Chaque système utilise un espace d'adressage IPv4.

  Un exemple similaire avec des adresses IPv6 est fourni à la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv6" à la page 554.
- Chaque système possède deux interfaces. L'interface `hme0` se connecte à Internet. Dans cet exemple, les adresses IP Internet commencent par `192.168`. L'interface `hme1` se connecte au LAN de la société, son intranet. Dans cet exemple, les adresses IP intranet commencent par le numéro `10`.
- Chaque système nécessite l'authentification ESP avec l'algorithme SHA–1. L'algorithme SHA–1 requiert une clé de 160 bits.
- Chaque système nécessite le chiffrement ESP avec l'algorithme AES. L'algorithme AES utilise une clé de 128 ou 256 bits.
- Chaque système peut se connecter à un routeur bénéficiant d'un accès direct à Internet.
- Chaque système utilise des associations de sécurité partagées (SA, Security Associations).

FIGURE 20–2 Exemple de VPN entre plusieurs sites séparés par Internet



Comme l'illustration précédente l'indique, les procédures pour le réseau IPv4 utilisent les paramètres de configuration suivants :

Paramètre	Europe	Californie
Nom du système	`enigma`	`partym`
Interface intranet du système	`hme1`	`hme1`
Adresse intranet du réseau, dite également adresse *-point* dans l'Étape 7	`10.16.16.6`	`10.1.3.3`
Interface Internet du système	`hme0`	`hme0`
Adresse Internet du système, dite également adresse *tsrc* dans l'Étape 7	`192.168.116.16`	`192.168.13.213`
Nom du routeur Internet	`router-E`	`router-C`
Adresse du routeur Internet	`192.168.116.4`	`192.168.13.5`
Nom du tunnel	`ip.tun0`	`ip.tun0`

Les adresses IPv6 sont utilisées dans les procédures. Les noms de tunnel sont identiques.

Paramètre	Europe	Californie
Adresse intranet du système	`6000:6666::aaaa:1116`	`6000:3333::eeee:1113`

Paramètre	Europe	Californie
Adresse Internet du système	`2001::aaaa:6666:6666`	`2001::eeee:3333:3333`
Adresse du routeur Internet	`2001::aaaa:0:4`	`2001::eeee:0:1`

▼ Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4

En mode Tunnel, le paquet IP interne détermine la stratégie IPsec qui protège son contenu.

Cette procédure prolonge la procédure "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 519. La configuration est décrite à la section "Description de la topologie réseau requise par les tâches IPsec afin de protéger un VPN" à la page 542.

Remarque – Effectuez cette procédure sur les deux systèmes.

Outre la connexion de deux systèmes, vous connectez deux intranets qui leur sont connectés. Les systèmes de cette procédure fonctionnent comme des passerelles.

Avant de commencer Vous devez vous trouver dans la zone globale pour configurer la stratégie IPsec pour le système ou pour une zone IP partagée. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale.

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

2 Contrôlez le flux de paquets avant de configurer IPsec.

a. Assurez-vous que le transfert IP et le routage dynamique IP sont désactivés.

```
# routeadm
Configuration       Current         Current
       Option       Configuration  System State
```

```
--------------------------------------------------
IPv4 forwarding     disabled           disabled
   IPv4 routing     default (enabled)   enabled
...
```

Si le transfert IP et le routage dynamique IP sont activés, désactivez-les.

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

La désactivation du transfert IP évite le transfert des paquets d'un réseau à un autre via ce système. La commande `routeadm` est décrite à la page de manuel `routeadm(1M)`.

b. Activez le multiréseau de destination strict IP.

```
# ndd -set /dev/ip ip_strict_dst_multihoming 1
```

L'activation du multiréseau de destination strict IP assure que les paquets de l'une des adresses de destination du système arrivent à l'adresse de destination adéquate.

Lorsque le multiréseau de destination strict est activé, les paquets arrivant sur une interface particulière doivent être adressés à l'une des adresses IP locales de cette interface. Tous les autres paquets sont abandonnés, même les paquets envoyés vers d'autres adresses locales du système.

Attention – Par défaut, lors de l'initialisation du système, la valeur multiréseau est désélectionnée. Pour rendre persistante la valeur modifiée, reportez-vous à la section "Protection contre l'usurpation d'adresse IP" à la page 572.

c. Désactivez la plupart des services réseau, voire tous les services réseau.

Remarque – Si le système a été installé avec le profil SMF "limité", vous pouvez ignorer cette étape. Tous les services réseau sont désactivés, à l'exception de Solaris Secure Shell.

La désactivation des services réseau évite que le système soit affecté par les paquets IP. Par exemple, vous pouvez utiliser un démon SNMP, une connexion `telnet` ou une connexion `rlogin`.

Procédez de l'une des manières suivantes :

- Si vous exécutez Solaris 10 11/06 ou une version supérieure, exécutez le profil SMF "limité".

  ```
  # netservices limited
  ```

- Dans le cas contraire, désactivez les services réseau un à un.

  ```
  # svcadm disable network/ftp:default
  # svcadm disable network/finger:default
  # svcadm disable network/login:rlogin
  ```

```
# svcadm disable network/nfs/server:default
# svcadm disable network/rpc/rstat:default
# svcadm disable network/smtp:sendmail
# svcadm disable network/telnet:default
```

d. Assurez-vous que la plupart des services réseau sont désactivés.

Assurez-vous que les montages en loopback et le service `ssh` sont en cours d'exécution.

```
# svcs | grep network
online         Aug_02   svc:/network/loopback:default
...
online         Aug_09   svc:/network/ssh:default
```

3 Ajoutez une paire de SA entre les deux systèmes.

Procédez de l'une des manières suivantes :

- Configurez IKE de manière à gérer les clés pour les SA. Suivez l'une des procédures de la section "Configuration du protocole IKE (liste des tâches)" à la page 593 afin de configurer IKE pour le VPN.
- Si, pour une raison particulière, vous souhaitez gérer les clés manuellement, reportez-vous à la section "Création manuelle d'associations de sécurité IPsec" à la page 528.

4 Ajoutez une stratégie IPsec.

Modifiez le fichier `/etc/inet/ipsecinit.conf` afin d'ajouter la stratégie IPsec pour le VPN. Pour renforcer la stratégie, reportez-vous à l'Exemple 20–12. Vous trouverez d'autres exemples à la section "Protection d'un VPN à l'aide d'IPsec via des tunnels en mode Tunnel (exemple)" à la page 538.

Dans cette stratégie, la protection IPsec n'est pas requise entre les systèmes du réseau local et l'adresse IP interne de la passerelle, d'où l'ajout d'une déclaration `bypass`.

a. Sur le système `enigma`, saisissez l'entrée suivante dans le fichier `ipsecinit.conf` :

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.16.16.6 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate tunnel}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. Sur le système `partym`, tapez l'entrée suivante dans le fichier `ipsecinit.conf` :

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate tunnel}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

5 (Facultatif) Vérifiez la syntaxe du fichier de stratégie IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 **Pour configurer le tunnel et le protéger à l'aide d'IPsec, suivez les étapes en fonction de la version de Solaris utilisée :**

- **À partir de la version Solaris 10 4/09, suivez les étapes Étape 7 à Étape 13, puis exécutez le protocole de routage tel qu'indiqué à l'Étape 22.**
- **Si vous exécutez une version antérieure à la version Solaris 10 4/09, suivez les étapes Étape 14 à Étape 22.**

7 **Configurez le tunnel `ip.tun0` dans le fichier `/etc/hostname.ip.tun0`.**

La syntaxe du fichier est la suivante :

system1-point system2-point `tsrc` *system1-taddr* `tdst` *system2-taddr* `router up`

a. **Sur le système `enigma`, ajoutez l'entrée suivante au fichier `hostname.ip.tun0` :**

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 tdst 192.168.13.213 router up
```

b. **Sur le système `partym`, ajoutez l'entrée suivante au fichier `hostname.ip.tun0` :**

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 tdst 192.168.116.16 router up
```

8 **Protégez le tunnel à l'aide de la stratégie IPsec créée.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9 **Pour lire les informations du fichier de configuration du tunnel dans le noyau, redémarrez les services réseau.**

```
# svcadm restart svc:/network/initial:default
```

10 **Activez le transfert IP pour l'interface `hme1`.**

a. **Sur le système `enigma`, ajoutez l'entrée de routeur au fichier `/etc/hostname.hme1`.**

```
192.168.116.16 router
```

b. **Sur le système `partym`, ajoutez l'entrée de routeur au fichier `/etc/hostname.hme1`.**

```
192.168.13.213 router
```

Le transfert IP signifie que les paquets arrivant peuvent être transférés. Le transfert IP signifie également que les paquets quittant l'interface peuvent provenir d'un autre emplacement. Pour que le transfert de paquet s'effectue sans erreur, vous devez activer le transfert IP à la fois sur l'interface réceptrice et sur l'interface émettrice.

Étant donné que l'interface `hme1` se trouve *dans* l'intranet, le transfert IP doit être activé pour `hme1`. Comme `ip.tun0` connecte les deux systèmes via Internet, le transfert IP doit être activé pour `ip.tun0`.

Le transfert IP de l'interface `hme0` est désactivé afin d'éviter toute injection de paquets par un concurrent *externe* dans l'intranet protégé. Le terme *externe* fait référence à Internet.

11 Assurez-vous que les protocoles de routage n'indiquent pas la route par défaut sur l'intranet.

a. Sur le système `enigma`, ajoutez l'indicateur `private` au fichier `/etc/hostname.hme0`.

```
10.16.16.6 private
```

b. Sur le système `partym`, ajoutez l'indicateur `private` au fichier `/etc/hostname.hme0`.

```
10.1.3.3 private
```

Même si le transfert de l'IP de `hme0` est désactivé, l'implémentation d'un protocole de routage peut permettre d'annoncer l'interface. Par exemple, le protocole `in.routed` peut encore annoncer que `hme0` est disponible pour transférer des paquets à ses homologues dans l'intranet. Pour éviter ces annonces, définissez l'indicateur *private* de l'interface.

12 Ajoutez manuellement une route par défaut sur l'interface `hme0`.

La route par défaut doit correspondre à un routeur bénéficiant d'un accès direct à Internet.

a. Sur le système `enigma`, ajoutez la route suivante :

```
# route add default 192.168.116.4
```

b. Sur le système `partym`, ajoutez la route suivante :

```
# route add default 192.168.13.5
```

Même si l'interface `hme0` ne fait pas partie de l'intranet, `hme0` n'a pas besoin de passer par Internet pour atteindre le système homologue. Pour trouver son homologue, `hme0` requiert des informations sur le routage Internet. Pour le reste d'Internet, le système VPN apparaît comme étant un hôte, non un routeur. Par conséquent, vous pouvez utiliser un routeur par défaut ou exécuter le protocole de recherche de routeur pour rechercher le système. Pour de plus amples informations, reportez-vous aux pages de manuel `route`(1M) et `in.routed`(1M).

13 Pour terminer la procédure, passez à l'Étape 22 pour exécuter un protocole de routage.

14 Configurez le tunnel `ip.tun0`.

Remarque – Les étapes suivantes permettent de configurer un tunnel sur un système exécutant une version antérieure à la version Solaris 10 4/09.

Utilisez les commandes `ifconfig` pour créer l'interface point à point :

```
# ifconfig ip.tun0 plumb
```

```
# ifconfig ip.tun0 system1-point system2-point \
tsrc system1-taddr tdst system2-taddr
```

a. Sur le système `enigma`, saisissez les commandes ci-dessous :

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213
```

b. Sur le système `partym`, tapez les commandes ci-dessous :

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.1.3.3 10.16.16.6  \
tsrc 192.168.13.213 tdst 192.168.116.16
```

15 Protégez le tunnel à l'aide de la stratégie IPsec créée.

```
# ipsecconf
```

16 Affichez le routeur pour le tunnel.

```
# ifconfig ip.tun0 router up
```

17 Activez le transfert IP pour l'interface `hme1`.

```
# ifconfig hme1 router
```

Le transfert IP signifie que les paquets arrivant peuvent être transférés. Le transfert IP signifie également que les paquets quittant l'interface peuvent provenir d'un autre emplacement. Pour que le transfert de paquet s'effectue sans erreur, vous devez activer le transfert IP à la fois sur l'interface réceptrice et sur l'interface émettrice.

Comme l'interface `hme1` se trouve *dans* l'intranet, le transfert IP doit être activé pour `hme1`. Comme `ip.tun0` connecte les deux systèmes via Internet, le transfert IP doit être activé pour `ip.tun0`.

Le transfert IP de l'interface `hme0` est désactivé afin d'éviter toute injection de paquets par un concurrent *externe* dans l'intranet protégé. Le terme *externe* fait référence à Internet.

18 Assurez-vous que les protocoles de routage n'indiquent pas la route par défaut sur l'intranet.

```
# ifconfig hme0 private
```

Même si le transfert IP de `hme0` est désactivé, l'implémentation d'un protocole de routage est susceptible d'annoncer l'interface. Par exemple, le protocole `in.routed` peut encore annoncer que `hme0` est disponible pour transférer des paquets à ses homologues dans l'intranet. Pour éviter ces annonces, définissez l'indicateur *private* de l'interface.

19 Ajoutez manuellement une route par défaut à travers `hme0`.

La route par défaut doit correspondre à un routeur bénéficiant d'un accès direct à Internet.

a. Sur le système `enigma`, ajoutez la route suivante :

```
# route add default 192.168.116.4
```

b. Sur le système `partym`, ajoutez la route suivante :

```
# route add default 192.168.13.5
```

Même si l'interface `hme0` ne fait pas partie de l'intranet, `hme0` n'a pas besoin de passer par Internet pour atteindre le système homologue. Pour trouver son homologue, `hme0` requiert des informations sur le routage Internet. Pour le reste d'Internet, le système VPN apparaît comme étant un hôte, non un routeur. Par conséquent, vous pouvez utiliser un routeur par défaut ou exécuter le protocole de recherche de routeur pour rechercher le système. Pour de plus amples informations, reportez-vous aux pages de manuel `route`(1M) et `in.routed`(1M).

20 Assurez-vous que le VPN démarre à la réinitialisation en ajoutant une entrée au fichier `/etc/hostname.ip.tun0`.

system1-point system2-point `tsrc` *system1-taddr* `tdst` *system2-taddr* `router up`

a. Sur le système `enigma`, ajoutez l'entrée suivante au fichier `hostname.ip.tun0` :

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 tdst 192.168.13.213 router up
```

b. Sur le système `partym`, ajoutez l'entrée suivante au fichier `hostname.ip.tun0` :

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 tdst 192.168.116.16 router up
```

21 Configurez les fichiers d'interface afin de transmettre les paramètres adéquats au démon de routage.

a. Sur le système `enigma`, modifiez les fichiers `/etc/hostname.` *interface*.

```
# cat /etc/hostname.hme0
## enigma
10.16.16.6 private

# cat /etc/hostname.hme1
## enigma
192.168.116.16 router
```

b. Sur le système `partym`, modifiez les fichiers `/etc/hostname.` *interface*.

```
# cat /etc/hostname.hme0
## partym
10.1.3.3 private

# cat /etc/hostname.hme1
## partym
192.168.13.213 router
```

22 Exécutez un protocole de routage.

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

Vous devrez peut-être configurer le protocole de routage avant de l'exécuter. Pour plus d'informations, reportez-vous à la section "Protocoles de routage dans Oracle Solaris" à la page 257. La procédure est décrite à la section "Configuration d'un routeur IPv4" à la page 124.

Exemple 20–10 Création temporaire des tunnels lors du test

Dans cet exemple, l'administrateur teste la création d'un tunnel sur un système Solaris 10 4/09. Par la suite, l'administrateur utilise la procédure "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544 pour rendre les tunnels permanents. Lors du test, l'administrateur effectue les séries d'actions suivantes sur les systèmes `system1` et `system2` :

- Sur les deux systèmes, l'administrateur exécute les cinq premières étapes de la procédure décrite à la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544.
- L'administrateur utilise la commande `ifconfig` pour monter et configurer un tunnel temporaire.

```
system1 # ifconfig ip.tun0 plumb
system1 # ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
          tsrc 192.168.116.16 tdst 192.168.13.213

# ssh system2
Password:      admin-password-on-system2
system2 # ifconfig ip.tun0 plumb
system2 # ifconfig ip.tun0  10.1.3.3 10.16.16.6 \
          tsrc 192.168.13.213 tdst 192.168.116.16
```

- L'administrateur active la stratégie IPsec sur le tunnel. La stratégie a été créée à l'Étape 4 de la procédure "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544.

```
system1 # svcadm refresh svc:/network/ipsec/policy:default
system2 # svcadm refresh svc:/network/ipsec/policy:default
```

- L'administrateur convertit l'interface Internet en routeur et empêche les protocoles de routage d'accéder à l'interface intranet.

```
system1 # ifconfig hme1 router ; ifconfig hme0 private

system2 # ifconfig hme1 router ; ifconfig hme0 private
```

- L'administrateur ajoute manuellement le routage et exécute sur les deux systèmes le protocole de routage en effectuant l'Étape 12 et l'Étape 22 de la procédure décrite à la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544.

Exemple 20–11 Création d'un tunnel sur un système Solaris de version antérieure en utilisant la ligne de commande

Dans la version Solaris 10 7/07, la syntaxe de la commande `ifconfig` a été simplifiée. Dans cet exemple, l'administrateur teste la création d'un tunnel sur un système exécutant une version de Solaris antérieure à la version Solaris 10 7/07. À l'aide de la syntaxe d'origine de la commande `ifconfig`, l'administrateur peut utiliser les mêmes commandes sur les deux systèmes communicants. Ensuite, l'administrateur doit effectuer la procédure de la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544 pour rendre les tunnels permanents.

Lors du test, l'administrateur doit effectuer les étapes suivantes sur les systèmes `system1` et `system2` :

- Sur les deux systèmes, l'administrateur exécute les cinq premières étapes de la procédure décrite à la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544.
- L'administrateur monte et configure le tunnel.

```
system1 # ifconfig ip.tun0 plumb
system1 # ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
          tsrc 192.168.116.16 tdst 192.168.13.213 \
          encr_algs aes encr_auth_algs sha1
system1 # ifconfig ip.tun0 router up

# ssh system2
Password:      admin-password-on-system2
system2 # ifconfig ip.tun0 plumb
system2 # ifconfig ip.tun0 10.1.3.3  10.16.16.6 \
          tsrc 192.168.13.213 tdst 192.168.116.16 \
          encr_algs aes encr_auth_algs sha1
system2 # ifconfig ip.tun0 router up
```

- L'administrateur active la stratégie IPsec sur le tunnel. La stratégie a été créée à l'Étape 4 de la procédure "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544.

```
system1 # svcadm refresh svc:/network/ipsec/policy:default
system2 # svcadm refresh svc:/network/ipsec/policy:default
```

- L'administrateur convertit l'interface Internet en routeur et empêche les protocoles de routage d'accéder à l'interface intranet.

```
system1 # ifconfig hme1 router ; ifconfig hme0 private
system2 # ifconfig hme1 router ; ifconfig hme0 private
```

- L'administrateur ajoute le routage sur les deux systèmes en exécutant l'Étape 12 et l'Étape 22 de la procédure de la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544.

Exemple 20–12 Requête de stratégie IPsec sur tous les systèmes sur un LAN

Dans cet exemple, l'administrateur met en commentaire la stratégie `bypass` configurée à l'Étape 4, ce qui renforce la protection. Avec cette configuration de stratégie, chaque système du LAN doit activer IPsec afin de communiquer avec le routeur.

```
# LAN traffic must implement IPsec.
# {laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate tunnel} ipsec {encr_algs aes encr_auth_algs sha1}
```

Exemple 20–13 Utilisation d'IPsec pour protéger le trafic Telnet différemment du trafic SMTP

Dans cet exemple, la première règle protège le trafic `telnet` sur le port 23 avec Blowfish et SHA-1. La deuxième règle protège le trafic SMTP sur le port 25 avec AES et MD5.

```
{laddr 10.1.3.3 ulp tcp dport 23 dir both}
  ipsec {encr_algs blowfish encr_auth_algs sha1 sa unique}
{laddr 10.1.3.3 ulp tcp dport 25 dir both}
 ipsec {encr_algs aes encr_auth_algs md5 sa unique}
```

Exemple 20–14 Utilisation d'un tunnel IPsec en mode Tunnel pour protéger un sous-réseau différemment d'un autre trafic réseau

La configuration de tunnel ci-dessous protège l'intégralité du trafic du sous-réseau `10.1.3.0/24` via le tunnel :

```
{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

Les configurations de tunnel ci-dessous protègent le trafic du sous-réseau `10.1.3.0/24` vers d'autres sous-réseaux via le tunnel. Les sous-réseaux dont le numéro commence par `10.2.`*x.x* traversent le tunnel.

```
{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24 raddr 10.2.1.0/24}
  ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}

{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24 raddr 10.2.2.0/24}
  ipsec {encr_algs blowfish encr_auth_algs sha1 sa shared}

{tunnel ip.tun0 negotiate tunnel laddr 10.1.3.0/24 raddr 10.2.3.0/24}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

▼ Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv6

Les étapes de configuration d'un VPN sur un réseau IPv6 sont identiques à celles de la configuration d'un VPN sur un réseau IPv4. Toutefois, la syntaxe des commandes est légèrement différente. Les raisons pour lesquelles des commandes spécifiques sont requises sont expliquées en détail aux étapes correspondantes de la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544.

Remarque – Effectuez cette procédure sur les deux systèmes.

Cette procédure utilise les paramètres de configuration ci-dessous.

Paramètre	Europe	Californie
Nom du système	`enigma`	`partym`
Interface intranet du système	`hme1`	`hme1`
Interface Internet du système	`hme0`	`hme0`
Adresse intranet du système	`6000:6666::aaaa:1116`	`6000:3333::eeee:1113`
Adresse Internet du système	`2001::aaaa:6666:6666`	`2001::eeee:3333:3333`
Nom du routeur Internet	`router-E`	`router-C`
Adresse du routeur Internet	`2001::aaaa:0:4`	`2001::eeee:0:1`
Nom du tunnel	`ip6.tun0`	`ip6.tun0`

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

2 Contrôlez le flux de paquets avant de configurer IPsec.

Les effets de ces commandes sont décrits à l'Étape 2 de la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4" à la page 544.

a. Assurez-vous que le transfert IP et le routage dynamique IP sont désactivés.

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

Si le transfert IP et le routage dynamique IP sont activés, vous pouvez les désactiver en tapant :

```
# routeadm -d ipv6-forwarding -d ipv6-routing
# routeadm -u
```

b. Activez le multiréseau de destination strict IP.

```
# ndd -set /dev/ip ip6_strict_dst_multihoming 1
```

Attention – La valeur par défaut de `ip6_strict_dst_multihoming` est rétablie lors de l'initialisation du système. Pour rendre persistante la valeur modifiée, reportez-vous à la section "Protection contre l'usurpation d'adresse IP" à la page 572.

c. Désactivez la plupart des services réseau, voire tous les services réseau.

Remarque – Si le système a été installé avec le profil SMF "limité", vous pouvez ignorer cette étape. Tous les services réseau sont désactivés, à l'exception de Solaris Secure Shell.

La désactivation des services réseau évite que le système soit affecté par les paquets IP. Par exemple, vous pouvez utiliser un démon SNMP, une connexion `telnet` ou une connexion `rlogin`.

Procédez de l'une des manières suivantes :

- Si vous exécutez Solaris 10 11/06 ou une version supérieure, exécutez le profil SMF "limité".

  ```
  # netservices limited
  ```

- Dans le cas contraire, désactivez les services réseau un à un.

  ```
  # svcadm disable network/ftp:default
  # svcadm disable network/finger:default
  # svcadm disable network/login:rlogin
  # svcadm disable network/nfs/server:default
  ```

```
# svcadm disable network/rpc/rstat:default
# svcadm disable network/smtp:sendmail
# svcadm disable network/telnet:default
```

d. Assurez-vous que la plupart des services réseau sont désactivés.

Assurez-vous que les montages en loopback et le service `ssh` sont en cours d'exécution.

```
# svcs | grep network
online         Aug_02   svc:/network/loopback:default
...
online         Aug_09   svc:/network/ssh:default
```

3 Ajoutez une paire de SA entre les deux systèmes.

Procédez de l'une des manières suivantes :

- Configurez IKE de manière à gérer les clés pour les SA. Suivez l'une des procédures de la section "Configuration du protocole IKE (liste des tâches)" à la page 593 afin de configurer IKE pour le VPN.
- Si, pour une raison particulière, vous souhaitez gérer les clés manuellement, reportez-vous à la section "Création manuelle d'associations de sécurité IPsec" à la page 528.

4 Ajoutez la stratégie IPsec pour le réseau VPN.

Modifiez le fichier `/etc/inet/ipsecinit.conf` afin d'ajouter la stratégie IPsec pour le VPN.

a. Sur le système `enigma`, saisissez l'entrée suivante dans le fichier `ipsecinit.conf` :

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic to and from this host can bypass IPsec.
{laddr 6000:6666::aaaa:1116 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate tunnel}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. Sur le système `partym`, tapez l'entrée suivante dans le fichier `ipsecinit.conf` :

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic to and from this host can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate tunnel}
  ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

5 (Facultatif) Vérifiez la syntaxe du fichier de stratégie IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6. **Pour configurer le tunnel et le protéger à l'aide d'IPsec, suivez les étapes en fonction de la version de Solaris utilisée :**

   - **À partir de la version Solaris 10 4/09, suivez les étapes Étape 7 à Étape 13, puis exécutez le protocole de routage tel qu'indiqué à l'Étape 22.**
   - **Si vous exécutez une version antérieure à la version Solaris 10 4/09, suivez les étapes Étape 14 à Étape 22.**

7. **Configurez le tunnel `ip6.tun0` dans le fichier `/etc/hostname.ip6.tun0`.**

   a. **Sur le système `enigma`, ajoutez l'entrée suivante au fichier `hostname.ip6.tun0` :**

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 router up
```

   b. **Sur le système `partym`, ajoutez l'entrée suivante au fichier `hostname.ip6.tun0` :**

```
6000:3333::eeee:1113  6000:6666::aaaa:1116 tsrc 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666 router up
```

8. **Protégez le tunnel à l'aide de la stratégie IPsec créée.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9. **Pour lire les informations du fichier de configuration du tunnel dans le noyau, redémarrez les services réseau.**

```
# svcadm restart svc:/network/initial:default
```

10. **Activez le transfert IP pour l'interface `hme1`.**

    a. **Sur le système `enigma`, ajoutez l'entrée de routeur au fichier `/etc/hostname6.hme1`.**

```
2001::aaaa:6666:6666 inet6 router
```

    b. **Sur le système `partym`, ajoutez l'entrée de routeur au fichier `/etc/hostname6.hme1`.**

```
2001::eeee:3333:3333 inet6 router
```

11. **Assurez-vous que les protocoles de routage n'indiquent pas la route par défaut sur l'intranet.**

    a. **Sur le système `enigma`, ajoutez l'indicateur `private` au fichier `/etc/hostname6.hme0`.**

```
6000:6666::aaaa:1116 inet6 private
```

    b. **Sur le système `partym`, ajoutez l'indicateur `private` au fichier `/etc/hostname6.hme0`.**

```
6000:3333::eeee:1113 inet6 private
```

12. **Ajoutez manuellement une route par défaut à travers `hme0`.**

    a. **Sur le système `enigma`, ajoutez la route suivante :**

```
# route add -inet6 default 2001::aaaa:0:4
```

b. Sur le système `partym`, ajoutez la route suivante :

```
# route add -inet6 default 2001::eeee:0:1
```

13 Pour terminer la procédure, passez à l'Étape 22 pour exécuter un protocole de routage.

14 Configurez un tunnel sécurisé `ip6.tun0`.

Remarque – Les étapes suivantes permettent de configurer un tunnel sur un système exécutant une version antérieure à la version Solaris 10 4/09.

---

a. Sur le système `enigma`, saisissez les commandes ci-dessous :

```
# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666   tdst 2001::eeee:3333:3333
```

b. Sur le système `partym`, tapez les commandes ci-dessous :

```
# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6 6000:3333::eeee:1113 6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333   tdst 2001::aaaa:6666:6666
```

15 Protégez le tunnel à l'aide de la stratégie IPsec créée.

```
# ipsecconf
```

16 Affichez le routeur pour le tunnel.

```
# ifconfig ip6.tun0 router up
```

17 Sur chaque système, exécutez le transfert IP pour l'interface `hme1`.

```
# ifconfig hme1 router
```

18 Assurez-vous que les protocoles de routage n'indiquent pas la route par défaut sur l'intranet.

```
# ifconfig hme0 private
```

19 Ajoutez manuellement une route par défaut à travers `hme0`.

La route par défaut doit correspondre à un routeur bénéficiant d'un accès direct à Internet.

a. Sur le système `enigma`, ajoutez la route suivante :

```
# route add -inet6 default 2001::aaaa:0:4
```

b. Sur le système `partym`, ajoutez la route suivante :

```
# route add -inet6 default 2001::eeee:0:1
```

20 Assurez-vous que le VPN démarre à la réinitialisation en ajoutant une entrée au fichier `/etc/hostname6.ip6.tun0`.

L'entrée réplique les paramètres spécifiés dans la commande `ifconfig` lors de l'Étape 14.

a. Sur le système `enigma`, ajoutez l'entrée suivante au fichier `hostname6.ip6.tun0` :

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666  tdst 2001::eeee:3333:3333 router up
```

b. Sur le système `partym`, ajoutez l'entrée suivante au fichier `hostname6.ip6.tun0` :

```
6000:3333::eeee:1113 6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333   tdst 2001::aaaa:6666:6666  router up
```

21 Sur chaque système, configurez les fichiers d'interface afin de transmettre les paramètres adéquats au démon de routage.

a. Sur le système `enigma`, modifiez les fichiers `/etc/hostname6.` *interface***.**

```
# cat /etc/hostname6.hme0
## enigma
6000:6666::aaaa:1116 inet6 private

#  cat /etc/hostname6.hme1
## enigma
2001::aaaa:6666:6666 inet6 router
```

b. Sur le système `partym`, modifiez les fichiers `/etc/hostname6.` *interface***.**

```
# cat /etc/hostname6.hme0
## partym
6000:3333::eeee:1113 inet6 private

# cat /etc/hostname6.hme1
## partym
2001::eeee:3333:3333 inet6 router
```

22 Exécutez un protocole de routage.

```
# routeadm -e ipv6-routing
# routeadm -u
```

Vous devrez peut-être configurer le protocole de routage avant de l'exécuter. Pour plus d'informations, reportez-vous à la section "Protocoles de routage dans Oracle Solaris" à la page 257. Pour connaître la procédure, reportez-vous à la section "Configuration d'un routeur IPv6" à la page 179.

▼ Protection d'un VPN à l'aide d'un tunnel IPsec en mode Transport sur IPv4

En mode Transport, l'en-tête extérieur détermine la stratégie IPsec qui protège le paquet IP interne.

Cette procédure prolonge la procédure “Sécurisation du trafic entre deux systèmes à l'aide d'IPsec” à la page 519. Outre la connexion de deux systèmes, vous connectez deux intranets qui leur sont connectés. Les systèmes de cette procédure fonctionnent comme des passerelles.

La configuration utilisée pour cette procédure est décrite à la section “Description de la topologie réseau requise par les tâches IPsec afin de protéger un VPN” à la page 542. Les raisons pour lesquelles des commandes spécifiques sont requises sont expliquées en détail aux étapes correspondantes de la section “Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4” à la page 544.

Remarque – Effectuez cette procédure sur les deux systèmes.

---

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

---

2 Contrôlez le flux de paquets avant de configurer IPsec.

a. Assurez-vous que le transfert IP et le routage dynamique IP sont désactivés.

```
# routeadm
Configuration       Current         Current
       Option       Configuration  System State
---------------------------------------------------
IPv4 forwarding     disabled           disabled
   IPv4 routing     default (enabled)   enabled
...
```

Si le transfert IP et le routage dynamique IP sont activés, vous pouvez les désactiver en tapant :

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

b. Activez le multiréseau de destination strict IP.

```
# ndd -set /dev/ip ip_strict_dst_multihoming 1
```

Attention – La valeur par défaut de `ip_strict_dst_multihoming` est rétablie lors de l'initialisation du système. Pour rendre persistante la valeur modifiée, reportez-vous à la section "Protection contre l'usurpation d'adresse IP" à la page 572.

c. Désactivez la plupart des services réseau, voire tous les services réseau.

Remarque – Si le système a été installé avec le profil SMF "limité", vous pouvez ignorer cette étape. Tous les services réseau sont désactivés, à l'exception de Solaris Secure Shell.

La désactivation des services réseau évite que le système soit affecté par les paquets IP. Par exemple, vous pouvez utiliser un démon SNMP, une connexion `telnet` ou une connexion `rlogin`.

Procédez de l'une des manières suivantes :

- Si vous exécutez Solaris 10 11/06 ou une version supérieure, exécutez le profil SMF "limité".

```
# netservices limited
```

- Dans le cas contraire, désactivez les services réseau un à un.

```
# svcadm disable network/ftp:default
# svcadm disable network/finger:default
# svcadm disable network/login:rlogin
# svcadm disable network/nfs/server:default
# svcadm disable network/rpc/rstat:default
# svcadm disable network/smtp:sendmail
# svcadm disable network/telnet:default
```

d. Assurez-vous que la plupart des services réseau sont désactivés.

Assurez-vous que les montages en loopback et le service `ssh` sont en cours d'exécution.

```
# svcs | grep network
online         Aug_02   svc:/network/loopback:default
...
online         Aug_09   svc:/network/ssh:default
```

3 Ajoutez une paire de SA entre les deux systèmes.

Procédez de l'une des manières suivantes :

- Configurez IKE de manière à gérer les clés pour les SA. Suivez l'une des procédures de la section "Configuration du protocole IKE (liste des tâches)" à la page 593 afin de configurer IKE pour le VPN.
- Si, pour une raison particulière, vous souhaitez gérer les clés manuellement, reportez-vous à la section "Création manuelle d'associations de sécurité IPsec" à la page 528.

4 **Ajoutez une stratégie IPsec.**

Modifiez le fichier `/etc/inet/ipsecinit.conf` afin d'ajouter la stratégie IPsec pour le VPN. Pour renforcer la stratégie, reportez-vous à l'Exemple 20–15.

a. **Sur le système `enigma`, saisissez l'entrée suivante dans le fichier `ipsecinit.conf` :**

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.16.16.6 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate transport}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

b. **Sur le système `partym`, tapez l'entrée suivante dans le fichier `ipsecinit.conf` :**

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate transport}
 ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

5 **(Facultatif) Vérifiez la syntaxe du fichier de stratégie IPsec.**

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6 **Pour configurer le tunnel et le protéger à l'aide d'IPsec, suivez les étapes en fonction de la version de Solaris utilisée :**

- **À partir de la version Solaris 10 4/09, suivez les étapes Étape 7 à Étape 13, puis exécutez le protocole de routage tel qu'indiqué à l'Étape 22.**
- **Si vous exécutez une version antérieure à la version Solaris 10 4/09, suivez les étapes Étape 14 à Étape 22.**

7 **Configurez le tunnel `ip.tun0` dans le fichier `/etc/hostname.ip.tun0`.**

a. **Sur le système `enigma`, ajoutez l'entrée suivante au fichier `hostname.ip.tun0` :**

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 tdst 192.168.13.213 router up
```

b. **Sur le système `partym`, ajoutez l'entrée suivante au fichier `hostname.ip.tun0` :**

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 tdst 192.168.116.16 router up
```

8 **Protégez le tunnel à l'aide de la stratégie IPsec créée.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9 **Pour lire le contenu du fichier `hostname.ip.tun0` dans le noyau, redémarrez les services réseau.**

```
# svcadm restart svc:/network/initial:default
```

10 Activez le transfert IP pour l'interface `hme1`.

a. Sur le système `enigma`, ajoutez l'entrée du routeur au fichier `/etc/hostname.hme1`.

```
192.168.116.16 router
```

b. Sur le système `partym`, ajoutez l'entrée du routeur au fichier `/etc/hostname.hme1`.

```
192.168.13.213 router
```

11 Assurez-vous que les protocoles de routage n'indiquent pas la route par défaut sur l'intranet.

a. Sur le système `enigma`, ajoutez l'indicateur `private` au fichier `/etc/hostname.hme0`.

```
10.16.16.6 private
```

b. Sur le système `partym`, ajoutez l'indicateur `private` au fichier `/etc/hostname.hme0`.

```
10.1.3.3 private
```

12 Ajoutez manuellement une route par défaut sur `hme0`.

a. Sur le système `enigma`, ajoutez la route suivante :

```
# route add default 192.168.116.4
```

b. Sur le système `partym`, ajoutez la route suivante :

```
# route add default 192.168.13.5
```

13 Pour terminer la procédure, passez à l'Étape 22 pour exécuter un protocole de routage.

14 Configurez le tunnel `ip.tun0`.

Remarque – Les étapes suivantes permettent de configurer un tunnel sur un système exécutant une version antérieure à la version Solaris 10 4/09.

Utilisez les commandes `ifconfig` pour créer l'interface point à point :

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 system1-point system2-point \
tsrc system1-taddr tdst system2-taddr
```

a. Sur le système `enigma`, saisissez les commandes ci-dessous :

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213
```

b. Sur le système `partym`, tapez les commandes ci-dessous :

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.1.3.3 10.16.16.6  \
tsrc 192.168.13.213 tdst 192.168.116.16
```

15 Protégez le tunnel à l'aide de la stratégie IPsec créée.

```
# ipsecconf
```

16 Affichez le routeur pour le tunnel.

```
# ifconfig ip.tun0 router up
```

17 Activez le transfert IP pour l'interface `hme1`.

```
# ifconfig hme1 router
```

18 Assurez-vous que les protocoles de routage n'indiquent pas la route par défaut sur l'intranet.

```
# ifconfig hme0 private
```

19 Ajoutez manuellement une route par défaut à travers `hme0`.

La route par défaut doit correspondre à un routeur bénéficiant d'un accès direct à Internet.

```
# route add default router-on-hme0-subnet
```

a. Sur le système `enigma`, ajoutez la route suivante :

```
# route add default 192.168.116.4
```

b. Sur le système `partym`, ajoutez la route suivante :

```
# route add default 192.168.13.5
```

20 Assurez-vous que le VPN démarre à la réinitialisation en ajoutant une entrée au fichier `/etc/hostname.ip.tun0`.

```
system1-point system2-point tsrc system1-taddr \
tdst system2-taddr encr_algs aes encr_auth_algs sha1 router up
```

a. Sur le système `enigma`, ajoutez l'entrée suivante au fichier `hostname.ip.tun0` :

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 \
tdst 192.168.13.213 router up
```

b. Sur le système `partym`, ajoutez l'entrée suivante au fichier `hostname.ip.tun0` :

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 \
tdst 192.168.116.16 router up
```

21 Configurez les fichiers d'interface afin de transmettre les paramètres adéquats au démon de routage.

a. Sur le système `enigma`, modifiez les fichiers `/etc/hostname.` *interface*.

```
# cat /etc/hostname.hme0
## enigma
10.16.16.6 private

# cat /etc/hostname.hme1
## enigma
192.168.116.16 router
```

b. Sur le système `partym`, modifiez les fichiers `/etc/hostname.` *interface*.

```
# cat /etc/hostname.hme0
## partym
10.1.3.3 private

# cat /etc/hostname.hme1
## partym
192.168.13.213 router
```

22 Exécutez un protocole de routage.

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

Exemple 20–15 Requête de stratégie IPsec sur tous les systèmes en mode Transport

Dans cet exemple, l'administrateur met en commentaire la stratégie `bypass` configurée à l'Étape 4, ce qui renforce la protection. Avec cette configuration de stratégie, chaque système du LAN doit activer IPsec afin de communiquer avec le routeur.

```
# LAN traffic must implement IPsec.
# {laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip.tun0 negotiate transport} ipsec {encr_algs aes encr_auth_algs sha1}
```

Exemple 20–16 Configuration d'un tunnel IPsec en mode Transport à l'aide d'une syntaxe désapprouvée

Dans cet exemple, l'administrateur connecte un système Solaris 10 7/07 à un système exécutant la version Solaris 10. Par conséquent, l'administrateur utilise la syntaxe Solaris 10 dans le fichier de configuration et inclut les algorithmes IPsec à la commande `ifconfig`.

L'administrateur suit la procédure décrite à la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Transport sur IPv4" à la page 559, à l'exception des modifications syntaxiques ci-dessous.

- Pour l'Étape 4, la syntaxe du fichier `ipsecinit.conf` est la suivante :

```
# LAN traffic to and from this address can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{} ipsec {encr_algs aes encr_auth_algs sha1}
```

- Pour les étapes Étape 14 à Étape 16, la syntaxe permettant de configurer un tunnel sécurisé est la suivante :

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213 \
encr_algs aes encr_auth_algs sha1

# ifconfig ip.tun0 router up

# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213 \
encr_algs aes encr_auth_algs sha1
```

  La stratégie IPsec utilisée dans les commandes `ifconfig` doit correspondre à celle qui est spécifiée dans le fichier `ipsecinit.conf`. À la réinitialisation, chaque système lit le fichier `ipsecinit.conf` pour connaître sa stratégie.

- Pour l'Étape 20, la syntaxe du fichier `hostname.ip.tun0` est la suivante :

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 \
tdst 192.168.13.213 encr_algs aes encr_auth_algs sha1 router up
```

▼ Protection d'un VPN à l'aide d'un tunnel IPsec en mode Transport sur IPv6

Les étapes de configuration d'un VPN sur un réseau IPv6 sont identiques à celles de la configuration d'un VPN sur un réseau IPv4. Toutefois, la syntaxe des commandes est légèrement différente. Les raisons pour lesquelles des commandes spécifiques sont requises sont expliquées en détail aux étapes correspondantes de la section “Protection d'un VPN à l'aide d'un tunnel IPsec en mode Tunnel sur IPv4” à la page 544.

Remarque – Effectuez cette procédure sur les deux systèmes.

Cette procédure utilise les paramètres de configuration ci-dessous.

Paramètre	Europe	Californie
Nom du système	`enigma`	`partym`
Interface intranet du système	`hme1`	`hme1`

Paramètre	Europe	Californie
Interface Internet du système	`hme0`	`hme0`
Adresse intranet du système	`6000:6666::aaaa:1116`	`6000:3333::eeee:1113`
Adresse Internet du système	`2001::aaaa:6666:6666`	`2001::eeee:3333:3333`
Nom du routeur Internet	`router-E`	`router-C`
Adresse du routeur Internet	`2001::aaaa:0:4`	`2001::eeee:0:1`
Nom du tunnel	`ip6.tun0`	`ip6.tun0`

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

2 Contrôlez le flux de paquets avant de configurer IPsec.

a. Assurez-vous que le transfert IP et le routage dynamique IP sont désactivés.

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

Si le transfert IP et le routage dynamique IP sont activés, vous pouvez les désactiver en tapant :

```
# routeadm -d ipv6-forwarding -d ipv6-routing
# routeadm -u
```

b. Activez le multiréseau de destination strict IP.

```
# ndd -set /dev/ip ip6_strict_dst_multihoming 1
```

Attention – La valeur par défaut de `ip6_strict_dst_multihoming` est rétablie lors de l'initialisation du système. Pour rendre persistante la valeur modifiée, reportez-vous à la section "Protection contre l'usurpation d'adresse IP" à la page 572.

c. Assurez-vous que la plupart des services réseau sont désactivés.

Assurez-vous que les montages en loopback et le service `ssh` sont en cours d'exécution.

```
# svcs | grep network
online         Aug_02   svc:/network/loopback:default
...
online         Aug_09   svc:/network/ssh:default
```

3 Ajoutez une paire de SA entre les deux systèmes.

Procédez de l'une des manières suivantes :

- Configurez IKE de manière à gérer les clés pour les SA. Suivez l'une des procédures de la section "Configuration du protocole IKE (liste des tâches)" à la page 593 afin de configurer IKE pour le VPN.
- Si, pour une raison particulière, vous souhaitez gérer les clés manuellement, reportez-vous à la section "Création manuelle d'associations de sécurité IPsec" à la page 528.

4 Ajoutez une stratégie IPsec.

Modifiez le fichier `/etc/inet/ipsecinit.conf` afin d'ajouter la stratégie IPsec pour le VPN.

a. Sur le système `enigma`, saisissez l'entrée suivante dans le fichier `ipsecinit.conf` :

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:6666::aaaa:1116 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate transport}
 ipsec {encr_algs aes encr_auth_algs sha1}
```

b. Sur le système `partym`, tapez l'entrée suivante dans le fichier `ipsecinit.conf` :

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{tunnel ip6.tun0 negotiate transport}
 ipsec {encr_algs aes encr_auth_algs sha1}
```

5 (Facultatif) Vérifiez la syntaxe du fichier de stratégie IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

6. **Pour configurer le tunnel et le protéger à l'aide d'IPsec, suivez les étapes en fonction de la version de Solaris utilisée :**

   - **À partir de la version Solaris 10 4/09, suivez les étapes Étape 7 à Étape 13, puis exécutez le protocole de routage tel qu'indiqué à l'Étape 22.**
   - **Si vous exécutez une version antérieure à la version Solaris 10 4/09, suivez les étapes Étape 14 à Étape 22.**

7. **Configurez le tunnel `ip6.tun0` dans le fichier `/etc/hostname.ip6.tun0`.**

   a. **Sur le système `enigma`, ajoutez l'entrée suivante au fichier `hostname.ip6.tun0` :**

```
6000:6666::aaaa:1116 6000:3333::eeee:1113 tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 router up
```

   b. **Sur le système `partym`, ajoutez l'entrée suivante au fichier `hostname.ip6.tun0` :**

```
6000:3333::eeee:1113  6000:6666::aaaa:1116 tsrc 2001::eeee:3333:3333 tdst 2001::aaaa:6666:6666 router up
```

8. **Protégez le tunnel à l'aide de la stratégie IPsec créée.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

9. **Pour lire le contenu du fichier `hostname.ip6.tun0` dans le noyau, redémarrez les services réseau.**

```
# svcadm restart svc:/network/initial:default
```

10. **Activez le transfert IP pour l'interface `hme1`.**

    a. **Sur le système `enigma`, ajoutez l'entrée de routeur au fichier `/etc/hostname6.hme1`.**

```
2001::aaaa:6666:6666 inet6 router
```

    b. **Sur le système `partym`, ajoutez l'entrée de routeur au fichier `/etc/hostname6.hme1`.**

```
2001::eeee:3333:3333 inet6 router
```

11. **Assurez-vous que les protocoles de routage n'indiquent pas la route par défaut sur l'intranet.**

    a. **Sur le système `enigma`, ajoutez l'indicateur `private` au fichier `/etc/hostname6.hme0`.**

```
6000:6666::aaaa:1116 inet6 private
```

    b. **Sur le système `partym`, ajoutez l'indicateur `private` au fichier `/etc/hostname6.hme0`.**

```
6000:3333::eeee:1113 inet6 private
```

12. **Ajoutez manuellement une route par défaut à travers `hme0`.**

    a. **Sur le système `enigma`, ajoutez la route suivante :**

```
# route add -inet6 default 2001::aaaa:0:4
```

b. Sur le système `partym`, ajoutez la route suivante :

```
# route add -inet6 default 2001::eeee:0:1
```

13 Pour terminer la procédure, passez à l'Étape 22 pour exécuter un protocole de routage.

14 Configurez un tunnel sécurisé `ip6.tun0`.

Remarque – Les étapes suivantes permettent de configurer un tunnel sur un système exécutant une version antérieure à la version Solaris 10 4/09.

---

a. Sur le système `enigma`, saisissez les commandes ci-dessous :

```
# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666   tdst 2001::eeee:3333:3333
```

b. Sur le système `partym`, tapez les commandes ci-dessous :

```
# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6  6000:3333::eeee:1113  6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333   tdst 2001::aaaa:6666:6666
```

15 Protégez le tunnel à l'aide de la stratégie IPsec créée.

```
# ipsecconf
```

16 Affichez le routeur pour le tunnel.

```
# ifconfig ip6.tun0 router up
```

17 Activez le transfert IP pour l'interface `hme1`.

```
# ifconfig hme1 router
```

18 Assurez-vous que les protocoles de routage n'indiquent pas la route par défaut sur l'intranet.

```
# ifconfig hme0 private
```

19 Sur chaque système, ajoutez manuellement une route par défaut à travers `hme0`.

La route par défaut doit correspondre à un routeur bénéficiant d'un accès direct à Internet.

a. Sur le système `enigma`, ajoutez la route suivante :

```
# route add -inet6 default 2001::aaaa:0:4
```

b. Sur le système `partym`, ajoutez la route suivante :

```
# route add -inet6 default 2001::eeee:0:1
```

20 Sur chaque système, assurez-vous que le VPN démarre à la réinitialisation en ajoutant une entrée au fichier `/etc/hostname6.ip6.tun0`.

L'entrée réplique les paramètres spécifiés dans la commande `ifconfig` lors de l'Étape 14.

a. Sur le système `enigma`, ajoutez l'entrée suivante au fichier `hostname6.ip6.tun0` :

```
6000:6666::aaaa:1116  6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666   tdst 2001::eeee:3333:3333  router up
```

b. Sur le système `partym`, ajoutez l'entrée suivante au fichier `hostname6.ip6.tun0` :

```
6000:3333::eeee:1113  6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333   tdst 2001::aaaa:6666:6666  router up
```

21 Configurez les fichiers d'interface afin de transmettre les paramètres adéquats au démon de routage.

a. Sur le système `enigma`, modifiez les fichiers `/etc/hostname6.` *interface***.**

```
# cat /etc/hostname6.hme0
## enigma
6000:6666::aaaa:1116 inet6 private

#  cat /etc/hostname6.hme1
## enigma
2001::aaaa:6666:6666 inet6 router
```

b. Sur le système `partym`, modifiez les fichiers `/etc/hostname6.` *interface***.**

```
# cat /etc/hostname6.hme0
## partym
6000:3333::eeee:1113 inet6 private

# cat /etc/hostname6.hme1
##
partym2001::eeee:3333:3333 inet6 router
```

22 Exécutez un protocole de routage.

```
# routeadm -e ipv6-routing
# routeadm -u
```

Exemple 20–17 Configuration d'IPsec en mode Transport sur IPv6 à l'aide d'une syntaxe désapprouvée

Dans cet exemple, l'administrateur connecte un système Solaris 10 7/07 à un système exécutant la version Solaris 10. Par conséquent, l'administrateur utilise la syntaxe Solaris 10 dans le fichier de configuration et inclut les algorithmes IPsec à la commande `ifconfig`.

La procédure suivie par l'administrateur est identique à celle de la section "Protection d'un VPN à l'aide d'un tunnel IPsec en mode Transport sur IPv6" à la page 566, à l'exception des modifications syntaxiques ci-dessous.

- Pour l'Étape 4, la syntaxe du fichier `ipsecinit.conf` est la suivante :

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-1.
{} ipsec {encr_algs aes encr_auth_algs sha1}
```

- Pour les étapes Étape 14 à Étape 17, la syntaxe permettant de configurer un tunnel sécurisé est la suivante :

```
# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666 tdst 2001::eeee:3333:3333 \
encr_algs aes encr_auth_algs sha1

# ifconfig ip6.tun0 inet6 router up
```

  La stratégie IPsec utilisée dans les commandes `ifconfig` doit correspondre à celle qui est spécifiée dans le fichier `ipsecinit.conf`. À la réinitialisation, chaque système lit le fichier `ipsecinit.conf` pour connaître sa stratégie.

- Pour l'Étape 20, la syntaxe du fichier `hostname6.ip6.tun0` est la suivante :

```
6000:6666::aaaa:1116  6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666   tdst 2001::eeee:3333:3333 \
encr_algs aes encr_auth_algs sha1 router up
```

▼ Protection contre l'usurpation d'adresse IP

Afin d'empêcher le système de transmettre des paquets vers une autre interface sans tenter de les déchiffrer, le système doit contrôler les éventuelles usurpations d'adresse IP. Une méthode de prévention consiste à définir un paramètre multiréseau strict de destination IP, par le biais de la commande `ndd`. Lorsque ce paramètre est défini dans un manifeste SMF, le paramètre est défini lors du redémarrage du système.

Remarque – Effectuez cette procédure sur les deux systèmes.

---

1 **Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Créez un manifeste SMF spécifique à un site afin de vérifier la présence d'éventuelles usurpations d'adresse IP.**

Utilisez l'exemple de script suivant, `/var/svc/manifest/site/spoof_check.xml`.

```
<?xml version="1.0"?>
<!DOCTYPE service_bundle SYSTEM "/usr/share/lib/xml/dtd/service_bundle.dtd.1">

<service_bundle type='manifest' name='Custom:ip_spoof_checking'>

<!--    This is a custom smf(5) manifest for this system. Place this
        file in /var/svc/manifest/site, the directory for local
        system customizations. The exec method uses an unstable
        interface to provide a degree of protection against IP
        spoofing attacks when this system is acting as a router.

        IP spoof protection can also be achieved by using ipfilter(5).
        If ipfilter is configured, this service can be disabled.

        Note: Unstable interfaces might be removed in later
        releases.  See attributes(5).
-->

<service
        name='site/ip_spoofcheck'
        type='service'
        version='1'>

        <create_default_instance enabled='false' />
        <single_instance />

        <!--    Don't enable spoof protection until the
                network is up.
        -->
        <dependency
                name='basic_network'
                grouping='require_all'
                restart_on='none'
                type='service'>
        <service_fmri value='svc:/milestone/network' />
        </dependency>

        <exec_method
                type='method'
                name='start'
                exec='/usr/sbin/ndd -set /dev/ip ip_strict_dst_multihoming 1'
<!--
     For an IPv6 network, use the IPv6 version of this command, as in:
                exec='/usr/sbin/ndd -set /dev/ip ip6_strict_dst_multihoming 1
```

```
-->
                timeout_seconds='60'
        />

        <exec_method
                type='method'
                name='stop'
                exec=':true'
                timeout_seconds='3'
        />

        <property_group name='startd' type='framework'>
                <propval
                        name='duration'
                        type='astring'
                        value='transient'
                />
        </property_group>

        <stability value='Unstable' />

</service>
</service_bundle>
```

3 Importez ce manifeste dans le référentiel SMF.

```
# svccfg import /var/svc/manifest/site/spoof_check.xml
```

4 Activez le service `ip_spoofcheck`.

Utilisez le nom qui est défini dans le fichier manifeste, `/site/ip_spoofcheck`.

```
# svcadm enable /site/ip_spoofcheck
```

5 Assurez-vous que le service `ip_spoofcheck` est en ligne.

```
# svcs /site/ip_spoofcheck
```

◆ ◆ ◆ CHAPITRE 21

Architecture IPsec (référence)

Ce chapitre contient les informations de référence suivante :

Pour obtenir les instructions relatives à l'implémentation d'IPsec sur votre réseau, reportez-vous au Chapitre 20, “Configuration d'IPsec (tâches)”. Pour une présentation d'IPsec, reportez-vous au Chapitre 19, “Architecture IPsec (présentation)”.

Utilitaire de gestion du service IPsec

L'utilitaire de gestion des services (SMF) fournit les services suivants pour IPsec :

- Le **service** `svc:/network/ipsec/policy` permet de gérer la stratégie IPsec. Par défaut, ce service est activé. La valeur de la propriété `config_file` détermine l'emplacement du fichier `ipsecinit.conf`. La valeur initiale est `/etc/inet/ipsecinit.conf`.
- Le **service** `svc:/network/ipsec/ipsecalgs` permet de gérer les algorithmes disponibles pour IPsec. Par défaut, ce service est activé.
- Le **service** `svc:/network/ipsec/manual-key` permet d'activer la gestion manuelle des clés. Par défaut, ce service est désactivé. La valeur de la propriété `config_file` détermine l'emplacement du fichier de configuration `ipseckeys`. La valeur initiale est `/etc/inet/secret/ipseckeys`.
- Le **service** `svc:/network/ipsec/ike` permet de gérer IKE. Par défaut, ce service est désactivé. Pour les propriétés configurables, reportez-vous à la section “Utilitaire de gestion du service IKE” à la page 639.

Pour plus d'informations sur l'utilitaire SMF, reportez-vous au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base*. Voir aussi les pages de manuel `smf(5)`, `svcadm(1M)` et `svccfg(1M)`.

Commande `ipsecconf`

Pour configurer la stratégie IPsec d'un hôte, vous devez exécuter la commande `ipsecconf`. À l'exécution de la commande de configuration de la stratégie, le système crée des entrées de stratégie IPsec dans le noyau. Elles lui permettent de vérifier la stratégie appliquée à tous les datagrammes IP entrants et sortants. Les datagrammes transférés ne sont pas soumis aux vérifications de stratégie ajoutées à l'aide de cette commande. La commande `ipsecconf` configure également la base de données de stratégie de sécurité (SPD, Security Policy Database).

- Pour plus d'informations sur la protection des paquets transférés, reportez-vous aux pages de manuel `ifconfig(1M)` et `tun(7M)`.
- Pour consulter les options de stratégie IPsec, reportez-vous à la page de manuel `ipsecconf(1M)`.
- Pour obtenir les instructions relatives à la protection du trafic entre systèmes à l'aide de la commande `ipsecconf`, reportez-vous à la section "Configuration du protocole IKE (liste des tâches)" à la page 593.

Pour exécuter la commande `ipsecconf`, vous devez prendre le rôle de superutilisateur ou un rôle équivalent. La commande accepte les entrées qui protègent le trafic bidirectionnel. Elle accepte également celles qui protègent le trafic unidirectionnel.

Les entrées de stratégie au format d'adresse locale et d'adresse distante peuvent protéger le trafic dans les deux directions à l'aide d'une entrée de stratégie unique. Par exemple, les entrées de modèles `laddr host1` et `raddr host2` protègent le trafic dans les deux directions quand aucune direction n'est spécifiée pour l'hôte nommé. Par conséquent, une seule entrée de stratégie est nécessaire pour chaque hôte.

Les entrées de stratégie au format adresse source vers adresse de destination protège le trafic dans une seule direction. Par exemple, une entrée de stratégie suivant le modèle `saddr host1 daddr host2` protège le trafic entrant ou le trafic sortant, non le trafic bidirectionnel. Par conséquent, pour protéger le trafic dans les deux directions, vous devez appliquer la commande `ipsecconf` à une autre entrée, `saddr host2 daddr host1`, par exemple.

Pour garantir l'activation de la stratégie IPsec au démarrage de la machine, vous pouvez créer le fichier de stratégie IPsec `/etc/inet/ipsecinit.conf`. Ce fichier est lu au démarrage des services réseau. Pour obtenir les instructions relatives à la création du fichier de stratégie IPsec, reportez-vous à la section "Protection du trafic à l'aide d'IPsec (liste des tâches)" à la page 517.

À partir de la version Solaris 10 4/09, avec l'option `-c`, la commande `ipsecconf` vérifie la syntaxe du fichier de stratégie IPsec que vous fournissez en argument.

Les entrées de stratégie ajoutées par le biais de la commande ipsecconf ne sont pas conservées après la réinitialisation du système. Pour vous assurer que la stratégie IPsec est active lorsque le système démarre, ajoutez l'entrée de stratégie au fichier /etc/inet/ipsecinit.conf. Dans la version actuelle, actualisez ou activez le service policy. Dans une version antérieure à la version Solaris 10 4/09, réinitialisez ou utilisez la commande ipsecconf. Pour des exemples, reportez-vous à la section "Protection du trafic à l'aide d'IPsec (liste des tâches)" à la page 517.

Fichier ipsecinit.conf

Pour appeler les stratégies de sécurité IPsec au démarrage du Système d'exploitation Solaris (SE Solaris), vous devez créer un fichier de configuration pour initialiser IPsec avec vos entrées de stratégie IPsec spécifiques. Le nom par défaut de ce fichier est /etc/inet/ipsecinit.conf. Reportez-vous à la page de manuel ipsecconf(1M) pour plus d'informations sur les entrées d'une stratégie et leur format. Une fois les stratégies configurées, vous pouvez exécuter la commande ipsecconf pour consulter ou modifier la configuration existante. À partir de la version Solaris 10 4/09, vous actualisez le service policy pour modifier la configuration existante.

Fichier exemple ipsecinit.conf

Le logiciel Solaris inclut le fichier exemple de stratégie IPsec, ipsecinit.sample. Vous pouvez l'utiliser comme modèle pour créer votre propre fichier ipsecinit.conf. Le fichier ipsecinit.sample contient les exemples suivants :

```
#
# For example,
#
#     {rport 23} ipsec {encr_algs des encr_auth_algs md5}
#
# will protect the telnet traffic originating from the host with ESP using
# DES and MD5. Also:
#
#     {raddr 10.5.5.0/24} ipsec {auth_algs any}
#
# will protect traffic to or from the 10.5.5.0 subnet with AH
# using any available algorithm.
#
#
# To do basic filtering, a drop rule may be used. For example:
#
#     {lport 23 dir in} drop {}
#     {lport 23 dir out} drop {}
# will disallow any remote system from telnetting in.
#
# If you are using IPv6, it may be useful to bypass neighbor discovery
# to allow in.iked to work properly with on-link neighbors. To do that,
# add the following lines:
#
```

```
#       {ulp ipv6-icmp type 133-137 dir both } pass { }
#
# This will allow neighbor discovery to work normally.
```

Considérations de sécurité à propos de ipsecinit.conf et ipsecconf

Prenez la plus grande précaution lorsque vous transmettez une copie du fichier `ipsecinit.conf` sur un réseau. Un utilisateur malintentionné est en mesure de lire un fichier monté sur le réseau lorsque ce fichier est en cours de lecture. Par exemple, si le fichier `/etc/inet/ipsecinit.conf` est ouvert ou copié à partir d'un système de fichiers monté via NFS, un utilisateur malintentionné peut modifier la stratégie qu'il contient.

Veillez à configurer les stratégies IPsec avant de démarrer toute communication. En effet, les nouvelles entrées de stratégie peuvent affecter les connexions existantes. De même, ne modifiez pas les stratégies au milieu d'une communication.

En particulier, vous ne pouvez pas modifier la stratégie IPsec des sockets SCTP, TCP ou UDP sur lesquels un appel de fonction `connect()` ou `accept()` a été émis. Un socket dont la stratégie ne peut pas être modifiée est appelé un *socket verrouillé*. Les nouvelles entrées de stratégie ne protègent pas les sockets qui sont déjà verrouillés. Pour plus d'informations, reportez-vous aux pages de manuel `connect`(3SOCKET) et `accept`(3SOCKET).

Protégez votre système d'attribution de nom. Lorsque les deux conditions suivantes sont vérifiées, vos noms d'hôtes ne sont plus fiables.

- Votre adresse source est un hôte que vous pouvez rechercher sur le réseau.
- Votre système d'attribution de nom est compromis.

Les défaillances de sécurité proviennent souvent d'une mauvaise utilisation des outils, non des outils eux-mêmes. Utilisez la commande `ipsecconf` avec prudence. Une console ou autre TTY connecté offrent les modes d'opération les plus sûrs.

Commande ipsecalgs

La structure cryptographique de Solaris fournit des algorithmes d'authentification et de chiffrement pour IPsec. La commande `ipsecalgs` permet d'établir la liste des algorithmes pris en charge par chacun des protocoles IPsec. La configuration `ipsecalgs` est stockée dans le fichier `/etc/inet/ipsecalgs`. En général, ce fichier n'a pas besoin d'être modifié. Cependant, si le fichier doit être modifié, utilisez la commande `ipsecalgs`. Le fichier ne doit jamais être édité directement. Dans la version actuelle, les algorithmes pris en charge sont synchronisés avec le noyau à l'initialisation du système par le service `svc:/network/ipsec/ipsecalgs:default`.

Les protocoles et algorithmes IPsec valides sont décrits par le DOI, ISAKMP, traité dans le document RFC 2407. Au sens global, un DOI (Domain of Interpretation, domaine

d'interprétation) définit les formats de données, les types d'échange du trafic réseau ainsi que les conventions d'appellation des informations liées à la sécurité. Les stratégies de sécurité, les algorithmes et les modes cryptographiques sont toutes des informations ayant trait à la sécurité.

En particulier, le DOI ISAKMP définit les conventions d'attribution de nom et de numéro des algorithmes IPsec valides et de leurs protocoles, `PROTO_IPSEC_AH` et `PROTO_IPSEC_ESP`. Chaque algorithme est associé à exactement un protocole. Ces définitions DOI ISAKMP figurent dans le fichier `/etc/inet/ipsecalgs`. Les numéros d'algorithme et de protocole sont définis par l'IANA (Internet Assigned Numbers Authority). La commande `ipsecalgs` permet d'allonger la liste des algorithmes IPsec.

Pour plus d'informations sur les algorithmes, reportez-vous à la page de manuel `ipsecalgs(1M)` Pour plus d'informations sur la structure cryptographique Solaris, reportez-vous au Chapitre 13, “Oracle Solaris Cryptographic Framework (Overview)” du *System Administration Guide: Security Services*.

Base de données des associations de sécurité IPsec

Les informations sur les numéros de clés des services de sécurité IPsec sont conservées dans la base de données des associations de sécurité (SADB). Les associations de sécurité (SA) protègent les paquets entrants et sortants. Les SADB sont gérées par un processus utilisateur, éventuellement par plusieurs processus de coopération, qui envoient des messages sur un socket de type spécial. Ce mode de gestion des SADB s'apparente à la méthode décrite à la page de manuel `route(7P)` Seuls les superutilisateurs ou les utilisateurs ayant un rôle équivalent ont accès à la base de données.

Le démon `in.iked` et la commande `ipseckey` utilisent l'interface socket `PF_KEY` dans le cadre de la gestion des SADB. Pour plus d'informations sur la gestion des requêtes et des messages par les SADB, reportez-vous à la page de manuel `pf_key(7P)`.

Utilitaires de génération de clés IPsec

Le protocole IKE permet la gestion automatique des clés pour les adresses IPv4 et IPv6. Pour obtenir les instructions relatives à la configuration IKE, reportez-vous au Chapitre 23, “Configuration du protocole IKE (tâches)”. L'utilitaire de génération manuelle de clés est la commande `ipseckey`, décrite à la page de manuel `ipseckey(1M)`.

Utilisez la commande `ipseckey` pour remplir manuellement la base de données des associations de sécurité (SADB). En règle générale, les SA sont générées manuellement lorsqu'IKE n'est pas disponible pour une raison quelconque. Cependant, si les valeurs SPI sont uniques, la génération manuelle des SA et IKE peuvent être utilisés en même temps.

La commande `ipseckey` permet d'afficher toutes les SA connues du système, que les clés aient été ajoutées manuellement ou par le biais d'IKE. À partir de la version Solaris 10 4/09, avec l'option `-c`, la commande `ipseckey` permet de vérifier la syntaxe du fichier de clés que vous spécifiez en tant qu'argument.

Les SA IPsec qui sont ajoutées par le biais de la commande `ipseckey` ne sont pas conservées après la réinitialisation du système. Dans la version actuelle, pour activer manuellement les SA ajoutés à l'initialisation du système, ajoutez des entrées au fichier `/etc/inet/secret/ipseckeys`, puis activez le service `svc:/network/ipsec/manual-key:default`. Pour connaître la procédure, reportez-vous à la section "Création manuelle d'associations de sécurité IPsec" à la page 528.

Bien qu'elle présente un nombre limité d'options générales, la commande `ipseckey` prend en charge un langage de commande enrichi. Si vous le souhaitez, une interface de programmation de génération manuelle de clés peut transmettre les requêtes. Pour de plus amples informations, reportez-vous à la page de manuel `pf_key(7P)`.

Considérations de sécurité pour la commande `ipseckey`

La commande `ipseckey` permet au superutilisateur ou à un rôle auquel a été attribué le profil de droits Network Security ou Network IPsec Management de saisir des informations de clés cryptographiques confidentielles. Un utilisateur malintentionné accédant à ces informations peut compromettre la sécurité du trafic IPsec.

Prenez en considération les points suivants lorsque vous gérez des informations de génération de clés à l'aide de la commande `ipseckey` :

- Avez-vous actualisé les informations relatives à la génération de clés ? L'actualisation périodique des clés est une pratique de sécurité essentielle. Elle permet de prémunir les éventuelles défaillances de l'algorithme et des clés, et de limiter les dommages subis par une clé exposée.
- Le TTY est-il connecté à un réseau ? La commande `ipseckey` est-elle en mode interactif ?
  - En mode interactif, la sécurité des informations de génération de clés constitue celle du chemin d'accès au réseau pour le trafic du TTY. Évitez d'exécuter la commande `ipseckey` lors d'une session rlogin ou telnet en clair.
  - Même les fenêtres locales sont vulnérables aux attaques d'un programme caché qui intercepte les événements de fenêtre.
- Avez-vous utilisé l'option `-f` ? Le fichier est-il en cours d'accès sur le réseau ? Le fichier est-il accessible en lecture par tout utilisateur ?
  - Un utilisateur malintentionné est en mesure de lire un fichier monté sur le réseau lorsque ce fichier est en cours de lecture. Le fichier contenant les informations de génération de clés ne doit pas être lisible par tous.

- Protégez votre système d'attribution de nom. Lorsque les deux conditions suivantes sont vérifiées, vos noms d'hôtes ne sont plus fiables.
  - Votre adresse source est un hôte que vous pouvez rechercher sur le réseau.
  - Votre système d'attribution de nom est compromis.

Les défaillances de sécurité proviennent souvent d'une mauvaise utilisation des outils, non des outils eux-mêmes. Utilisez la commande `ipseckey` avec prudence. Une console ou autre TTY connecté offrent les modes d'opération les plus sûrs.

Extensions IPsec d'autres utilitaires

La commande `ifconfig` offre des options de gestion de la stratégie IPsec sur une interface tunnel. La commande `snoop` peut analyser les en-têtes AH et ESP.

IPsec et commande `ifconfig`

Dans les versions Solaris 10, Solaris 10 7/05, Solaris 10 1/06, et Solaris 10 11/06 : pour prendre en charge IPsec, la commande `ifconfig` offre les options de sécurité suivantes ; dans la version Solaris 10 7/07, ces options de sécurité sont gérées par la commande `ipsecconf`.

- `auth_algs`
- `encr_auth_algs`
- `encr_algs`

Vous devez indiquer toutes les options de sécurité IPsec d'un tunnel dans un appel unique. Par exemple, si la protection du trafic se limite à l'utilisation d'ESP, vous devez configurer le tunnel `ip.tun0` une seule fois avec les deux options de sécurité, comme illustré ci-dessous :

```
# ifconfig ip.tun0 encr_algs aes encr_auth_algs md5
```

De la même manière, une entrée `ipsecinit.conf` configure le tunnel une fois avec les deux options de sécurité, comme illustré ci-dessous :

```
# WAN traffic uses ESP with AES and MD5.
   {} ipsec {encr_algs aes encr_auth_algs md5}
```

Option de sécurité `auth_algs`

Cette option active AH IPsec pour un tunnel dont vous spécifiez l'algorithme d'authentification. L'option `auth_algs` présente le format suivant :

`auth_algs` *authentication-algorithm*

En ce qui concerne l'algorithme, vous pouvez indiquer un numéro ou un nom, y compris le paramètre *any* pour n'exprimer aucune préférence d'algorithme spécifique. Pour désactiver la sécurité du tunnel, spécifiez l'option suivante :

```
auth_algs none
```

Pour obtenir la liste des algorithmes d'authentification disponibles, exécutez la commande `ipsecalgs`.

Remarque – L'option `auth_algs` n'est pas compatible avec NAT-Traversal. Pour plus d'informations, reportez-vous à la section "Passage de la translation d'adresses et IPsec" à la page 511.

Option de sécurité `encr_auth_algs`

Cette option active ESP IPsec pour un tunnel dont vous spécifiez l'algorithme d'authentification. L'option `encr_auth_algs` présente le format suivant :

`encr_auth_algs` *authentication-algorithm*

En ce qui concerne l'algorithme, vous pouvez indiquer un numéro ou un nom, y compris le paramètre *any* pour n'exprimer aucune préférence d'algorithme spécifique. Si vous indiquez un algorithme de chiffrement ESP sans algorithme d'authentification, la valeur de l'algorithme d'authentification ESP est définie par défaut sur le paramètre *any*.

Pour obtenir la liste des algorithmes d'authentification disponibles, exécutez la commande `ipsecalgs`.

Option de sécurité `encr_algs`

Cette option active ESP IPsec pour un tunnel dont vous spécifiez l'algorithme de chiffrement. L'option `encr_algs` présente le format suivant :

`encr_algs` *encryption-algorithm*

En ce qui concerne l'algorithme, vous pouvez indiquer un nom ou un numéro. Pour désactiver la sécurité du tunnel, spécifiez l'option suivante :

```
encr_algs none
```

Si vous spécifiez un algorithme d'authentification ESP sans algorithme de chiffrement, la valeur de chiffrement d'ESP est définie par défaut sur le paramètre *null*.

Pour obtenir la liste des algorithmes de chiffrement disponibles, exécutez la commande `ipsecalgs`.

IPsec et commande snoop

La commande snoop permet l'analyse des en-têtes ESP et AH. En raison du chiffrement des données ESP, la commande snoop ne détecte pas les en-têtes chiffrés et protégés par ESP. AH ne chiffre pas les données. Par conséquent, la commande snoop peut contrôler le trafic protégé par AH. L'option -V de la commande signale l'utilisation d'AH sur un paquet. Pour plus d'informations, reportez-vous à la page de manuel snoop(1M).

La section "Vérification de la protection des paquets par IPsec" à la page 533 contient un exemple détaillé de sortie snoop sur un paquet protégé.

◆ ◆ ◆ CHAPITRE 22

Protocole IKE (présentation)

Le protocole IKE (Internet Key Exchange, échange de clé Internet) automatise la gestion des clés pour IPsec. Ce chapitre aborde les sujets suivants :

Pour plus d'informations sur l'implémentation du protocole IKE, reportez-vous au Chapitre 23, “Configuration du protocole IKE (tâches)”. Pour obtenir des informations de référence, reportez-vous au Chapitre 24, “Protocole IKE (référence)”. Pour plus d'informations sur les protocoles IPsec, reportez-vous au Chapitre 19, “Architecture IPsec (présentation)”.

Nouveautés du protocole IKE

Solaris 10 4/09 : À partir de cette version, l'utilitaire de gestion des services (SMF) gère IKE en tant que service. Par défaut, le service `svc:/network/ipsec/ike:default` est désactivé. Par ailleurs, dans cette version, le profil de droits Network IPsec Management permet d'administrer IPsec et IKE.

Solaris 10 7/07 : à partir de cette version, le protocole IKE peut utiliser l'algorithme AES et être configuré dans la zone globale en vue de son utilisation dans des zones non globales.

- L'option de socket `SO_ALLZONES` permet au protocole IKE de gérer le trafic dans les zones non globales.

- Vous trouverez une liste complète des nouvelles fonctionnalités de Solaris et la description des différentes versions de Solaris dans le guide *Nouveautés apportées à Oracle Solaris 10 8/11*.

Gestion des clés avec IKE

La gestion des numéros de clé des associations de sécurité (Security Associations, SA) pour IPsec est appelée *gestion des clés*. La gestion automatique des clés requiert un canal de communication sécurisé pour la création, l'authentification et l'échange des clés. Le Système d'exploitation Solaris utilise IKE pour automatiser la gestion des clés. IKE s'intègre facilement dans les environnement à grande échelle et peut fournir un canal sécurisé pour un grand volume de trafic. Les associations de sécurité IPsec sur paquets IPv4 et IPv6 peuvent utiliser le protocole IKE.

Lorsque IKE est utilisé sur un système équipé d'une carte Sun Crypto Accelerator 1000, 6000 ou Sun Crypto Accelerator 4000, les opérations de clés publiques peuvent être déchargées sur l'accélérateur. Les opérations de clés publiques n'utilisent pas les ressources du système d'exploitation. Lorsque IKE est utilisé sur un système équipé d'une carte Sun Crypto Accelerator 4000 ou Sun Crypto Accelerator 6000, les certificats et les clés publiques et privées peuvent être stockés sur la carte. Le stockage des clés hors du système fournit une couche de protection supplémentaire.

Négociation des clés IKE

Le démon IKE `in.iked` négocie et authentifie les numéros de clé des associations de sécurité (SA, security associations) de façon sécurisée. Il utilise des germes de sécurité aléatoires pour les clés des fonctions internes fournies par le Système d'exploitation Solaris. Le protocole IKE assure une confidentialité de transmission parfaite (PFS, perfect forward secrecy). En mode PFS, les clés qui protègent la transmission des données ne sont pas utilisées pour générer des clés complémentaires. Les germes de sécurité employés pour créer des clés de transmission de données ne sont pas réutilisés. Reportez-vous à la page de manuel `in.iked(1M)`.

Lorsque le démon IKE découvre la clé de chiffrement d'un système public distant, le système local peut utiliser cette clé. Il l'emploie pour chiffrer les messages, qui ne peuvent alors être lus que par ce système distant. L'intervention du démon IKE se décompose en deux phases, dites d'*échange*.

Terminologie relative aux clés IKE

Le tableau ci-dessous répertorie les termes utilisés dans la négociation des clés et les acronymes les plus couramment employés. Vous y trouverez également une définition de chacun de ces termes ainsi que leur contexte d'utilisation.

TABLEAU 22–1 Terminologie de négociation des clés, acronymes et utilisation

Terminologie de négociation des clés	Acronymes	Définition et utilisation
Échange de clés		Processus de génération de clés pour les algorithmes cryptographiques asymétriques. Les principales méthodes utilisées sont les protocoles RSA et Diffie-Hellman.
Protocole Diffie-Hellman	DH	Protocole d'échange de clés impliquant la génération et l'authentification de clés et souvent appelé *échange de clés authentifiées*.
Protocole RSA	RSA	Protocole d'échange de clés impliquant la génération et le transport de clés. Ce protocole porte le nom de ses trois créateurs : Rivest, Shamir et Adleman.
Confidentialité de transmission parfaite	PFS (perfect forward secrecy)	Ne s'applique qu'à l'échange de clés authentifiées. Le mode PFS garantit que l'éventuelle découverte de secrets à long terme ne compromet pas les clés des communications précédentes. Perfect Forward Secrecy, secret rigoureux des transmission .Avec la fonction PFS, la clé visant à protéger la transmission des données n'est pas utilisée pour dériver d'autres clés. Il en est de même pour la source de la clé.
Méthode Oakley		Méthode de création sécurisée de clés pour la phase 2. Ce protocole est similaire à l'échange de clés Diffie-Hellman et implique la génération et l'authentification de clés. La méthode Oakley s'emploie pour négocier des PFS.

Phase 1 d'IKE

La phase 1 est connue sous le nom de *Main Mode* (mode principal). Pendant la phase 1, IKE utilise des méthodes de chiffrement de clé publique pour s'authentifier auprès d'entités IKE homologues. Il en résulte une association de sécurité (SA, security association) ISAKMP (Internet Security Association and Key Management Protocol). Une SA ISAKMP est un canal sécurisé sur lequel IKE négocie les numéros de clé des datagrammes IP. Contrairement aux SA IPsec, les SA ISAKMP sont bidirectionnelles. Il n'est donc pas nécessaire de disposer de plus d'une association de sécurité.

La façon dont IKE négocie les numéros de clé lors de la phase 1 peut être configurée. IKE lit les informations concernant la configuration dans le fichier `/etc/inet/ike/config`. Ces informations incluent :

- des paramètres généraux tels que le nom des certificats de clés publiques ;
- l'activation ou non du mode de confidentialité de transmission parfaite (PFS) ;
- les interfaces concernées ;
- les protocoles de sécurité et leurs algorithmes ;
- la méthode d'authentification.

Les deux méthodes d'authentification utilisent respectivement les clés prépartagées et les certificats de clés publiques. Les certificats de clés publiques peuvent être autosignés ou émis par l'autorité de certification (AC) d'un fournisseur d'infrastructures de clés publiques (PKI). telles que beTrusted, Entrust, GeoTrust, RSA Security et Verisign.

Phase 2 d'IKE

La phase 2 est connue sous le nom de *Quick Mode* (mode rapide). Lors de la phase 2, IKE crée et gère les SA IPsec entre les systèmes qui exécutent le démon IKE. IKE utilise le canal sécurisé qui a été créé lors de la phase 1 pour protéger la transmission des numéros de clé. Le démon IKE crée les clés à partir d'un générateur de nombres aléatoires à l'aide du périphérique `/dev/random`. Le démon actualise les clés à une fréquence qui peut être configurée. Les numéros de clé sont accessibles aux algorithmes spécifiés dans le fichier de configuration `ipsecinit.conf` de la stratégie IPsec.

Choix de configuration IKE

Le fichier de configuration `/etc/inet/ike/config` contient des entrées de stratégie IKE. Pour que deux démons IKE puissent s'authentifier mutuellement, les entrées doivent être valides et les numéros de clé doivent être disponibles. Les entrées des fichiers de configuration déterminent la façon dont les numéros de clé seront utilisés pour authentifier l'échange qui a lieu lors de la phase 1. Il y a deux possibilités : les clés prépartagées ou les certificats de clés publiques.

Si l'entrée est `auth_method preshared`, ce sont les clés prépartagées qui sont utilisées pour authentifier l'échange. Si `auth_method` possède une valeur autre que `preshared`, l'authentification s'effectue à l'aide de certificats de clés publiques. Ces certificats peuvent être autosignés ou installés par un fournisseur de PKI. Pour plus d'informations, reportez-vous à la page de manuel `ike.config(4)`.

IKE avec clés prépartagées

Les clés prépartagées sont créées par un administrateur sur un système. Elles sont ensuite partagées hors bande avec les administrateurs de systèmes distants. Prenez soin de créer de longues clés aléatoires et de protéger le fichier et la transmission hors bande. Les clés sont placées dans le fichier `/etc/inet/secret/ike.preshared` de chaque système. Le fichier `ike.preshared` est réservé à IKE et le fichier `ipseckeys` à IPsec. Toute compromission des clés du fichier `ike.preshared` compromet toutes les clés qui en sont dérivées.

Le système de clés prépartagées doit être identique au système distant de clés correspondant. Les clés sont liées à une adresse IP donnée. Elles sont plus sécurisées lorsqu'un administrateur contrôle les systèmes communicants. Pour plus d'informations, reportez-vous à la page de manuel `ike.preshared(4)`.

IKE avec certificats de clés publiques

Grâce aux certificats de clés publiques, les systèmes communicants n'ont plus besoin de partager de numéros de clé secrets hors bande. Les clés publiques utilisent le protocole Diffie-Hellman (DH) pour authentifier et négocier les clés. Les certificats de clés publiques peuvent être soit autosignés, soit certifiés par une autorité de certification (AC).

Les certificats de clés publiques autosignés sont créés par l'administrateur. La commande `ikecert certlocal -ks` permet de créer la partie privée des biclés du système. Le certificat autosigné est ensuite émis, au format X.509, par le système distant. Le certificat du système distant est entré à l'aide de la commande `ikecert certdb` pour la partie publique de la clé. Les certificats autosignés résident dans le répertoire `/etc/inet/ike/publickeys` des systèmes communicants. Lorsque vous utilisez l'option `-T`, les certificats résident sur le matériel connecté.

Les certificats autosignés sont à mi-chemin entre les clés prépartagées et les AC. Contrairement aux clés prépartagées, les certificats autosignés peuvent être utilisés sur une machine portable ou sur un système susceptible d'être renuméroté. Pour autosigner un certificat pour un système n'ayant pas de numéro fixe, utilisez un nom alternatif de `DNS` (`www.example.org`) ou d'`email` (`root@domain.org`).

Les clés publiques peuvent être délivrées par un fournisseur de PKI ou une AC. Elles doivent être installées, avec les certificats AC qui les accompagnent, dans le répertoire `/etc/inet/ike/publickeys.` Lorsque vous utilisez l'option `-T`, les certificats résident sur le matériel connecté. Les fournisseurs émettent également des listes de révocation de certificats (LRC). Outre les clés et les certificats AC, vous devez également installer les LRC dans le répertoire `/etc/inet/ike/crls`.

Les certificats AC présentent l'avantage d'être certifiés par une organisation externe, et non par l'administrateur du site. Il s'agit en quelque sorte de certificats "certifiés". Comme les certificats autosignés, les certificats AC peuvent être utilisés sur une machine portable ou sur un système susceptible d'être renuméroté. Contrairement aux certificats autosignés, ils s'intègrent facilement aux environnement à grande échelle afin de protéger un grand nombre de systèmes communicants.

Protocole IKE et accélération matérielle

Les algorithmes IKE recoupent de nombreux calculs, notamment lors de la phase 1. Les systèmes qui traitent un grand nombre d'échanges peuvent utiliser une carte Sun Crypto Accelerator 1000 pour traiter les opérations de clés publiques. Les cartes Sun Crypto Accelerator 6000 et Sun Crypto Accelerator 4000 peuvent également être utilisées pour gérer les calculs onéreux relatifs à la phase 1.

Pour plus d'informations sur la manière dont le protocole IKE doit être configuré pour décharger les calculs sur la carte d'accélération, reportez-vous à la section “Configuration du

protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 1000 " à la page 633. Pour plus d'informations sur le stockage des clés, reportez-vous à la section "Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 4000 " à la page 634 et à la page de manuel `cryptoadm`(1M).

Protocole IKE et stockage matériel

Les certificats de clés publiques, ainsi que les clés privées et publiques peuvent être stockés sur une carte Sun Crypto Accelerator 6000 ou &sca 4;. En chiffrement RSA, la longueur maximale des clés prise en charge par la carte Sun Crypto Accelerator 4000 est de 2 048 bits. En chiffrement DSA, elle est de 1 024 bits. La carte Sun Crypto Accelerator 6000 prend en charge les algorithmes SHA-512 et ECC.

Pour plus d'informations sur la manière dont le protocole IKE doit être configuré pour accéder à la carte, reportez-vous à la section "Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 1000 " à la page 633. Pour plus d'informations sur l'ajout de certificats et de clés publiques à la carte, reportez-vous à la section "Génération et stockage de certificats de clés publiques sur le matériel" à la page 618.

Utilitaires et fichiers IKE

Vous trouverez, dans le tableau ci-dessous, une liste des fichiers de configuration de la stratégie IKE, les emplacements de stockage des clés IKE et les différentes commandes et divers services permettant d'implémenter IKE. Pour plus d'informations sur les services, reportez-vous au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base*.

TABLEAU 22–2 Fichiers de configuration IKE, emplacements de stockage des clés, commandes et services

Fichier, emplacement, commande ou service	Description	Pour plus d'informations
`svc:/network/ipsec/ike`	Dans la version actuelle, le service SMF gère IKE.	`smf`(5)
Démon `/usr/lib/inet/in.iked`	Démon IKE (Internet Key Exchange). Active la gestion automatique des clés. Dans la version actuelle, le service `ike` active ce démon. Dans les versions précédentes, la commande `in.iked` est utilisée.	`in.iked`(1M)
Commande `/usr/sbin/ikeadm`	Commande d'administration IKE permettant d'afficher et de modifier la stratégie IKE.	`ikeadm`(1M)
Commande `/usr/sbin/ikecert`	Commande de gestion de bases de données de certificats permettant de manipuler les bases de données locales détentrices de certificats de clés publiques. Ces bases de données peuvent également être stockées sur une carte Sun Crypto Accelerator 4000 connectée.	`ikecert`(1M)

TABLEAU 22–2 Fichiers de configuration IKE, emplacements de stockage des clés, commandes et services *(Suite)*

Fichier, emplacement, commande ou service	Description	Pour plus d'informations
Fichier `/etc/inet/ike/config`	Fichier de configuration par défaut de la stratégie IKE dans le répertoire `/etc/inet`. Contient les règles du site pour la concordance des requêtes IKE entrantes et la préparation des requêtes IKE sortantes. Dans la version actuelle, si ce fichier existe, le démon `in.iked` démarre lorsque le service `IKE` est activé. L'emplacement de ce fichier peut être modifié à l'aide de la commande `svccfg`.	`ike.config(4)`
Fichier `ike.preshared`	Fichier de clés prépartagées du répertoire `/etc/inet/secret`. Contient des numéros de clé secrets destinés à l'authentification pendant la phase 1. Ce fichier s'utilise lorsque IKE est configuré avec des clés prépartagées.	`ike.preshared(4)`
Répertoire `ike.privatekeys`	Répertoire de clés privés de `/etc/inet/secret`. Contient les clés privées de la biclé.	`ikecert(1M)`
Répertoire `publickeys`	Répertoire de `/etc/inet/ike` contenant les fichiers de certificats et clés publiques. Contient la clé publique de la biclé.	`ikecert(1M)`
Répertoire `crls`	Répertoire de `/etc/inet/ike` contenant les listes de révocation des clés publiques et des fichiers de certificats.	`ikecert(1M)`
Carte Sun Crypto Accelerator 1000	Matériel accélérant les opérations de clés publiques en les déchargeant du système d'exploitation.	`ikecert(1M)`
Carte Sun Crypto Accelerator 4000	Matériel accélérant les opérations de clés publiques en les déchargeant du système d'exploitation. Les clés publiques, les clés privées et les certificats de clés publiques peuvent également être stockés sur cette carte.	`ikecert(1M)`

Modifications apportées à IKE dans Solaris10

À partir de Solaris 9, IKE inclut les fonctionnalités suivantes :

- IKE peut être utilisé pour automatiser l'échange de clés pour IPsec via des réseaux IPv6. Pour plus d'informations, reportez-vous à la section "Gestion des clés avec IKE" à la page 586.

  Remarque – IKE ne peut pas être utilisé pour gérer des clés IPsec dans une zone non globale.

- Les opérations IKE relatives aux clés publiques peuvent être accélérées grâce à l'ajout d'une carte Sun Crypto Accelerator 1000 ou Sun Crypto Accelerator 4000 sur laquelle elles sont déchargées. Le déchargement accélère le chiffrement et réduit ainsi l'utilisation des ressources de système d'exploitation. Pour plus d'informations, reportez-vous à la section

"Protocole IKE et accélération matérielle" à la page 589. Pour plus d'informations sur les procédures, reportez-vous à la section "Configuration du protocole IKE en vue de l'utilisation du matériel connecté (liste des tâches)" à la page 632.

- Les certificats de clés publiques, les clés privées et les clés publiques peuvent être stockés sur une carte Sun Crypto Accelerator 4000. Pour plus d'informations sur le stockage des clés, reportez-vous à la section "Protocole IKE et stockage matériel" à la page 590.
- IKE peut être utilisé pour automatiser l'échange de clés pour IPsec depuis un système situé derrière un boîtier NAT. Cependant, les clés IPsec de l'ESP traversant le NAT ne peuvent pas être accélérées à l'aide d'un composant matériel. Pour plus d'informations, reportez-vous à la section "Passage de la translation d'adresses et IPsec" à la page 511. Pour plus d'informations sur les procédures, reportez-vous à la section "Configuration du protocole IKE pour les systèmes portables (liste des tâches)" à la page 624.
- Des paramètres de retransmission et de délai d'expiration des paquets ont été ajoutés au fichier `/etc/inet/ike/config`. Ces paramètres ajustent la négociation de la phase 1 d'IKE (Main Mode) afin de traiter les interférences réseau, les augmentations de trafic et l'interopération avec des plates-formes possédant des implémentations du protocole IKE différentes. Pour plus d'informations sur ces paramètres, reportez-vous à la page de manuel `ike.config`(4) Pour plus d'informations sur les procédures, reportez-vous à la section "Modification des paramètres de transmission du protocole IKE (liste des tâches)" à la page 635.

◆ ◆ ◆ CHAPITRE 23

Configuration du protocole IKE (tâches)

Ce chapitre décrit la procédure de configuration du protocole Internet Key Exchange (IKE) sur vos systèmes. Une fois configuré, ce protocole génère automatiquement les numéros de clé IPsec sur votre réseau. Le présent chapitre contient les informations suivantes :

Pour voir une présentation du protocole IKE, reportez-vous au Chapitre 22, "Protocole IKE (présentation)". Pour obtenir des informations de référence sur le protocole IKE, reportez-vous au Chapitre 24, "Protocole IKE (référence)". Pour consulter d'autres procédures, reportez-vous aux sections Exemples des pages de manuel `ikeadm`(1M), `ikecert`(1M) et `ike.config`(4).

Configuration du protocole IKE (liste des tâches)

L'authentification du protocole IKE peut s'effectuer à l'aide de clés prépartagées ou de certificats autosignés ou émanant d'autorités de certifications (AC). Les méthodes d'authentification IKE sont liées par une règle aux points d'extrémité protégés. Vous pouvez donc utiliser toutes les méthodes d'authentification IKE ou une seule d'entre elles sur un système. Un pointeur menant à une bibliothèque PKCS #11 permet aux certificats d'utiliser un accélérateur matériel connecté.

Une fois le protocole IKE configuré, vous devez effectuer les tâches IPsec qui utilisent cette configuration. Le tableau ci-dessous répertorie les tâches correspondant aux différentes configurations IKE.

Tâche	Description	Voir
Configuration du protocole IKE avec des clés prépartagées	Protégez les communications entre deux systèmes en faisant en sorte qu'ils partagent une clé secrète.	"Configuration du protocole IKE avec des clés prépartagées (liste des tâches)" à la page 594
Configuration du protocole IKE avec des certificats de clés publiques	Protégez les communications à l'aide de certificats de clés publiques. Ces certificats peuvent être autosignés ou attestés par un fournisseur de PKI.	"Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches)" à la page 606
Franchissement d'un boîtier NAT	Configurez les protocoles IPsec et IKE pour communiquer avec un système portable	"Configuration du protocole IKE pour les systèmes portables (liste des tâches)" à la page 624
Configuration du protocole IKE pour générer et stocker les certificats de clés publiques sur le matériel connecté	Accélérez les opérations IKE à l'aide d'une carte Sun Crypto Accelerator 1000 ou Sun Crypto Accelerator 4000. Vous pouvez également stocker les certificats de clés publiques sur la carte Sun Crypto Accelerator 4000.	"Configuration du protocole IKE en vue de l'utilisation du matériel connecté (liste des tâches)" à la page 632
Ajustement des paramètres de négociation de la phase 1	Modifiez la durée des négociations de clés IKE.	"Modification des paramètres de transmission du protocole IKE (liste des tâches)" à la page 635

Configuration du protocole IKE avec des clés prépartagées (liste des tâches)

Le tableau ci-dessous répertorie les procédures de configuration et de maintenance du protocole IKE avec des clés prépartagées.

Tâche	Description	Voir
Configuration du protocole IKE avec des clés prépartagées	Créez un fichier de stratégie IKE ainsi qu'une clé à partager.	"Configuration du protocole IKE avec des clés prépartagées" à la page 595
Actualisation des clés prépartagées sur un système IKE en cours d'exécution	Ajoutez des numéros de clé IKE sur les systèmes communicants.	"Actualisation des clés IKE prépartagées" à la page 598
Ajout de clés prépartagées à un système IKE en cours d'exécution	Ajoutez une nouvelle entrée de stratégie IKE et de nouveaux numéros de clé à un système appliquant actuellement la stratégie IKE.	"Ajout d'une clé IKE prépartagée pour une nouvelle entrée de stratégie dans `ipsecinit.conf`" à la page 601
Vérification de la concordance des clés prépartagées	Affichez les clés prépartagées sur les deux systèmes pour vous assurer qu'elles sont identiques.	"Méthode de vérification de la concordance des clés prépartagées IKE" à la page 604

Configuration du protocole IKE avec des clés prépartagées

Les clés prépartagées sont la méthode d'authentification la plus simple pour IKE. Elles s'utilisent notamment lors de la configuration du protocole IKE sur deux systèmes gérés par le même administrateur. N'oubliez cependant pas que, contrairement aux certificats de clés publiques, les clés prépartagées sont liées à une adresse IP donnée et ne peuvent pas s'utiliser avec des systèmes portables ou des systèmes susceptibles d'être renumérotés. Tenez également compte du fait que, si vous utilisez des clés prépartagées, vous ne pourrez pas décharger de calculs IKE sur le matériel connecté.

▼ Configuration du protocole IKE avec des clés prépartagées

La longueur des clés des algorithmes d'implémentation du protocole IKE est variable. Elle dépend du niveau de sécurité dont vous souhaitez doter le site. En règle générale, la longueur des clés est proportionnelle au niveau de sécurité.

Les noms de systèmes choisis pour illustrer cette procédure sont : `enigma` et `partym`. Remplacez `enigma` et `partym` par les noms de vos systèmes.

1 **Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

---

2 **Copiez le fichier `/etc/inet/ike/config.sample` dans le fichier `/etc/inet/ike/config` sur chacun des systèmes.**

3 Entrez les règles et paramètres globaux dans le fichier `ike/config` sur chacun des systèmes.

Les règles et paramètres globaux de ce fichier doivent garantir le fonctionnement de la stratégie IPsec du fichier `ipsecinit.conf`. Les exemples `ike/config` ci-dessous vont de pair avec les exemples `ipsecinit.conf` de la section "Sécurisation du trafic entre deux systèmes à l'aide d'IPsec" à la page 519.

a. Modifiez par exemple le fichier `/etc/inet/ike/config` sur le système `enigma` :

```
### ike/config file on enigma, 192.168.116.16

## Global parameters
#
## Phase 1 transform defaults
p1_lifetime_secs 14400
p1_nonce_len 40
#
## Defaults that individual rules can override.
p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 2
#
## The rule to communicate with partym
#  Label must be unique
{ label "enigma-partym"
  local_addr 192.168.116.16
  remote_addr 192.168.13.213
  p1_xform
   { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
  p2_pfs 5
}
```

Remarque – Tous les arguments du paramètre `auth_method` doivent se trouver sur la même ligne.

---

b. Modifiez le fichier `/etc/inet/ike/config` sur le système `partym` :

```
### ike/config file on partym, 192.168.13.213
## Global Parameters
#
p1_lifetime_secs 14400
p1_nonce_len 40
#
p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 2

## The rule to communicate with enigma
#  Label must be unique
{ label "partym-enigma"
  local_addr 192.168.13.213
  remote_addr 192.168.116.16
p1_xform
   { auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
p2_pfs 5
}
```

4 **Vérifiez la syntaxe du fichier sur chacun des systèmes.**

```
# /usr/lib/inet/in.iked -c -f /etc/inet/ike/config
```

5 **Générez des nombres aléatoires que vous utiliserez comme numéros de clé.**

Si votre site possède un générateur de nombres aléatoires, utilisez-le. Sur un système Solaris, vous pouvez utiliser la commande `od`. La commande suivante vous permet par exemple d'imprimer deux lignes de nombres hexadécimaux :

```
% od -X -A n /dev/random | head -2
         f47cb0f4 32e14480 951095f8 2b735ba8
         0a9467d0 8f92c880 68b6a40e 0efe067d
```

Pour plus de détails sur la commande `od`, reportez-vous à la section "Génération de numéros aléatoires sur un système Solaris" à la page 527 et à la page de manuel `od(1)`.

Remarque – D'autres systèmes d'exploitation peuvent nécessiter des numéros de clé au format ASCII. Pour générer une clé identique dans les deux formats, hexadécimal et ASCII, reportez-vous à l'Exemple 23–1.

---

6 **Créez une clé à partir du résultat de l'Étape 5.**

```
f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
```

Pour cette procédure, l'algorithme d'authentification est SHA–1, comme indiqué à l'Étape 3. La taille du hachage, c'est-à-dire la taille de la sortie de l'algorithme d'authentification, détermine la taille minimale recommandée pour une clé prépartagée. La taille de la sortie de l'algorithme SHA–1 est de 160 bits ou 40 caractères. Dans cet exemple, la clé possède 56 caractères, ce qui permet au protocole IKE de disposer de numéros de clé supplémentaires.

7 **Créez un fichier `/etc/inet/secret/ike.preshare` sur chacun des systèmes.**

Placez la clé prépartagée dans chacun des fichiers.

a. **Sur le système `enigma` par exemple, le fichier `ike.preshared` se présente comme suit :**

```
# ike.preshared on enigma, 192.168.116.16
#...
{ localidtype IP
    localid 192.168.116.16
    remoteidtype IP
    remoteid 192.168.13.213
    # enigma and partym's shared key in hex (192 bits)
    key f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
    }
```

b. **Sur le système `partym`, le fichier `ike.preshared` se présente comme suit :**

```
# ike.preshared on partym, 192.168.13.213
#...
{ localidtype IP
    localid 192.168.13.213
    remoteidtype IP
```

```
        remoteid 192.168.116.16
        # partym and enigma's shared key in hex (192 bits)
        key f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
        }
```

Remarque – Les clés prépartagées doivent être identiques sur chacun des systèmes.

Exemple 23–1 Génération de numéros de clé identiques pour deux systèmes dotés de systèmes d'exploitation différents

Le protocole IPsec de Solaris fonctionne avec d'autres systèmes d'exploitation. Si votre système communique avec un système qui requiert des clés prépartagées ASCII, vous devez générer une clé dans les deux formats, hexadécimal et ASCII.

Dans cet exemple, l'administrateur système de Solaris veut générer une clé de 56 caractères. Il utilise la commande ci-dessous pour générer une clé hexadécimale à partir d'une phrase de passe ASCII. L'option `-tx1` imprime les octets un par un sur tous les systèmes Solaris.

```
# /bin/echo "papiermache with cashews and\c" | od -tx1 | cut -c 8-55 | \
tr -d '\n' | tr -d ' ' | awk '{print}'
7061706965726d6163686520776974682063617368657773206 16e64
```

Après suppression des décalages et concaténation de la sortie hexadécimale, la clé hexadécimale pour le système Solaris est `7061706965726d6163686520776974682063617368657773206 16e64`. L'administrateur place cette valeur dans le fichier `ike.preshared` sur le système Solaris.

```
# Shared key in hex (192 bits)
key 7061706965726d6163686520776974682063617368657773206 16e64
```

Sur le système qui requiert des clés prépartagées ASCII, la phrase de passe correspond à la clé prépartagée. L'administrateur Solaris communique la phrase de passe `papiermache with cashews and` à l'autre administrateur par téléphone.

▼ Actualisation des clés IKE prépartagées

Cette procédure permet de remplacer une clé prépartagée existante à intervalles réguliers.

1 **Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

2 Générez des nombres aléatoires et créez une clé possédant une longueur appropriée.

Pour plus d'informations, reportez-vous à la section "Génération de numéros aléatoires sur un système Solaris" à la page 527. Si vous générez une clé prépartagée pour un système Solaris qui communique avec un système d'exploitation nécessitant une clé ASCII, reportez-vous à l'Exemple 23–1.

3 Remplacez la clé actuelle par une nouvelle clé.

À titre d'exemple, sur les hôtes `enigma` et `partym`, cela revient à remplacer la valeur de `key` stockée dans le fichier `/etc/inet/secret/ike.preshared` par un nouveau nombre possédant la même longueur.

4 Lisez la nouvelle clé dans le noyau.

- **À partir de la version Solaris 10 4/09 actualisez le service `ike`.**

  ```
  # svcadm refresh ike
  ```

- **Si vous exécutez une version antérieure à la version Solaris 10 4/09, arrêtez et redémarrez le démon `in.iked`.**

  a. **Vérifiez le niveau de privilège du démon `in.iked`.**

  ```
  # /usr/sbin/ikeadm get priv
  Current privilege level is 0x0, base privileges enabled
  ```

  Vous pouvez modifier les numéros de clé si la commande renvoie un niveau de privilège `0x1` ou `0x2`. Si le niveau renvoyé est `0x0`, vous ne pouvez ni modifier ni afficher les numéros de clé. Par défaut, le démon `in.iked` s'exécute au niveau de privilège `0x0`.

  b. **Si le niveau de privilège est `0x0`, arrêtez le démon et redémarrez-le.**

  Lorsque le démon redémarre, il lit la nouvelle version du fichier `ike.preshared`.

  ```
  # pkill in.iked
  # /usr/lib/inet/in.iked
  ```

  c. **Si le niveau de privilège est `0x1` ou `0x2`, lisez la nouvelle version du fichier `ike.preshared`.**

  ```
  # ikeadm read preshared
  ```

▼ Affichage des clés IKE prépartagées

Par défaut, la commande `ikeadm` vous empêche de consulter les clés réelles dans le fichier de vidage d'une SA phase 1. L'affichage des clés est utile lors du débogage.

Pour afficher les clés réelles, vous devez augmenter le niveau de privilège du démon. Pour obtenir une description des niveaux de privilège, reportez-vous à la section “Commande d'administration du protocole IKE ” à la page 641.

Remarque – Pour effectuer cette procédure sur une version antérieure à la version Solaris 10 4/09, voir l'Exemple 23–2.

Avant de commencer IKE est configuré et le service `ike` est en cours d'exécution.

1 Affichez les clés IKE prépartagées.

```
# ikeadm
ikeadm> dump preshared
```

2 Si une erreur se produit, vous devez augmenter le niveau de privilège du démon `in.iked`.

a. Augmentez le niveau de privilège du démon `in.iked` dans le référentiel SMF.

```
# svcprop -p config/admin_privilege ike
base
# svccfg -s ike setprop config/admin_privilege=keymat
```

b. Augmentez le niveau de privilège du démon `in.iked` en cours d'exécution.

```
# svcadm refresh ike ; svcadm restart ike
```

c. (Facultatif) Confirmez que le niveau de privilège est `keymat`.

```
# svcprop -p config/admin_privilege ike
keymat
```

d. Affichez les clés en exécutant de nouveau l'Étape 1.

3 Réappliquez le niveau de privilège de base au démon IKE.

a. Après l'affichage des clés, rétablissez le niveau de privilège à sa valeur par défaut.

```
# svccfg -s ike setprop config/admin_privilege=base
```

b. Actualisez, puis redémarrez IKE.

```
# svcadm refresh ike ; svcadm restart ike
```

Exemple 23–2 Vérification des clés IKE prépartagées dans une version antérieure à la version Solaris 10 4/09

Dans l'exemple suivant, l'administrateur affiche les clés sur un système Solaris n'exécutant pas la version actuelle de Solaris. L'administrateur souhaite vérifier que les clés de ce système sont identiques aux clés du système communicant. Après avoir vérifié que les clés sont identiques sur les deux systèmes, l'administrateur rétablit le niveau de privilège sur 0.

- Tout d'abord, l'administrateur détermine le niveau de privilège du démon `in.iked`.

```
adm1 # /usr/sbin/ikeadm get priv
Current privilege level is 0x0, base privileges enabled
```

- Le niveau de privilège n'étant pas 0x1 ni 0x2, l'administrateur arrête le démon `in.iked`, puis augmente le niveau de privilège sur 2.

```
adm1 # pkill in.iked
adm1 # /usr/lib/inet/in.iked -p 2
Setting privilege level to 2
```

- L'administrateur affiche les clés.

```
adm1 # ikeadm dump preshared
PSKEY: Preshared key (24 bytes): f47cb.../192
LOCIP: AF_INET: port 0, 192.168.116.16 (adm1).
REMIP: AF_INET: port 0, 192.168.13.213 (com1).
```

- L'administrateur se connecte à distance au système communicant et détermine si les clés sont identiques.
- L'administrateur rétablit ensuite le niveau de privilège de base.

```
# ikeadm set priv base
```

▼ Ajout d'une clé IKE prépartagée pour une nouvelle entrée de stratégie dans `ipsecinit.conf`

Si vous ajoutez des entrées de stratégie IPsec pendant que IPsec and IKE sont en cours d'exécution, vous devez lire la nouvelle stratégie et les règles IKE dans le noyau. À partir de la version Solaris 10 4/09, redémarrez le service `policy` et actualisez le service `ike` une fois les nouvelles clés ajoutées.

Remarque – Pour effectuer cette procédure sur une version antérieure à la version Solaris 10 4/09, voir l'Exemple 23–3.

Avant de commencer

L'exécution de cette procédure nécessite le respect des conditions suivantes :

- Le système `enigma` est paramétré selon la procédure décrite à la section "Configuration du protocole IKE avec des clés prépartagées" à la page 595.
- Le système `enigma` protégera son trafic avec un nouveau système, `ada`.

- Le démon `in.iked` est exécuté sur les deux systèmes.
- Les interfaces des systèmes figurent en tant qu'entrées dans le fichier `/etc/hosts` sur les deux systèmes. Ci-dessous un exemple d'entrée :

  ```
  192.168.15.7 ada
  192.168.116.16 enigma
  ```

  Cette procédure fonctionne également avec une adresse IPv6 du fichier `/etc/inet/ipnodes`. À partir de la version Solaris 10 6/07, les entrées IPv6 sont placées dans le fichier `/etc/hosts`.
- Vous avez ajouté une nouvelle entrée de stratégie au fichier `/etc/inet/ipsecinit.conf` sur les deux systèmes. Ces entrées se présentent de la manière suivante :

  ```
  # ipsecinit.conf file for enigma
  {laddr enigma raddr ada} ipsec {auth_algs any encr_algs any sa shared}

  # ipsecinit.conf file for ada
  {laddr ada raddr enigma} ipsec {auth_algs any encr_algs any sa shared}
  ```
- Dans la version actuelle, vous avez vérifié la syntaxe du fichier `/etc/inet/ipsecinit.conf` sur les deux systèmes à l'aide de :

  ```
  # ipsecconf -c -f /etc/inet/ipsecinit.conf
  ```

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

---

2 Sur ce système, générez des nombres aléatoires et construisez une clé de 64 ou 448 bits.

Pour plus d'informations, reportez-vous à la section “Génération de numéros aléatoires sur un système Solaris” à la page 527. Si vous générez une clé prépartagée pour un système Solaris qui communique avec un système d'exploitation nécessitant une clé ASCII, reportez-vous à l'Exemple 23–1.

3 Transmettez la clé à l'administrateur du système distant.

Vous devez tous deux ajouter simultanément la même clé prépartagée. La sécurité de cette clé est directement liée à celle du moyen de transmission. Utilisez donc de préférence un moyen hors bande de type courrier recommandé ou fax protégé. Vous pouvez également utiliser une session `ssh` pour administrer les deux systèmes.

4 Créez une règle pour la gestion des clés de `enigma` et `ada` par IKE.

a. Sur le système `enigma`, ajoutez la règle suivante au fichier `/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
 p1_xform
 {auth_method preshared oakley_group 5 auth_alg sha1 encr_alg blowfish}
 p2_pfs 5
    }
```

b. Sur le système `ada`, ajoutez la règle suivante :

```
### ike/config file on ada, 192.168.15.7

## The rule to communicate with enigma

{label "ada-to-enigma"
 local_addr 192.168.15.7
 remote_addr 192.168.116.16
 p1_xform
 {auth_method preshared oakley_group 5 auth_alg sha1 encr_alg blowfish}
 p2_pfs 5
}
```

5 Assurez-vous que les clés IKE prépartagées sont disponibles lors de la réinitialisation.

a. Sur le système `enigma`, ajoutez les informations suivantes au fichier `/etc/inet/secret/ike.preshared` :

```
# ike.preshared on enigma for the ada interface
#
{ localidtype IP
  localid 192.168.116.16
  remoteidtype IP
  remoteid 192.168.15.7
  # enigma and ada's shared key in hex (32 - 448 bits required)
  key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d
}
```

b. Sur le système `ada`, ajoutez les informations suivantes au fichier `ike.preshared` :

```
# ike.preshared on ada for the enigma interface
#
{ localidtype IP
  localid 192.168.15.7
  remoteidtype IP
  remoteid 192.168.116.16
  # ada and enigma's shared key in hex (32 - 448 bits required)
  key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d
}
```

6 **Sur chaque système, redémarrez le service de stratégie IPsec afin de sécuriser l'interface ajoutée.**

```
# svcadm restart policy
```

7 **Sur chaque système, actualisez le service `ike`.**

```
# svcadm refresh ike
```

8 **Assurez-vous que les systèmes peuvent communiquer entre eux.**

Reportez-vous à la section "Méthode de vérification de la concordance des clés prépartagées IKE" à la page 604.

Exemple 23–3 Ajout d'une clé IKE prépartagée pour une nouvelle entrée de stratégie IPsec

Dans l'exemple suivant, l'administrateur ajoute une clé prépartagée à un système Solaris n'exécutant pas la version actuelle de Solaris. L'administrateur suit la procédure précédente pour modifier les fichiers `ike/config` et `ike.preshared` et pour générer des clés et contacter le système distant. L'administrateur utilise différentes commandes pour lire la nouvelle stratégie IPsec et les nouvelles règles IKE dans le noyau.

- Avant de générer une nouvelle clé, l'administrateur définit le niveau de privilège du démon `in.iked` sur 2.

```
# pkill in.iked
# /usr/lib/inet/in.iked -p 2
Setting privilege level to 2
```

- Après l'envoi de la clé à l'autre système et l'ajout d'une nouvelle clé au système, l'administrateur réduit le niveau de privilège.

```
# ikeadm set priv base
```

- Ensuite, l'administrateur lit la nouvelle stratégie IPsec dans le noyau.

```
# ipsecconf -a /etc/inet/ipsecinit.conf
```

- Enfin, l'administrateur lit les nouvelles règles IKE dans le noyau.

```
# ikeadm read rules
```

▼ Méthode de vérification de la concordance des clés prépartagées IKE

La concordance clés prépartagées des systèmes communicants est nécessaire à l'authentification.

Avant de commencer IPsec est configuré et a été activé entre les deux systèmes sur lesquels vous travaillez. Vous exécutez la version actuelle Solaris 10.

Remarque – Pour effectuer cette procédure sur une version antérieure à la version Solaris 10 4/09, voir l'Exemple 23–2.

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

2 Sur chaque système, vérifiez le niveau de privilège du démon `in.iked`.

```
# svcprop -p config/admin_privilege ike
base
```

- **Si le niveau de privilège est `keymat`, passez à l'Étape 3.**
- **Si le niveau de privilège est `base` ou `modkeys`, augmentez le niveau de privilège.**

  Effectuez une actualisation, puis redémarrez le service `ike`.

  ```
  # svccfg -s ike setprop config/admin_privilege=keymat
  # svcadm refresh ike ; svcadm restart ike
  # svcprop -p config/admin_privilege ike
  keymat
  ```

3 Affichez, sur chacun des systèmes, les informations concernant les clés prépartagées.

```
# ikeadm dump preshared
PSKEY: Preshared key (24 bytes): f47cb.../192
LOCIP: AF_INET: port 0, 192.168.116.16 (enigma).
REMIP: AF_INET: port 0, 192.168.13.213 (partym).
```

4 Comparez les résultats obtenus.

Si les clés prépartagées ne sont pas identiques, remplacez l'une d'entre elles dans le fichier `/etc/inet/secret/ike.preshared`.

5 Lorsque la vérification est terminée, rétablissez le niveau de privilège par défaut sur chacun des systèmes.

```
# svccfg -s ike setprop config/admin_privilege=base
# svcadm restart ike
```

Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches)

Le tableau ci-dessous répertorie les procédures de création de certificats de clés publiques pour IKE. Ces procédures incluent l'accélération et le stockage de certificats sur le matériel connecté.

Tâche	Description	Voir
Configuration du protocole IKE avec des certificats de clés publiques autosignés	Créez et placez deux certificats sur chaque système : ■ un certificat autosigné ; ■ le certificat de clé publique du système distant.	"Configuration du protocole IKE avec des certificats de clés publiques autosignés" à la page 607
Configuration du protocole IKE avec un certificat PKI émanant d'une autorité de certification	Créez une demande de certificat et placez trois certificats sur chacun des systèmes : ■ le certificat créé par l'autorité de certification (AC) suite à votre demande ; ■ le certificat de clé publique de l'AC ; ■ la LRC de l'AC.	"Configuration du protocole IKE avec des certificats signés par une AC" à la page 612
Configuration de certificats de clés publiques sur le matériel local	Procédez de l'une des manières suivantes : ■ Générez un certificat autosigné sur le matériel local et ajoutez la clé publique d'un système distant sur le matériel. ■ Générez une demande de certificat sur le matériel local et ajoutez les certificats de clés publiques de l'AC sur le matériel.	"Génération et stockage de certificats de clés publiques sur le matériel" à la page 618
Mise à jour de la liste de révocation de certificats (LRC) d'une PKI	Accédez à la LRC depuis un point de distribution central.	"Traitement des listes de révocation de certificats" à la page 622

Configuration du protocole IKE avec des certificats de clés publiques

Grâce aux certificats de clés publiques, les systèmes communicants n'ont plus besoin de partager de numéros de clé secrets hors bande. Contrairement aux clés prépartagées, les certificats de clés publiques peuvent être utilisés sur une machine portable ou sur un système susceptible d'être renuméroté.

Les certificats de clés publiques peuvent également être stockés sur le matériel connecté. Pour plus d'informations sur cette procédure, reportez-vous à la section "Configuration du protocole IKE en vue de l'utilisation du matériel connecté (liste des tâches)" à la page 632.

▼ Configuration du protocole IKE avec des certificats de clés publiques autosignés

Les certificats autosignés nécessitent un temps système inférieur à celui des certificats publics émanant d'une AC, mais s'intègrent plus difficilement dans un environnement à grande échelle.

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

---

2 Ajoutez un certificat autosigné à la base de données `ike.privatekeys`.

```
# ikecert certlocal -ks|-kc -m keysize -t keytype \
-D dname -A altname \
[-S validity-start-time] [-F validity-end-time] [-T token-ID]
```

`-ks`	Crée un certificat autosigné.
`-kc`	Crée une demande de certificat. Pour plus d'informations sur cette procédure, reportez-vous à la section "Configuration du protocole IKE avec des certificats signés par une AC" à la page 612.
`-m` *taille de clé*	Taille de la clé. La *taille de clé* peut être 512, 1 024, 2 048, 3 072 ou 4 096.
`-t` *type de clé*	Spécifie le type d'algorithme à utiliser. Le *type de clé* peut être `rsa-sha1`, `rsa-md5` ou `dsa-sha1`.
`-D` *nom distinctif*	Nom distinctif X.509 de l'objet du certificat. Le *nom distinctif* se présente de la manière suivante : C=pays, O=organisation, OU=unité d'organisation, CN=nom commun. Les balises valides sont C, O, OU et CN.
`-A` *nom alternatif*	Nom alternatif du certificat. Le *nom alternatif* se présente de la manière suivante : `tag=value`. Les balises valides sont `IP`, `DNS`, `email` et `DN`.
`-S`, *début de validité*	Indique la date de début de validité absolue ou relative du certificat.
`-F`, *fin de validité*	Indique la date de fin de validité absolue ou relative du certificat.

-T *ID de jeton* Permet à un jeton matériel PKCS #11 de générer les clés. Les certificats sont alors stockés sur le matériel.

a. Exécutée par exemple sur le système `partym`, la commande se présente comme suit :

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
-A IP=192.168.13.213
Creating software private keys.
  Writing private key to file /etc/inet/secret/ike.privatekeys/0.
Enabling external key providers - done.
Acquiring private keys for signing - done.
Certificate:
 Proceeding with the signing operation.
 Certificate generated successfully (.../publickeys/0)
Finished successfully.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIICLTCCAZagAwIBAgIBATANBgkqhkiG9w0BAQQFADBNMQswCQYDVQQGEwJVUzEX
...
6sKTxpg4GP3GkQGcd0r1rhW/3yaWBkDwOdFCqEUyffzU
-----END X509 CERTIFICATE-----
```

b. Exécutée sur le système `enigma`, elle se présente de la manière suivante :

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax" \
-A IP=192.168.116.16
Creating software private keys.
  ...
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIICKDCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQQFADBJMQswCQYDVQQGEwJVUzEV
...
jpxfLM98xyFVyLCbkr3dZ3Tvxvi732BXePKF2A==
-----END X509 CERTIFICATE-----
```

3 Enregistrez le certificat et envoyez-le au système distant.

Vous pouvez le coller dans un e-mail.

a. Transmettez le certificat de `partym` à l'administrateur de `enigma` :

```
To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIICLTCCAZagAwIBAgIBATANBgkqhkiG9w0BAQQFADBNMQswCQYDVQQGEwJVUzEX
...
6sKTxpg4GP3GkQGcd0r1rhW/3yaWBkDwOdFCqEUyffzU
-----END X509 CERTIFICATE-----
```

b. L'administrateur de `enigma` vous envoie le certificat `enigma` suivant :

```
To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIICKDCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQQFADBJMQswCQYDVQQGEwJVUzEV
```

```
...
jpxfLM98xyFVyLCbkr3dZ3Tvxvi732BXePKF2A==
-----END X509 CERTIFICATE-----
```

4 Sur chaque système, ajoutez le certificat que vous avez reçu.

a. Copiez la clé publique que l'administrateur vous a envoyée par e-mail.

b. Saisissez la commande `ikecert certdb -a` et appuyez sur la touche Retour.

Aucune invite ne s'affiche lorsque vous appuyez sur la touche Retour.

```
# ikecert certdb -a       Press the Return key
```

c. Collez la clé publique, puis appuyez sur la touche Retour. Pour clore l'entrée, appuyez sur Ctrl-D.

```
-----BEGIN X509 CERTIFICATE-----
MIIC...
...
----END X509 CERTIFICATE-----       Press the Return key
<Control>-D
```

5 Vérifiez auprès de l'autre administrateur que ce certificat est bien de lui.

Vous pouvez par exemple lui téléphoner et comparer la valeur de hachage de la clé publique. La valeur de hachage de clé publique du certificat partagé doit être identique pour les deux systèmes.

a. Répertoriez les certificats stockés sur votre système.

Par exemple, sur le système `partym`, le certificat public se trouve à l'emplacement 1 et le certificat privé à l'emplacement 0.

```
partym # ikecert certdb -l
Certificate Slot Name: 0   Type: rsa-md5      Private Key
    Subject Name: <C=US, O=PartyCompany, OU=US-Partym, CN=Partym>
    Key Size: 1024
    Public key hash: B2BD13FCE95FD27ECE6D2DCD0DE760E2

Certificate Slot Name: 1   Type: rsa-md5      Public Certificate
    (Private key in certlocal slot 0)      Points to certificate's private key
    Subject Name: <C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax>
    Key Size: 1024
    Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

b. Comparez cette valeur avec le hachage de la clé publique sur le système `enigma`.

Vous pouvez communiquer la valeur de hachage par téléphone.

```
enigma # ikecert certdb -l
Certificate Slot Name: 4   Type: rsa-md5      Private Key
    Subject Name: <C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax>
```

```
    Key Size: 1024
    Public key hash: DF3F108F6AC669C88C6BD026B0FCE3A0

Certificate Slot Name: 5   Type: rsa-md5      Public Certificate
    (Private key in certlocal slot 4)
    Subject Name: <C=US, O=PartyCompany, OU=US-Partym, CN=Partym>
    Key Size: 1024
    Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

6 Approuvez les deux certificats sur chacun des systèmes.

Éditez le fichier `/etc/inet/ike/config` pour reconnaître les certificats.

L'administrateur du système distant fournit la valeur des paramètres `cert_trust`, `remote_addr` et `remote_id`.

a. Sur le système `partym` par exemple, le fichier `ike/config` se présente de la manière suivante :

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

# Verified remote address and remote ID
# Verified public key hash per telephone call from administrator
cert_trust "192.168.13.213"      Local system's certificate Subject Alt Name
cert_trust "192.168.116.16"      Remote system's certificate Subject Alt Name

## Parameters that may also show up in rules.

p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 5

{
 label "US-partym to JA-enigmax"
 local_id_type dn
 local_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
 remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

 local_addr  192.168.13.213
 remote_addr 192.168.116.16

 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

b. Sur le système `enigma`, ajoutez les valeurs de `enigma` des paramètres locaux dans le fichier `ike/config`.

Pour les paramètres distants, utilisez les valeurs de `partym`. Assurez-vous que la valeur du mot-clé `label` est unique. Elle doit différer de la valeur `label` du système distant.

```
...
{
 label "JA-enigmax to US-partym"
 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
...
```

Exemple 23–4 Vérification de la validité du certificat d'un autre administrateur

Dans cet exemple, les administrateurs vérifient la concordance des certificats à l'aide de l'attribut Subject Name.

Le premier administrateur enregistre la sortie de la génération et du listage du certificat dans un fichier. La sortie de la commande `ikecert` s'imprimant en erreur standard, l'administrateur redirige l'erreur standard vers le fichier.

```
sys1# cd /
sys1# ikecert certlocal -ks -m1024 -t rsa-md5 \
-D"C=US, O=TestCo, CN=Co2Sys" 2>/tmp/for_co2sys
Certificate added to database.
sys1# ikecert certdb -l "C=US, O=TestCo, CN=Co2Sys" 2>>/tmp/for_co2sys
```

L'administrateur vérifie le contenu du fichier.

```
sys1# cat /tmp/for_co2sys
Creating private key.
-----BEGIN X509 CERTIFICATE-----
MIIB7TCCAVagAwIBAgIEZkHfOTANBgkqhkiG9w0BAQQFADAxMQwwCgYDVQQGEwNV
U0ExEDAOBgNVBAoMB3Rlc3RfY28xDzANBgNVBAMTBkVuaWdtYTAeFw0wODAxMTUx
OTI1MjBaFw0xMjAxMTUxOTI1MjBaMDExDDAKBgNVBAYTA1VTQTEQMA4GA1UECgwH
dGVzdF9jbzEPMA0GA1UEAxMGRW5pZ21hMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQCPxGv0rUzHMnFtkx9uwYuPiWbftmWfa9iDt6ELOEuw3zlboy2qtuRUZohz
FIbCxAJevdCY6a+pktvYy3/2nJL0WATObO5T0FKn3F0bphajinLYbyCrYhEzD9E2
gkiT2D9/ttbSiMvi9usphprEDcLAFaWgCJiHnKPBEkjC0vhA3wIDAQABoxIwEDAO
BgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEEBQADgYEAL/q6xgweylGQylqLCwzN
5PIpjfzsNPf3saTyh3VplwEOW6WTHwRQT17IO/1Oc6Jnz9Mr0ZrbHWDXq+1sx180
F8+DMW1Qv1UR/lGMq3ufDG3qedmSN6txDF8qLlPCUML0YL8m4oGdewqGb+78aPyE
Y/cJRsK1hWbYyseqcIkjj5k=
-----END X509 CERTIFICATE-----
Certificate Slot Name: 2   Key Type: rsa
        (Private key in certlocal slot 2)
        Subject Name: <C=US, O=TestCo, CN=Co2Sys>
        Key Size: 1024
        Public key hash: C46DE77EF09084CE2B7D9C70479D77FF
```

Ensuite, l'administrateur envoie le fichier par courrier électronique au deuxième administrateur.

Celui-ci place le fichier dans un répertoire sécurisé, puis importe le certificat à partir du fichier.

```
sys2# cd /
sys2# ikecert certdb -a < /sec/co2sys
```

La commande `ikecert` importe uniquement le texte entre les lignes `-----BEGIN` et `-----END`. L'administrateur vérifie que le certificat local possède une clé de hachage publique identique à celle du fichier `co2sys`.

```
sys2# ikecert certdb -l
Certificate Slot Name: 1   Key Type: rsa
        (Private key in certlocal slot 1)
        Subject Name: <C=US, O=TestCo, CN=Co2Sys>
        Key Size: 1024
        Public key hash: C46DE77EF09084CE2B7D9C70479D77FF
```

Le deuxième administrateur s'assure par téléphone que le premier administrateur a bien envoyé ce message électronique et vérifie l'attribut Subject Name du certificat.

Exemple 23–5 Spécification de dates de début et de fin de validité de certificat.

Dans cet exemple, l'administrateur du système `partym` définit la période de validité du certificat. Le certificat est antidaté de 2,5 jours et sa période de validité est de 4 ans et 6 mois à compter de la date de création.

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
-A IP=192.168.13.213 \
-S -2d12h -F +4y6m
```

L'administrateur du système `enigma` définit la période de validité du certificat. Le certificat est antidaté de 2 jours et sa période de validité s'étend jusqu'au 31 décembre 2010, minuit.

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax" \
-A IP=192.168.116.16 \
-S -2d -F "12/31/2010 12:00 AM"
```

▼ Configuration du protocole IKE avec des certificats signés par une AC

Les certificats publics émanant d'autorités de certification (AC) requièrent une négociation avec une organisation externe. Ces certificats s'intègrent très facilement dans les environnements à grande échelle afin protéger un grand nombre de systèmes communicants.

1. **Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

   Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

   ---

2. **La commande `ikecert certlocal -kc` permet de créer une demande de certificat.**

   Pour consulter la description des arguments de la commande, reportez-vous à l'Étape 2 de la section "Configuration du protocole IKE avec des certificats de clés publiques autosignés" à la page 607.

   ```
   # ikecert certlocal -kc -m keysize -t keytype \
   -D dname -A altname
   ```

   a. **La commande suivante permet par exemple de créer une demande de certificats sur le système `partym` :**

   ```
   # ikecert certlocal -kc -m 1024 -t rsa-md5 \
   > -D "C=US, O=PartyCompany\, Inc., OU=US-Partym, CN=Partym" \
   > -A "DN=C=US, O=PartyCompany\, Inc., OU=US-Partym"
   Creating software private keys.
     Writing private key to file /etc/inet/secret/ike.privatekeys/2.
   Enabling external key providers - done.
   Certificate Request:
     Proceeding with the signing operation.
     Certificate request generated successfully (.../publickeys/0)
   Finished successfully.
   -----BEGIN CERTIFICATE REQUEST-----
   MIIByjCCATMCAQAwUzELMAkGA1UEBhMCVVMxHTAbBgNVBAoTFEV4YW1wbGVDb21w
   ...
   lcM+tw0ThRrfuJX9t/Qa1R/KxRlMA3zckO80mO9X
   -----END CERTIFICATE REQUEST-----
   ```

   b. **La commande suivante permet de créer une demande de certificat sur le système `enigma` :**

   ```
   # ikecert certlocal -kc -m 1024 -t rsa-md5 \
   > -D "C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax, CN=Enigmax" \
   > -A "DN=C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax"
   Creating software private keys.
   ...
   Finished successfully.
   -----BEGIN CERTIFICATE REQUEST-----
   MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu
   ...
   ```

```
8qlqdjaStLGfhDOO
-----END CERTIFICATE REQUEST-----
```

3 Soumettez la demande de certificat à un fournisseur de PKI.

Le fournisseur de PKI vous indiquera la procédure de soumission des demandes de certificat. Dans la plupart des cas, celle-ci s'effectue en remplissant un formulaire directement sur le site Web du fournisseur. Dans ce formulaire, vous devrez notamment indiquer la preuve de la légitimité de votre demande. Il suffit généralement de coller votre certificat dans le formulaire. Après avoir vérifié votre demande, le fournisseur émet les deux objets de certificats suivants et une liste des certificats révoqués :

- Votre certificat de clé publique – Ce certificat est basé sur la demande que vous avez envoyée au fournisseur. Cette demande est intégrée au certificat, qui vous identifie de manière unique.
- Un certificat AC – La signature du fournisseur. L'AC vérifie que votre certificat de clé publique est légitime.
- Une liste de révocation de certificats (LRC) – La liste la plus récente des certificats révoqués par le fournisseur. Cette liste n'est pas expédiée sous la forme d'un objet de certificat séparé si l'accès à la LRC est intégré au certificat de clé publique.

  Si un URI de LRC est intégré au certificat de clé publique, IKE peut récupérer automatiquement la LRC. De la même façon, si une entrée de DN (nom de répertoire sur un serveur LDAP) est intégrée au certificat de clé publique, IKE peut récupérer la LRC sur un serveur LDAP que vous avez spécifié et la mettre en cache.

  Pour consulter un exemple d'URI et d'entrée de DN intégrés à un certificat de clé publique, reportez-vous à la section "Traitement des listes de révocation de certificats" à la page 622.

4 Ajoutez tous les certificats sur votre système.

L'option `-a` de la commande `ikecert certdb -a` ajoute l'objet collé à la base de données de certificats correspondante de votre système. Pour plus d'informations, reportez-vous à la section "IKE avec certificats de clés publiques" à la page 589.

a. Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

b. Ajoutez le certificat de clé publique que vous avez reçu du fournisseur de PKI.

```
# ikecert certdb -a
     Press the Return key
     Paste the certificate:
-----BEGIN X509 CERTIFICATE-----
...
-----END X509 CERTIFICATE----
     Press the Return key
<Control>-D
```

c. Ajoutez le certificat AC émanant du fournisseur de PKI.

```
# ikecert certdb -a
     Press the Return key
     Paste the CA:
-----BEGIN X509 CERTIFICATE-----
...
-----END X509 CERTIFICATE----
     Press the Return key
<Control>-D
```

d. Si le fournisseur de PKI vous a envoyé une liste de révocation de certificats, ajoutez-la à la base de données `certrldb` :

```
# ikecert certrldb -a
     Press the Return key
     Paste the CRL:
-----BEGIN CRL-----
...
-----END CRL----
     Press the Return key
<Control>-D
```

5 Le mot-clé `cert_root` permet d'identifier le fournisseur de PKI dans le fichier `/etc/inet/ike/config`.

Utilisez le nom que le fournisseur de PKI vous a indiqué.

a. Sur le système `partym`, par exemple, le fichier `ike/config` peut se présenter de la manière suivante :

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

## Parameters that may also show up in rules.

p1_xform
 { auth_method rsa_sig oakley_group 1 auth_alg sha1 encr_alg des }
p2_pfs 2

{
 label "US-partym to JA-enigmax - Example PKI"
 local_id_type dn
 local_id  "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
 remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

 local_addr  192.168.13.213
 remote_addr 192.168.116.16

 p1_xform
```

```
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

Remarque – Tous les arguments du paramètre `auth_method` doivent se trouver sur la même ligne.

b. Créez un fichier similaire sur le système `enigma`.

Le fichier `enigma` `ike/config` doit :

- inclure la même valeur `cert_root` ;
- utiliser les valeurs de `enigma` pour les paramètres locaux ;
- utiliser les valeurs de `partym` pour les paramètres distants ;
- créer une valeur unique pour le mot-clé `label`. Elle doit différer de la valeur `label` du système distant.

```
...
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 Spécifiez le mode de traitement des LRC par le protocole IKE.

Choisissez l'option appropriée :

- **Pas de LRC disponible**

  Si le fournisseur de PKI ne fournit pas de LRC, ajoutez le mot-clé `ignore_crls` au fichier `ike/config`.

  ```
  # Trusted root cert
  ...
  cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example,...
  ignore_crls
  ...
  ```

  Le mot-clé `ignore_crls` indique au protocole IKE de ne pas chercher de LRC.

- **LRC disponible**

  Si le fournisseur de PKI vous communique un point de distribution central pour les LRC, vous pouvez modifier le fichier `ike/config` de manière à ce qu'il pointe sur cet emplacement.

Pour consulter des exemples de ce type de configuration, reportez-vous à la section "Traitement des listes de révocation de certificats" à la page 622.

Exemple 23–6 Utilisation de `rsa_encrypt` lors de la configuration du protocole IKE

Lorsque vous utilisez `auth_method rsa_encrypt` dans le fichier `ike/config`, vous devez ajouter le certificat homologue à la base de données `publickeys`.

1. Envoyez ce certificat à l'administrateur du système distant.

   Vous pouvez le coller dans un e-mail.

   L'administrateur de `partym` envoie le message suivant :

   ```
   To: admin@ja.enigmaexample.com
   From: admin@us.partyexample.com
   Message: -----BEGIN X509 CERTIFICATE-----
   MII...
   ----END X509 CERTIFICATE-----
   ```

   L'administrateur de `enigma` envoie l'e-mail suivant :

   ```
   To: admin@us.partyexample.com
   From: admin@ja.enigmaexample.com
   Message: -----BEGIN X509 CERTIFICATE-----
   MII
   ...
   -----END X509 CERTIFICATE-----
   ```

2. Sur chacun des systèmes, ajoutez à la base de données `publickeys` locale le certificat envoyé par e-mail.

   ```
   # ikecert certdb -a
       Press the Return key
   -----BEGIN X509 CERTIFICATE-----
   MII...
   -----END X509 CERTIFICATE-----
       Press the Return key
   <Control>-D
   ```

En cachant les identités à l'aide du protocole IKE, la méthode d'authentification utilisée en chiffrement RSA prévient les risques d'écoute électronique. Étant donné que la méthode `rsa_encrypt` cache l'identité de l'homologue, le protocole IKE ne peut récupérer son certificat. La méthode `rsa_encrypt` requiert donc que les homologues IKE connaissent leurs clés publiques respectives.

C'est pourquoi vous devez ajouter le certificat de l'homologue à la base de données `publickeys` lorsque vous utilisez la méthode `auth_method` de `rsa_encrypt` dans le fichier `/etc/inet/ike/config`. La base de données `publickeys` détient alors trois certificats pour chaque couple de systèmes communicants :

- votre certificat de clé publique ;
- le certificat AC ;
- le certificat de clé publique de l'homologue.

Dépannage – La charge du protocole IKE, qui inclut les trois certificats, peut s'avérer trop importante pour le chiffrement via `rsa_encrypt`. L'apparition d'erreurs indiquant que l'autorisation a échoué ou que la charge n'est pas conforme peut signifier que la méthode `rsa_encrypt` est incapable de chiffrer la totalité de la charge. Pour réduire la charge, utilisez une autre méthode (par exemple, `rsa_sig`, qui ne requiert que deux certificats).

▼ Génération et stockage de certificats de clés publiques sur le matériel

Le processus de génération et de stockage de certificats de clés publiques sur du matériel est similaire au processus de génération et de stockage de certificats de clés publiques sur un système. Dans le premier cas, il convient d'identifier le matériel à l'aide des commandes `ikecert certlocal` et `ikecert certdb`, accompagnées de l'option `-T` et de l'ID de jeton.

Avant de commencer

- Le matériel doit être configuré.
- Excepté si le mot-clé `pkcs11_path` du fichier `/etc/inet/ike/config` pointe sur une autre bibliothèque, le matériel utilise `/usr/lib/libpkcs11.so`. Cette bibliothèque doit être implémentée conformément aux standards suivants : RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki), c'est-à-dire une bibliothèque PKCS #11.

  Pour consulter les instructions de paramétrage, reportez-vous à la section "Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 4000 " à la page 634.

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

2 Générez un certificat autosigné ou une demande de certificat et spécifiez l'ID de jeton.

Procédez de l'une des manières suivantes :

Remarque – Pour RSA, la carte Sun Crypto Accelerator 4000 prend en charge des clés d'une longueur maximum de 2 048 bits. Pour DSA, la longueur maximum des clés est de 1 024 bits.

- **Pour un certificat autosigné, utilisez la syntaxe suivante :**

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
> -a -T dca0-accel-stor IP=192.168.116.16
Creating hardware private keys.
Enter PIN for PKCS#11 token:      Type user:password
```

L'argument de l'option `-T` est l'ID de jeton de la carte Sun Crypto Accelerator 4000 connectée.

- **Pour une demande de certificat, utilisez la syntaxe suivante :**

```
# ikecert certlocal -kc -m 1024 -t rsa-md5 \
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
> -a -T dca0-accel-stor IP=192.168.116.16
Creating hardware private keys.
Enter PIN for PKCS#11 token:      Type user:password
```

Pour obtenir une description des arguments de la commande `ikecert`, reportez-vous à la page de manuel `ikecert(1M)`.

3 Lorsque l'invite demandant le PIN s'affiche, entrez le nom de l'utilisateur de la carte Sun Crypto Accelerator 4000 suivi de deux points et du mot de passe de l'utilisateur.

Si la carte Sun Crypto Accelerator 4000 possède un utilisateur `ikemgr` dont le mot de passe est `rgm4tigt`, entrez :

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt
```

Remarque – La réponse est stockée en *texte en clair* sur le disque.

Après entrée du mot de passe, le certificat s'imprime :

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt
-----BEGIN X509 CERTIFICATE-----
```

```
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu
...
oKUDBbZ9O/pLWYGr
-----END X509 CERTIFICATE-----
```

4 Envoyez votre certificat aux personnes concernées.

Procédez de l'une des manières suivantes :

- **Envoyez le certificat autosigné au système distant.**

  Vous pouvez le coller dans un e-mail.

- **Envoyez la demande de certificat à un fournisseur de PKI.**

  Pour ce faire, suivez les instructions du fournisseur de PKI. Pour plus d'informations, reportez-vous à l'Étape 3 de la section "Configuration du protocole IKE avec des certificats signés par une AC" à la page 612.

5 Éditez le fichier `/etc/inet/ike/config` sur votre système pour reconnaître les certificats.

Procédez de l'une des manières suivantes :

- **Certificat autosigné**

  Utilisez les valeurs fournies par l'administrateur du système distant pour les paramètres `cert_trust`, `remote_id` et `remote_addr`. Sur le système `enigma` par exemple, le fichier `ike/config` se présente comme suit :

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

cert_trust "192.168.116.16"       Local system's certificate Subject Alt Name
cert_trust "192.168.13.213"       Remote system's certificate Subject Alt name


# Solaris 10 1/06 release: default path does not have to be typed in #pkcs11_path
"/usr/lib/libpkcs11.so"      Hardware connection

# Solaris 10 release: use this path
#pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
...
{
 label "JA-enigmax to US-partym"
 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
```

```
 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

- **Demande de certificat**

  Entrez le nom que le fournisseur de PKI vous a communiqué comme valeur du mot-clé `cert_root`. Sur le système `enigma` par exemple, le fichier `ike/config` peut se présenter comme suit :

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

# Solaris 10 1/06 release: default path does not have to be typed in #pkcs11_path
"/usr/lib/libpkcs11.so"      Hardware connection

# Solaris 10 release: use this path
#pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
...
{
 label "JA-enigmax to US-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

 p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha1 encr_alg aes}
}
```

6 **Placez les certificats de l'autre partie sur le matériel.**

Répondez à la demande de PIN comme vous l'avez fait au cours de l'Étape 3.

Remarque – Vous *devez* ajouter les certificats de clés publiques au matériel connecté qui a généré votre clé privée.

- **Certificat autosigné.**

  Ajoutez le certificat autosigné du système distant. Dans cet exemple, il est stocké dans le fichier `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 le certificat autosigné a utilisé `rsa_encrypt` comme valeur du paramètre `auth_method`, ajoutez le certificat de l'homologue au magasin du matériel.

- **Certificats émanant d'un fournisseur de PKI.**

  Ajoutez le certificat généré par le fournisseur suite à votre demande et ajoutez l'AC.

```
# 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
```

  Pour ajouter une liste de révocation de certificats (LRC) communiquée par un fournisseur de PKI, reportez-vous à la section "Traitement des listes de révocation de certificats" à la page 622.

▼ Traitement des listes de révocation de certificats

Les listes de révocation de certificats (LRC) sont émises par une AC et contiennent les certificats périmés ou compromis. Vous pouvez traiter les LRC de quatre façons :

- Vous devez faire en sorte que le protocole IKE ignore les listes de révocation de certificats si votre AC n'en émet pas. Pour plus d'informations, reportez-vous à l'Étape 6 de la section "Configuration du protocole IKE avec des certificats signés par une AC" à la page 612.
- Vous pouvez faire en sorte que le protocole IKE accède aux LRC à partir d'un URI (uniform resource indicator, identificateur universel de ressources) dont l'adresse est intégrée au certificat de clé publique de l'AC.
- Vous pouvez faire en sorte que le protocole IKE accède aux LRC à partir d'un serveur LDAP dont l'entrée de nom de répertoire (DN, directory name) est intégrée au certificat de clé publique de l'AC.
- Vous pouvez traiter les LRC comme des arguments de la commande `ikecert certrldb`. Voir l'Exemple 23–7.

La section ci-dessous décrit la procédure permettant de paramétrer l'utilisation des LRC à partir d'un point de distribution central dans le protocole IKE.

1 Affichez le certificat que vous avez reçu de l'AC.

```
# ikecert certdb -lv certspec
```

`-l`	Liste les certificats dans la base de données de certificats IKE.
`-v`	Liste les certificats en mode détaillé. Utilisez cette option avec précaution.

spécification de certificat Modèle permettant de rechercher les certificats correspondants dans la base de données de certificats IKE.

Par exemple, le certificat ci-dessous a été émis par Sun Microsystems (les détails ont été modifiés).

```
# ikecert certdb -lv example-protect.sun.com
Certificate Slot Name: 0   Type: dsa-sha1
   (Private key in certlocal slot 0)
 Subject Name: <O=Sun Microsystems Inc, CN=example-protect.sun.com>
 Issuer Name: <CN=Sun Microsystems Inc CA (Cl B), O=Sun Microsystems Inc>
 SerialNumber: 14000D93
   Validity:
      Not Valid Before: 2002 Jul 19th, 21:11:11 GMT
      Not Valid After:  2005 Jul 18th, 21:11:11 GMT
   Public Key Info:
      Public Modulus  (n) (2048 bits): C575A...A5
      Public Exponent (e) (  24 bits): 010001
   Extensions:
      Subject Alternative Names:
              DNS = example-protect.sun.com
      Key Usage: DigitalSignature KeyEncipherment
      [CRITICAL]
   CRL Distribution Points:
      Full Name:
         URI = #Ihttp://www.sun.com/pki/pkismica.crl#i
         DN = <CN=Sun Microsystems Inc CA (Cl B), O=Sun Microsystems Inc>
      CRL Issuer:
      Authority Key ID:
      Key ID:              4F ... 6B
      SubjectKeyID:        A5 ... FD
      Certificate Policies
      Authority Information Access
```

Notez l'entrée `CRL Distribution Points`. L'entrée URI indique que la LRC de cette organisation est disponible sur le Web. L'entrée DN indique que la LRC est disponible sur un serveur LDAP. Après que le protocole IKE a accédé à la LRC, celle-ci est mise en cache en vue de futures utilisations.

Pour accéder à la LRC, vous devez tout d'abord accéder à un point de distribution.

2 Choisissez l'une des méthodes suivantes pour accéder à la LRC depuis un point de distribution central.

- **Utilisez l'URI.**

  Ajoutez le mot-clé `use_http` au fichier `/etc/inet/ike/config` de l'hôte. Le fichier `ike/config` se présente comme suit :

  ```
  # Use CRL from organization's URI
  use_http
  ...
  ```

- **Utilisez un proxy Web.**

  Ajoutez le mot-clé `proxy` au fichier `ike/config`. Le mot-clé `proxy` adopte un URL comme argument, comme indiqué ci-dessous :

  ```
  # Use own web proxy
  proxy "http://proxy1:8080"
  ```

- **Utilisez un serveur LDAP.**

  Utilisez le nom du serveur LDAP comme argument du mot-clé `ldap-list` dans le fichier `/etc/inet/ike/config` de l'hôte. Le nom du serveur LDAP est fourni par votre organisation. L'entrée dans le fichier `ike/config` se présente comme suit :

  ```
  # Use CRL from organization's LDAP
  ldap-list "ldap1.sun.com:389,ldap2.sun.com"
  ...
  ```

Le protocole IKE récupère la LRC et la met en cache jusqu'à ce que le certificat expire.

Exemple 23–7 Ajout d'une LRC à la base de données `certrldb` locale

Si la LRC du fournisseur de PKI n'est pas disponible à partir d'un point de distribution central, vous pouvez ajouter cette liste manuellement à la base de données `certrldb` locale. Pour extraire la LRC dans un fichier, suivez les instructions du fournisseur de PKI, puis ajoutez la LRC à la base de données à l'aide de la commande `ikecert certrldb -a`.

```
# ikecert certrldb -a < Sun.Cert.CRL
```

Configuration du protocole IKE pour les systèmes portables (liste des tâches)

Le tableau ci-dessous décrit les procédures permettant de configurer le protocole IKE pour gérer des systèmes qui se connectent à distance à un site central.

Tâche	Description	Voir
Établissement de la communication avec un site central depuis un lieu hors site	Permettez aux systèmes hors site de communiquer avec un site central. Ces systèmes peuvent être portables.	"Configuration du protocole IKE pour les systèmes hors site" à la page 625
Utilisation d'un certificat racine et du protocole IKE sur un système central acceptant le trafic des systèmes portables	Configurez un système de passerelle pour accepter le trafic IPsec d'un système ne possédant pas d'adresse IP fixe.	Exemple 23–8

Tâche	Description	Voir
Utilisation d'un certificat racine et du protocole IKE sur un système ne possédant pas d'adresse IP fixe	Configurez le système portable de manière à protéger son trafic avec le site central (par exemple, le siège de l'entreprise).	Exemple 23–9
Utilisation de certificats autosignés et du protocole IKE sur un système central acceptant le trafic de systèmes portables	Configurez un système de passerelle avec des certificats autosignés pour accepter le trafic IPsec d'un système portable.	Exemple 23–10
Utilisation de certificats autosignés et du protocole IKE sur un système ne possédant pas d'adresse IP fixe	Configurez un système portable avec des certificats autosignés pour protéger son trafic avec un site central.	Exemple 23–11

Configuration du protocole IKE pour les systèmes portables

Lorsqu'ils sont configurés correctement, les ordinateurs portables peuvent communiquer avec les ordinateurs centraux de l'entreprise via IPsec et IKE. L'utilisation combinée d'une stratégie IPsec globale et d'une méthode d'authentification de clé publique permet de protéger le trafic des systèmes hors site avec le système central.

▼ Configuration du protocole IKE pour les systèmes hors site

Les protocoles IPsec et IKE requièrent un ID unique pour identifier la source et la destination. Pour les systèmes portables hors site ne possédant pas d'adresse IP unique, vous devez utiliser un autre type d'ID permettant d'identifier un système de manière unique (par exemple, `DNS`, `DN` ou `email`).

Il est toujours préférable de configurer les systèmes portables ou hors site possédant une adresse IP unique avec un autre type d'ID. Par exemple, si ces systèmes tentent de se connecter à un site central par l'intermédiaire d'un boîtier NAT, leur adresse unique n'est pas utilisée. Le boîtier NAT leur assigne une adresse IP arbitraire que le système central ne reconnaît pas.

Les clés prépartagées ne sont pas, elles non plus, un moyen d'authentification approprié pour les systèmes portables, car elles requièrent une adresse IP fixe. Les certificats autosignés ou les certificats PKI permettent par contre aux systèmes portables de communiquer avec le site central.

1 **Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

2 Configurez le système central de manière à ce qu'il reconnaisse les systèmes portables.

a. Paramétrez le fichier `/etc/hosts`.

Il n'est pas nécessaire que le système central reconnaisse des adresses spécifiques de systèmes portables.

```
# /etc/hosts on central
central 192.xxx.xxx.x
```

b. Paramétrez le fichier `ipsecinit.conf`.

Le système central nécessite une stratégie autorisant une plage étendue d'adresses IP. Les certificats de la stratégie IKE garantissent ultérieurement la légitimité des systèmes connectés.

```
# /etc/inet/ipsecinit.conf on central
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

c. Paramétrez le fichier `ike.config`.

Le DNS identifie le système central et les certificats permettent d'authentifier le système.

```
## /etc/inet/ike/ike.config on central
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server   "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root    "C=US, O=Domain Org, CN=Domain STATE"
#
# List self-signed certificates - trust server and enumerated others
#cert_trust    "DNS=central.domain.org"
#cert_trust    "DNS=mobile.domain.org"
#cert_trust    "DN=CN=Domain Org STATE (CLASS), O=Domain Org
#cert_trust    "email=root@central.domain.org"
#cert_trust    "email=user1@mobile.domain.org"
#

# Rule for mobile systems with certificate
{
```

```
  label "Mobile systems with certificate"
  local_id_type DNS

# Any mobile system who knows my DNS or IP can find me.

  local_id "central.domain.org"
  local_addr 192.xxx.xxx.x

# Root certificate ensures trust,
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

3 Connectez-vous à chacun des systèmes portables et configurez-les de manière à ce qu'ils trouvent le système central.

a. Paramétrez le fichier `/etc/hosts`.

Le fichier `/etc/hosts` n'a pas besoin d'une adresse pour le système portable, mais peut en fournir une. Il doit contenir une adresse IP publique pour le système central.

```
# /etc/hosts on mobile
mobile 10.x.x.xx
central 192.xxx.xxx.x
```

b. Paramétrez le fichier `ipsecinit.conf`.

Le système portable doit être capable de trouver le système central à partir de son adresse IP publique. Les deux systèmes doivent avoir la même stratégie IPsec.

```
# /etc/inet/ipsecinit.conf on mobile
# Find central
{raddr 192.xxx.xxx.x} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}
```

c. Paramétrez le fichier `ike.config`.

L'identificateur ne peut pas être une adresse IP. Pour les systèmes portables, les identificateurs valides sont les suivants :

- `DN=`*nom-répertoire-ldap*
- `DNS=`*adresse-DNS*
- `email=`*adresse-e-mail*

Les certificats permettent d'authentifier le système portable.

```
## /etc/inet/ike/ike.config on mobile
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
```

```
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server   "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root    "C=US, O=Domain Org, CN=Domain STATE"
#
# Self-signed certificates - trust me and enumerated others
#cert_trust    "DNS=mobile.domain.org"
#cert_trust    "DNS=central.domain.org"
#cert_trust    "DN=CN=Domain Org STATE (CLASS), O=Domain Org
#cert_trust    "email=user1@domain.org"
#cert_trust    "email=root@central.domain.org"
#
# Rule for off-site systems with root certificate
{
    label "Off-site mobile with certificate"
    local_id_type DNS

# NAT-T can translate local_addr into any public IP address
# central knows me by my DNS

    local_id "mobile.domain.org"
    local_addr 0.0.0.0/0

# Find central and trust the root certificate
    remote_id "central.domain.org"
    remote_addr 192.xxx.xxx.x

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

4 Lisez la configuration IKE dans le noyau.

- **À partir de la version Solaris 10 4/09, activez le service `ike`.**

  ```
  # svcadm enable svc:/network/ipsec/ike
  ```

- **Si vous exécutez une version antérieure à la version Solaris 10 4/09, réinitialisez le système.**

  ```
  # init 6
  ```

  Vous pouvez également arrêter et relancer le démon `in.iked`.

Exemple 23–8 Configuration d'un ordinateur central pour qu'il accepte le trafic IPsec d'un système portable

Le protocole IKE peut commencer les négociations derrière un boîtier NAT, mais il est préférable de ne pas faire intervenir de boîtier de ce type. Dans l'exemple ci-dessous, les certificats racine ont été émis par une AC. Ils ont été placés sur les deux systèmes (un système

portable et un système central). Le système central accepte les négociations IPsec émanant d'un système situé derrière un boîtier NAT. `main1` est le système acceptant les connexions de systèmes hors site. Pour paramétrer les systèmes hors site, reportez-vous à l'Exemple 23–9.

```
## /etc/hosts on main1
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server   "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
  label "Off-site system with root certificate"
  local_id_type DNS
  local_id "main1.domain.org"
  local_addr 192.168.0.100

# Root certificate ensures trust,
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha1}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha1}
}
```

Exemple 23–9 Configuration d'un système situé derrière un boîtier NAT avec IPsec

Dans l'exemple ci-dessous, les certificats racine ont été émis par une AC et placés sur le système portable et sur le système central. `mobile1` se connecte au siège de l'entreprise depuis un domicile privé. Le réseau du FAI (fournisseur d'accès Internet) utilise un boîtier NAT pour

pouvoir assigner une adresse privée à `mobile1`. Le boîtier NAT convertit l'adresse privée en une adresse IP publique partagée par d'autres nœuds du réseau du FAI. Le siège de l'entreprise ne se trouve pas derrière un boîtier NAT. Pour paramétrer l'ordinateur du siège de l'entreprise, reportez-vous à l'Exemple 23–8.

```
## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server   "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
  label "Off-site mobile1 with root certificate"
  local_id_type DNS
  local_id "mobile1.domain.org"
  local_addr 0.0.0.0/0

# Find main1 and trust the root certificate
  remote_id "main1.domain.org"
  remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

Exemple 23–10 Acceptation de certificats autosignés émanant d'un système portable

Dans l'exemple ci-dessous, les certificats autosignés ont été émis par le système portable et le système central, et ont été placés sur les deux systèmes. `main1` est le système acceptant les connexions de systèmes hors site. Pour paramétrer les systèmes hors site, reportez-vous à l'Exemple 23–11.

```
## /etc/hosts on main1
main1 192.168.0.100
```

```
## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Self-signed certificates - trust me and enumerated others
cert_trust    "DNS=main1.domain.org"
cert_trust    "jdoe@domain.org"
cert_trust    "user2@domain.org"
cert_trust    "user3@domain.org"
#
# Rule for off-site systems with trusted certificate
{
  label "Off-site systems with trusted certificates"
  local_id_type DNS
  local_id "main1.domain.org"
  local_addr 192.168.0.100

# Trust the self-signed certificates
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

Exemple 23–11 Utilisation de certificats autosignés pour contacter un système central

Dans l'exemple ci-dessous, `mobile1` se connecte au siège de l'entreprise depuis un domicile privé. Les certificats ont été émis par le système portable et le système central, et ont été placés sur les deux systèmes. Le réseau du FAI utilise un boîtier NAT pour assigner une adresse privée à `mobile1`. Le boîtier NAT convertit l'adresse privée en une adresse IP publique partagée par d'autres nœuds du réseau du FAI. Le siège de l'entreprise ne se trouve pas derrière un boîtier NAT. Pour paramétrer l'ordinateur du siège de l'entreprise, reportez-vous à l'Exemple 23–10.

```
## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha1 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters

# Self-signed certificates - trust me and the central system
cert_trust    "jdoe@domain.org"
cert_trust    "DNS=main1.domain.org"
```

```
#
# Rule for off-site systems with trusted certificate
{
  label "Off-site mobile1 with trusted certificate"
  local_id_type email
  local_id "jdoe@domain.org"
  local_addr 0.0.0.0/0

# Find main1 and trust the certificate
  remote_id "main1.domain.org"
  remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha1 }
}
```

Configuration du protocole IKE en vue de l'utilisation du matériel connecté (liste des tâches)

Le tableau ci-dessous répertorie les procédures permettant de signaler au protocole IKE la connexion des composants matériels. Pour que le protocole IKE puisse utiliser un composant matériel connecté, vous devez préalablement l'informer de l'existence de ce composant. Pour utiliser le composant matériel, suivez les procédures décrites à la section “Configuration du protocole IKE avec des certificats de clés publiques” à la page 606.

Remarque – Vous n'avez pas besoin de renseigner l'IKE sur le matériel sur puce. Par exemple, le processeur UltraSPARC® T2 offre l'accélération cryptographique. Vous n'avez pas besoin de configurer IKE pour qu'il recherche les accélérateurs sur puce.

Tâche	Description	Voir
Déchargement des opérations de clés IKE sur la carte Sun Crypto Accelerator 1000	Reliez le protocole IKE à la bibliothèque PKCS #11.	“Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 1000 ” à la page 633
Déchargement des opérations de clés IKE et stockage des clés sur la carte Sun Crypto Accelerator 4000	Reliez le protocole IKE et la bibliothèque PKCS #11, puis répertoriez le matériel connecté.	“Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 4000 ” à la page 634

Configuration du protocole IKE en vue de l'utilisation du matériel connecté

Les certificats des clés publiques peuvent également être stockés sur un matériel connecté. La carte Sun Crypto Accelerator 1000 est destinée uniquement au stockage. Les cartes Sun Crypto Accelerator 4000 et Sun Crypto Accelerator 6000 permettent le stockage, ainsi que le déchargement d'opérations de clés publiques du système vers la carte.

▼ Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 1000

Avant de commencer

La procédure ci-dessous suppose que la carte Sun Crypto Accelerator 1000 est connectée au système et que le ou les logiciels correspondants ont été installés et configurés. Pour obtenir des instructions, reportez-vous au *Sun Crypto Accelerator 1000 Board Version 2.0 Installation and User's Guide*.

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

---

2 Assurez-vous que la bibliothèque PKCS #11 est liée.

Entrez la commande suivante pour déterminer si la bibliothèque PKCS #11 est liée :

```
# ikeadm get stats
Phase 1 SA counts:
Current:   initiator:          0   responder:          0
Total:     initiator:          0   responder:          0
Attempted: initiator:          0   responder:          0
Failed:    initiator:          0   responder:          0
           initiator fails include 0 time-out(s)
PKCS#11 library linked in from /usr/lib/libpkcs11.so
#
```

3 **Solaris10 1/06 : à partir de cette version, vous pouvez stocker des clés dans le fichier keystore de clés softtoken.**

Pour plus d'informations sur le keystore fourni par la structure cryptographique de Solaris, reportez-vous à la page de manuel `cryptoadm`(1M). Pour plus d'informations sur l'utilisation du keystore, reportez-vous à l'Example 23–12.

▼ Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 4000

Avant de commencer

La procédure ci-dessous suppose que la carte Sun Crypto Accelerator 4000 est connectée au système et que le ou les logiciels correspondants ont été installés et configurés. Pour obtenir des instructions, reportez-vous au *Sun Crypto Accelerator 4000 Board Version 1.1 Installation and User's Guide*.

Si vous utilisez une carte Sun Crypto Accelerator 6000, reportez-vous au *Sun Crypto Accelerator 6000 Board Version 1.1 User's Guide*.

1 **Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

---

2 **Assurez-vous que la bibliothèque PKCS #11 est liée.**

IKE utilise les routines de la bibliothèque pour gérer la génération des clés et leur stockage sur la carte Sun Crypto Accelerator 4000. Entrez la commande suivante pour déterminer si une bibliothèque PKCS #11 a été liée :

```
$ ikeadm get stats
...
PKCS#11 library linked in from /usr/lib/libpkcs11.so
$
```

Remarque – Pour RSA, la carte Sun Crypto Accelerator 4000 prend en charge des clés d'une longueur maximum de 2 048 bits. Pour DSA, la longueur maximum des clés est de 1 024 bits.

---

3 Déterminez l'ID de jeton de la carte Sun Crypto Accelerator 4000.

```
$ ikecert tokens
Available tokens with library "/usr/lib/libpkcs11.so":

"Sun Metaslot                          "
```

La bibliothèque renvoie un ID de jeton, également appelé nom du keystore, de 32 caractères. Dans l'exemple ci-dessous, vous pouvez utiliser le jeton `Sun Metaslot` avec la commande `ikecert` pour stocker et accélérer les clés IKE.

Pour plus d'informations sur l'utilisation du jeton, reportez-vous à la section "Génération et stockage de certificats de clés publiques sur le matériel" à la page 618.

Les espaces situés à la fin sont automatiquement remplis par la commande `ikecert`.

Exemple 23–12 Découverte et utilisation de jetons metaslot

Les jetons peuvent être stockés sur un disque, sur une carte connectée ou dans le fichier keystore de clés softtoken fourni par la structure de chiffrement de Solaris. L'ID de jeton du keystore de softtoken peut se présenter comme suit :

```
$ ikecert tokens
Available tokens with library "/usr/lib/libpkcs11.so":

"Sun Metaslot                          "
```

Pour créer une phrase de passe pour un keystore de softtoken, reportez-vous à la page de manuel `pktool(1)`.

La commande ci-dessous permet d'ajouter un certificat au keystore de softtoken. `Sun.Metaslot.cert` est le fichier contenant le certificat AC.

```
# ikecert certdb -a -T "Sun Metaslot" < Sun.Metaslot.cert
Enter PIN for PKCS#11 token:      Type user:passphrase
```

Modification des paramètres de transmission du protocole IKE (liste des tâches)

Le tableau ci-dessous répertorie les procédures permettant de configurer les paramètres de transmission du protocole IKE.

Tâche	Description	Voir
Amélioration de l'efficacité de la négociation des clés	Modifiez les paramètres de négociation des clés.	"Modification de la durée de la phase 1 de la négociation des clés IKE" à la page 636

Tâche	Description	Voir
Configuration de la négociation des clés pour autoriser les délais de transmission	Allongez la durée de négociation des clés.	Exemple 23–13
Configuration de la négociation des clés pour qu'elle s'effectue rapidement ou pour que les échecs s'affichent rapidement	Réduisez la durée de négociation des clés.	Exemple 23–14

Modification des paramètres de transmission du protocole IKE

Lorsque le protocole IKE négocie les clés, la vitesse de transmission risque de compromettre la réussite de l'opération. En temps normal, il n'est pas nécessaire de modifier les valeurs par défaut des paramètres de transmission du protocole IKE. Dans certains cas (par exemple, optimisation de la négociation sur des lignes surchargées ou pour la reproduction d'un problème), vous pouvez toutefois juger utile de le faire.

Le fait de prolonger la durée de négociation permet à IKE de négocier les clés sur les lignes de transmission problématiques. Vous pouvez augmenter certains paramètres pour que la négociation réussisse dès la première tentative. Si elle échoue, vous pouvez espacer les tentatives suivantes pour optimiser les chances de succès.

Le fait de réduire la durée de négociation permet d'utiliser des lignes fiables. Vous pouvez relancer plus rapidement toute négociation ayant échoué. La réduction de la durée de négociation permet également d'accélérer le processus de reproduction d'un problème afin d'établir un diagnostic. Elle permet également d'utiliser les associations de sécurité (SA, security associations) de la phase 1 pendant toute leur durée de vie.

▼ Modification de la durée de la phase 1 de la négociation des clés IKE

1 Sur la console du système, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

Remarque – En vous connectant à distance, vous exposez le trafic de données confidentielles à des risques d'écoute électronique. Même si vous protégez la connexion à distance d'une manière ou d'une autre, la sécurité du système se limite à celle de la session à distance. Utilisez la commande `ssh` pour une connexion à distance sécurisée.

2 Modifiez la valeur par défaut des paramètres globaux de transmission sur chacun des systèmes.

Sur chacun des systèmes, modifiez les paramètres de durée de la phase 1 dans le fichier `/etc/inet/ike/config`.

```
### ike/config file on     system

## Global parameters
#
## Phase 1 transform defaults
#
#expire_timer      300
#retry_limit         5
#retry_timer_init    0.5 (integer or float)
#retry_timer_max    30   (integer or float)
```

`expire_timer` Délai de suppression d'une tentative de négociation IKE de phase 1 en attente (en secondes). Par défaut, la tentative reste active pendant 30 secondes.

`retry_limit` Nombre de retransmissions avant abandon de toute négociation IKE. Par défaut, IKE essaie cinq fois.

`retry_timer_init` Intervalle initial entre les retransmissions. Cet intervalle est doublé jusqu'à ce que la valeur `retry_timer_max` soit atteinte. L'intervalle initial est de 0,5 secondes.

`retry_timer_max` Intervalle maximum (en secondes) entre les retransmissions. L'intervalle de retransmission cesse d'augmenter lorsque cette limite est atteinte. Par défaut, cette limite est de 30 secondes.

3 Lisez la configuration modifiée dans le noyau.

- **À partir de la version Solaris 10 4/09, actualisez le service `ike`.**

  ```
  # svcadm refresh svc:/network/ipsec/ike
  ```

- **Si vous exécutez une version antérieure à la version Solaris 10 4/09, réinitialisez le système.**

  ```
  # init 6
  ```

  Vous pouvez également arrêter et relancer le démon `in.iked`.

Exemple 23–13 Augmentation de la durée de négociation de la phase 1 du protocole IKE

Dans l'exemple ci-dessous, un système est connecté à son homologue IKE via une ligne encombrée. Les paramètres d'origine figurent en commentaires dans le fichier. Les nouveaux paramètres augmentent la durée de négociation.

```
### ike/config file on partym
## Global Parameters
#
## Phase 1 transform defaults
#expire_timer   300
#retry_limit      5
#retry_timer_init 0.5 (integer or float)
#retry_timer_max 30   (integer or float)
#
expire_timer  600
retry_limit  10
retry_timer_init  2.5
retry_timer_max  180
```

Exemple 23–14 Réduction de la durée de négociation de la phase 1 du protocole IKE

Dans l'exemple ci-dessous, un système est connecté à son homologue IKE via une ligne à haut débit peu encombrée. Les paramètres d'origine figurent en commentaires dans le fichier. Les nouveaux paramètres diminuent la durée de négociation.

```
### ike/config file on partym
## Global Parameters
#
## Phase 1 transform defaults
#expire_timer   300
#retry_limit      5
#retry_timer_init 0.5 (integer or float)
#retry_timer_max 30   (integer or float)
#
expire_timer  120
retry_timer_init  0.20
```

◆ ◆ ◆ CHAPITRE 24

Protocole IKE (référence)

Ce chapitre aborde les sujets suivants :

Pour plus d'informations sur l'implémentation du protocole IKE, reportez-vous au Chapitre 23, “Configuration du protocole IKE (tâches)”. Pour obtenir une présentation du protocole, reportez-vous au Chapitre 22, “Protocole IKE (présentation)”.

Utilitaire de gestion du service IKE

Service `svc:/network/ipsec/ike:default` : l'utilitaire de gestion des services (SMF) fournit le service `ike` qui permet de gérer IKE. Par défaut, ce service est désactivé. Avant d'activer ce service, vous devez créer un fichier de configuration IKE, `/etc/inet/ike/config`.

Les propriétés suivantes du service `ike` sont configurables :

- **Propriété** `config_file` : emplacement du fichier de configuration IKE. La valeur initiale est `/etc/inet/ike/config`.
- **Propriété** `debug level` : niveau de débogage du démon `in.iked`. La valeur initiale est `op`, ce qui signifie opérationnelle. Pour connaître les valeurs possibles, reportez-vous au tableau sur les niveaux de débogage sous *Object Types* de la page de manuel `ikeadm`(1M).
- **Propriété** `admin_privilege` : niveau de privilège du démon `in.iked`. La valeur initiale est `base`. Les autres valeurs sont `modkeys` et `keymat`. Pour plus de détails, reportez-vous à la section “Commande d'administration du protocole IKE ” à la page 641.

Pour plus d'informations sur l'utilitaire SMF, reportez-vous au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base*. Voir aussi les pages de manuel `smf(5)`, `svcadm(1M)` et `svccfg(1M)`.

Démon IKE

Le démon `in.iked` automatise la gestion des clés cryptographiques pour IPsec sur les systèmes Solaris. Il négocie avec un système distant exécutant le même protocole pour fournir, de manière protégée, des numéros de clé authentifiés destinés aux associations de sécurité (SA). Le démon doit s'exécuter sur tous les systèmes qui sont censés communiquer en toute sécurité.

Par défaut, le service `svc:/network/ipsec/ike:default` n'est pas activé. Après que vous avez configuré le fichier `/etc/inet/ike/config` et activé le service `ike`, le démon `in.iked` se lance à l'initialisation du système.

Une fois le démon IKE en cours d'exécution, le système s'authentifie auprès de son entité IKE homologue lors de la phase 1. L'homologue, ainsi que les méthodes d'authentification, sont définis dans le fichier de stratégie IKE. Le démon crée alors les clés pour la phase 2. Les clés IKE sont actualisées automatiquement à un intervalle spécifié dans le fichier de stratégie. Le démon `in.iked` est à l'écoute des demandes IKE entrantes émanant du réseau et des demandes de trafic hors bande via le socket `PF_KEY`. Pour plus d'informations, reportez-vous à la page de manuel `pf_key(7P)`.

Le démon IKE est pris en charge par deux commandes. La commande `ikeadm` peut être utilisée pour afficher et modifier temporairement la stratégie IKE. Pour modifier de manière définitive la stratégie IKE, vous devez modifier les propriétés du service `ike`. Pour connaître la procédure, reportez-vous à la section "Affichage des clés IKE prépartagées" à la page 600.

et la commande `ikecert` d'afficher et de gérer les bases de données de clés publiques. Cette dernière gère les bases de données `ike.privatekeys` et `publickeys` locales, ainsi que les opérations de clés publiques et le stockage de ces clés sur du matériel.

Fichier de stratégie IKE

Le fichier de configuration de la stratégie IKE, `/etc/inet/ike/config`, gère les clés des interfaces protégées dans le fichier de stratégie IPsec, `/etc/inet/ipsecinit.conf`. Le fichier de stratégie IKE gère les clés pour IKE et pour les SA IPsec. Le démon IKE requiert lui-même des numéros de clé lors de la phase 1.

La gestion des clés avec IKE inclut des règles et des paramètres globaux. Les règles IKE identifient les systèmes ou réseaux sécurisés par les numéros de clé. Elles spécifient également la méthode d'authentification. Les paramètres globaux incluent des éléments tels que le chemin vers un accélérateur matériel connecté. Pour consulter des exemples de fichiers de stratégie IKE,

reportez-vous à la section "Configuration du protocole IKE avec des clés prépartagées (liste des tâches)" à la page 594. Pour des exemples et une description des entrées de stratégies IKE, consultez la page de manuel `ike.config(4)`.

Les SA IPsec prises en charge par IKE protègent les datagrammes IP conformément aux stratégies paramétrées dans le fichier de configuration des stratégies IPsec, `/etc/inet/ipsecinit.conf`. Le fichier de stratégie IKE détermine si la confidentialité de transmission parfaite (PFS, perfect forward security) est utilisée lors de la création des SA IPsec.

Le fichier `ike/config` peut inclure le chemin vers une bibliothèque implémentée conformément au standard RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki). IKE utilise la bibliothèque PKCS #11 pour accéder au matériel d'accélération et de stockage des clés.

En matière de sécurité, les considérations concernant le fichier `ike/config` sont similaires à celles concernant le fichier `ipsecinit.conf`. Pour plus d'informations, reportez-vous à la section "Considérations de sécurité à propos de `ipsecinit.conf` et `ipsecconf`" à la page 578.

Commande d'administration du protocole IKE

La commande `ikeadm` permet d'effectuer les opérations suivantes :

- afficher les différents aspects du processus du démon IKE ;
- modifier les paramètres qui sont transmis au démon IKE ;
- afficher les statistiques concernant la création de SA pendant la phase 1 ;
- déboguer les processus IKE ;
- afficher les différents aspects de l'état d'IKE ;
- modifier les propriétés du démon IKE ;
- afficher les statistiques concernant la création de SA pendant la phase 1 ;
- déboguer les échanges du protocole IKE.

Pour consulter des exemples et une description complète des options de cette commande, reportez-vous à la page de manuel `ikeadm(1M)`

Le niveau de privilège du démon IKE en cours d'exécution détermine les aspects du démon IKE susceptibles d'être affichés et modifiés. Trois niveaux de privilège sont possibles.

Niveau `base`	Vous ne pouvez ni afficher ni modifier les numéros de clé. Le niveau `base` est le niveau de privilège par défaut.
Niveau `modkeys`	À ce niveau, vous pouvez supprimer, modifier et ajouter des clés prépartagées.
Niveau `keymat`	Ce niveau vous permet d'afficher les numéros de clé actuels à l'aide de la commande `ikeadm`.

Pour modifier temporairement un privilège, vous pouvez utiliser la commande `ikeadm`. Pour une modification permanente, modifiez la propriété `admin_privilege` du service `ike`. Pour connaître la procédure, reportez-vous à la section "Procédure de gestion des services IKE et IPsec" à la page 536.

En matière de sécurité, les considérations concernant la commande `ikeadm` sont similaires à celles concernant la commande `ipseckey`. Pour plus d'informations, reportez-vous à la section "Considérations de sécurité pour la commande `ipseckey`" à la page 580.

Fichiers de clés prépartagées IKE

Lorsque vous créez des clés manuellement, elles sont stockées dans des fichiers du répertoire `/etc/inet/secret`. Le fichier `ike.preshared` contient les clés prépartagées des SA ISAKMP (Internet Security Association and Key Management Protocol) et le fichier `ipseckeys` contient les clés prépartagées des SA IPsec. Ces fichiers sont protégés en mode `0600` et le répertoire `secret` en mode `0700`.

- Lorsque vous configurez le fichier `ike/config` pour demander des clés prépartagées, vous créez un fichier `ike.preshared`. Vous entrez les numéros de clé des SA ISAKMP, c'est-à-dire de l'authentification IKE, dans le fichier `ike.preshared`. Les clés prépartagées étant utilisées pour authentifier la phase 1, le fichier doit être valide avant le démarrage du démon `in.iked`.
- Le fichier `ipseckeys` contient les numéros de clé des SA IPsec. Pour consulter des exemples de gestion manuelle de ce fichier, reportez-vous à la section "Création manuelle d'associations de sécurité IPsec" à la page 528. Le démon IKE n'utilise pas ce fichier. Les numéros de clé générés par IKE pour les SA IPsec sont stockés dans le noyau.

Remarque – Les clés prépartagées ne peuvent être stockées sur des composants matériels. Elles sont générées et stockées sur le système.

Commandes et bases de données de clés publiques IKE

La commande `ikecert` permet de manipuler les bases de données de clés publiques du système local. Utilisez-la lorsque le fichier `ike/config` requiert des certificats de clés publiques. Ces bases de données étant utilisées par IKE pour authentifier la phase 1 de l'échange, elles doivent être alimentées avant l'activation du démon `in.iked`. Trois sous-commandes permettent de gérer chacune des trois bases de données : `certlocal`, `certdb` et `certrldb`.

La commande `ikecert` permet aussi de gérer le stockage des clés. Elles peuvent être stockées sur disque, sur une carte Sun Crypto Accelerator 6000 ou &sca 4; connectée, ou dans un fichier keystore de clés softtoken. Ce fichier est disponible lorsque le metaslot de la structure

cryptographique de Solaris est utilisé pour communiquer avec le matériel. La commande `ikecert` utilise la bibliothèque PKCS #11 pour localiser le lieu de stockage des clés.

- **Solaris 10 1/06** : à partir de cette version, il est inutile de spécifier la bibliothèque. Par défaut, la bibliothèque PKCS #11 est `/usr/lib/libpkcs11.so`.
- **Solaris 10** : dans cette version, il est nécessaire de spécifier l'entrée de PKCS #11. pour que l'option `-T` de la commande `ikecert` fonctionne. Cette entrée se présente de la manière suivante :

  ```
  pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
  ```

Pour plus d'informations, consultez la page de manuel `ikecert`(1M) Pour plus d'informations sur le metaslot et sur le fichier keystore de clés softtoken, reportez-vous à la page de manuel `cryptoadm`(1M).

Commande `ikecert tokens`

L'argument `tokens` répertorie les ID de jetons disponibles. Les ID de jetons permettent aux commandes `ikecert certlocal` et `ikecert certdb` de générer des certificats de clés publiques et des demandes de certificats. Ces certificats et demandes de certificats peuvent également être stockés par la structure cryptographique dans le fichier keystore de clés softtoken ou sur une carte Sun Crypto Accelerator 6000 ou &sca 4; connectée. La commande `ikecert` utilise la bibliothèque PKCS #11 pour déterminer l'emplacement de stockage des certificats.

Commande `ikecert certlocal`

La sous-commande `certlocal` gère la base de données des clés privées. Les options de cette sous-commande permettent d'ajouter, d'afficher et de supprimer des clés privées. Cette sous-commande permet également de créer un certificat autosigné ou une demande de certificat. L'option `-ks` crée un certificat autosigné et l'option `-kc` une demande de certificat. Les clés sont stockées sur le système, dans le répertoire `/etc/inet/secret/ike.privatekeys`, ou sur un composant matériel connecté (option `-T`).

Lorsque vous créez une clé privée, les options de la commande `ikecert certlocal` doivent avoir des entrées connexes dans le fichier `ike/config`. Le tableau ci-dessous détaille les correspondances entre les options `ikecert` et les entrées `ike/config`.

TABLEAU 24–1 Correspondances entre les options `ikecert` et les entrées `ike/config`

Option `ikecert`	Entrée`ike/config`	Description
`-A` *nom-alternatif-sujet*	`cert_trust` *nom-alternatif-sujet*	Pseudonyme identifiant le certificat de manière unique. Il peut s'agir d'une adresse IP, d'une adresse e-mail ou d'un nom de domaine.
`-D`, *nom-distinctif-X.509*	*nom-distinctif-X.509*	Nom complet de l'autorité de certification, incluant le pays (C), le nom de l'organisation (ON), l'unité d'organisation (OU) et le nom commun (CN).
`-t dsa-sha1`	`auth_method dss_sig`	Méthode d'authentification légèrement plus lente que RSA.
`-t rsa-md5` et `-t rsa-sha1`	`auth_method rsa_sig`	Méthode d'authentification légèrement plus rapide que la méthode DSA. La clé publique RSA doit être suffisamment importante pour chiffrer la charge utile la plus lourde. Les charges les plus lourdes sont habituellement les données d'identité (par exemple, le nom distinctif X.509).
`-t rsa-md5` et `-t rsa-sha1`	`auth_method rsa_encrypt`	Le chiffrement RSA met les identités d'IKE à l'abri des écoutes électroniques, mais implique que les homologues IKE connaissent leurs clés publiques respectives.
`-T`	`pkcs11_path`	La bibliothèque PKCS #11 prend en charge l'accélération des clés sur les cartes Sun Crypto Accelerator 1000, Sun Accelerator 6000 et Sun Crypto Accelerator 4000. La bibliothèque fournit également les jetons qui gèrent le stockage des clés sur les cartes Sun Crypto Accelerator 6000 et Sun Crypto Accelerator 4000.

Lorsque vous émettez une demande de certificat à l'aide de la commande `ikecert certlocal -kc`, vous envoyez la sortie de cette commande à un fournisseur de PKI ou à une AC. Si votre entreprise possède sa propre PKI, vous envoyez cette sortie à votre administrateur de PKI. Le fournisseur de PKI, l'AC ou votre administrateur de PKI crée alors les certificats. Ceux qui vous sont transmis par le fournisseur de PKI ou l'AC sont entrés dans la sous-commande `certdb.` La liste de révocation de certificats (LRC) que le fournisseur de PKI vous envoie est entrée dans la sous-commande `certrldb`.

Commande `ikecert certdb`

La sous-commande `certdb` gère la base de données des clés publiques. Les options de cette sous-commande vous permettent d'ajouter, d'afficher et de supprimer des certificats et des clés publiques. Cette sous-commande accepte l'entrée de certificats générés par la commande `ikecert certlocal -ks` sur un système distant. Pour plus d'informations sur cette procédure, reportez-vous à la section “Configuration du protocole IKE avec des certificats de clés publiques

autosignés" à la page 607. Cette commande accepte également l'entrée de certificats émanant de fournisseurs PKI ou d'AC. Pour plus d'informations sur cette procédure, reportez-vous à la section "Configuration du protocole IKE avec des certificats signés par une AC" à la page 612.

Les certificats et les clés publiques sont stockés sur le système, dans le répertoire `/etc/inet/ike/publickeys` . L'option `-T` permet de stocker les certificats, les clés privées et les clés publiques sur les composants matériels connectés.

Commande `ikecert certdb`

La sous-commande `certrldb` gère la base de données des listes de révocation de certificats (LRC), `/etc/inet/ike/crls`. Cette base de données met à jour les listes de révocation des clés publiques. Les certificats qui ne sont plus valides figurent dans ces listes. Lorsqu'un fournisseur de PKI vous fait parvenir une LRC, vous pouvez l'installer dans cette base de données à l'aide de la commande `ikecert certrldb`. Pour plus d'informations sur cette procédure, reportez-vous à la section "Traitement des listes de révocation de certificats" à la page 622.

Répertoire `/etc/inet/ike/publickeys`

Le répertoire `/etc/inet/ike/publickeys` contient la partie publique des biclés et leur certificat, qui sont stockés dans des fichiers ou à des *emplacements*. Ce répertoire est protégé en mode `0755` et peut être alimenté à l'aide de la commande `ikecert certdb`. L'option `-T` permet de stocker les clés sur une carte Sun Crypto Accelerator 6000 ou &sca 4; plutôt que dans le répertoire `publickeys`.

Les emplacements contiennent, sous forme chiffrée, le nom distinctif X.509 des certificats qui ont été générés sur un autre système. Si vous utilisez des certificats autosignés, vous devez indiquer le certificat que l'administrateur du système distant vous a envoyé comme entrée de commande. Si vous utilisez des certificats d'une AC, vous installez deux certificats signés d'une AC dans la base de données. Vous installez un certificat basé sur la requête de signature de certificat envoyée à l'AC. Vous installez également un certificat de l'AC.

Répertoire `/etc/inet/secret/ike.privatekeys`

Le répertoire `/etc/inet/secret/ike.privatekeys` contient des fichiers de clés privées qui font partie de biclés, c'est-à-dire les numéros de clé des SA ISAKMP. Ce répertoire est protégé en mode `0700`. La commande `ikecert certlocal` permet d'alimenter le répertoire `ike.privatekeys`. Les clés privées sont effectives uniquement lors de l'installation de leur clé publique homologue, de certificats autosignés ou de certificats AC. Les clés publiques homologues sont stockées dans le répertoire `/etc/inet/ike/publickey s` ou sur une carte Sun Crypto Accelerator 6000 ou &sca 4;.

Répertoire `/etc/inet/ike/crls`

Le répertoire `/etc/inet/ike/crls` contient les fichiers des listes de révocation de certificats (LRC). Chaque fichier correspond à un fichier de certificat public du répertoire `/etc/inet/ike/publickeys`. Les fournisseurs de PKI fournissent les LRC correspondant à leurs certificats. La commande `ikecert certrldb` permet d'alimenter la base de données.

◆ ◆ ◆ CHAPITRE 25

IP Filter dans Oracle Solaris (présentation)

Ce chapitre fournit une présentation d'IP Filter, une fonction d'Oracle Solaris. Les tâches IP Filter sont décrites au Chapitre 26, “IP Filter (tâches)”.

Le présent chapitre contient les informations suivantes :

Nouvelles fonctions d'IP Filter

Cette section décrit les nouvelles fonctions d'IP Filter.

Vous trouverez une liste complète des nouvelles fonctionnalités et la description des différentes versions d'Oracle Solaris dans le guide *Nouveautés apportées à Oracle Solaris 10 8/11*.

Crochets de filtre de paquets

À partir de la version Solaris 10 7/07:, les crochets de filtre de paquets sont désormais utilisés pour filtrer les paquets dans Oracle Solaris. Cette fonctionnalité offre les avantages suivants pour l'administration du système :

- Les crochets de filtre de paquets simplifient la configuration d'IP Filter.

- Le filtrage de paquets entre les zones est à présent pris en charge.
- Les crochets de filtre améliorent les performances d'IP Filter.

Pour de plus amples informations sur ces crochets, reportez-vous à la section “Crochets de filtre de paquets” à la page 659. Pour obtenir la description des tâches associées aux crochets de filtre de paquets, reportez-vous au Chapitre 26, “IP Filter (tâches)”.

Filtrage de paquets IPv6 pour IP Filter

SE Solaris 6/06 : pour les administrateurs système dont une partie de l'infrastructure réseau est configurée avec IPv6, le filtrage de paquets IPv6 est dorénavant inclus à IP Filter. Ce filtrage peut se baser sur l'adresse IPv6 source/de destination, sur les pools contenant des adresses IPv6 et sur les en-têtes d'extension IPv6.

L'option `-6` a été ajoutée aux commandes `ipf` et `ipfstat` pour les utiliser avec IPv6. L'interface de ligne de commande ne change pas pour les commandes `ipmon` et `ippool`, mais celles-ci prennent également en charge IPv6. La commande `ipmon` a été améliorée afin de permettre la journalisation des paquets IPv6 et la commande `ippool` prend désormais en charge l'inclusion des adresses IPv6 dans les pools.

Pour de plus amples informations, reportez-vous à IPv6 pour IP Filter. Pour obtenir la description des tâches associées au filtrage de paquets IPv6, reportez-vous au Chapitre 26, “IP Filter (tâches)”.

En outre, IPv6 est pris en charge dans la fonction NAT de l'IP Filter. Pour de plus amples informations sur NAT, reportez-vous à la section “Utilisation de la fonctionnalité NAT d'IP Filter” à la page 656.

Introduction à IP Filter

La fonction IP Filter d'Oracle Solaris remplace le pare-feu SunScreen dans le système d'exploitation. Tout comme le pare-feu SunScreen, IP Filter assure un filtrage de paquets avec état, ainsi que la translation d'adresse réseau (NAT, Network Address Translation). IP Filter permet également le filtrage de paquets sans état, ainsi que la création et la gestion des pools d'adresses.

Le filtrage de paquets assure une protection de base contre les attaques potentielles via le réseau. IP Filter peut filtrer les paquets par adresse IP, port, protocole, interface réseau et direction du trafic. IP Filter peut également filtrer en fonction d'une adresse IP source individuelle, d'une adresse IP de destination, d'une plage d'adresses IP ou par pools d'adresses.

IP Filter est dérivé du logiciel Open Source IPFilter. Les modalités de la licence, l'attribution et le copyright du logiciel Open Source IPFilter se trouvent par défaut à l'emplacement

suivant :`/usr/lib/ipf/IPFILTER.LICENCE`. Si vous avez installé Oracle Solaris dans un autre emplacement que celui par défaut, modifiez le chemin afin d'accéder au fichier se trouvant à l'emplacement de l'installation.

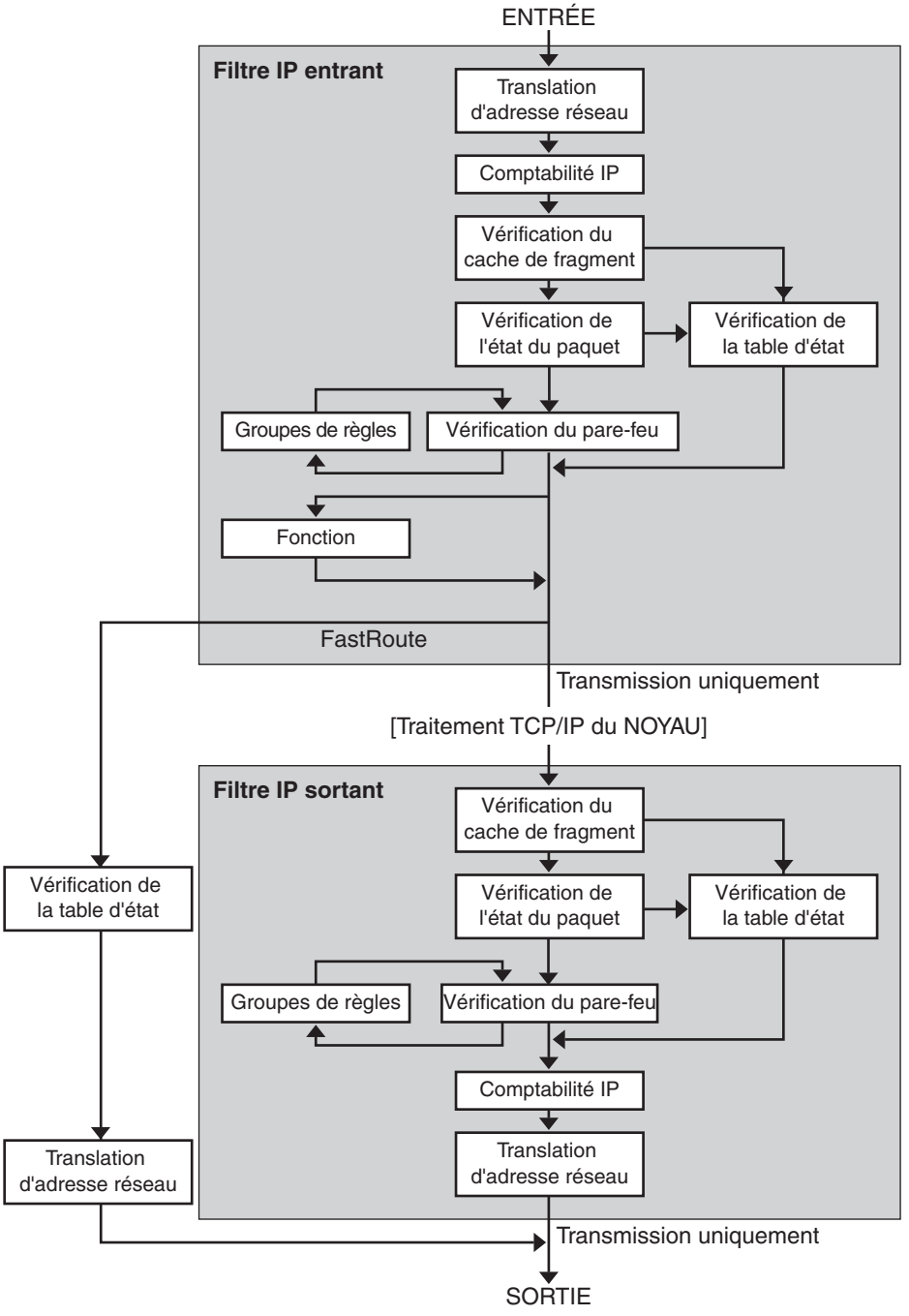
Sources d'informations relatives au logiciel Open Source IPFilter

La page d'accueil du logiciel Open Source IPFilter de Darren Reed se trouve à l'adresse `http://coombs.anu.edu.au/~avalon/ip-filter.html`. Ce site Web fournit des informations relatives au logiciel Open Source IPFilter, notamment un lien vers le didacticiel "IP Filter Based Firewalls HOWTO" (Brendan Conoboy et Erik Fichtner, 2002). Vous trouverez dans ce didacticiel les instructions de construction de pare-feux dans un environnement BSD UNIX, expliquées pas à pas. Bien qu'il soit destiné à un environnement BSD UNIX, ce didacticiel est également applicable à la configuration de la fonction IP Filter d'Oracle Solaris.

Traitement des paquets avec IP Filter

Au cours du traitement d'un paquet, IP Filter exécute une séquence d'étapes. Le diagramme ci-dessous illustre les étapes du traitement d'un paquet et l'intégration du filtrage à la pile de protocole TCP/IP.

FIGURE 25–1 Séquence de traitement d'un paquet



Le traitement d'un paquet inclut les opérations suivantes :

- **Translation d'adresse réseau (NAT)**

  Translation d'une adresse IP privée vers une adresse publique, ou définition d'alias pour plusieurs adresses privées vers une adresse publique unique. NAT (Network Address Translation, translation d'adresse réseau) permet à une organisation de résoudre le problème d'épuisement des adresses IP lorsqu'elle utilise un réseau et requiert l'accès à Internet.

- **Comptabilité IP**

  Les règles d'entrée et de sortie peuvent être configurées séparément, avec enregistrement du nombre d'octets transmis. En cas de correspondance d'une règle, le nombre d'octets du paquet est ajouté à la règle et des statistiques en cascade sont rassemblées.

- **Vérification du cache de fragment**

  Si un paquet du trafic en cours constitue un fragment et que le paquet précédent a été autorisé, le fragment de paquet est également autorisé, sans consultation de la table d'état ni vérification de règle.

- **Vérification de l'état du paquet**

  Si la règle contient l'instruction `keep state`, tous les paquets d'une session spécifiée sont automatiquement transmis ou bloqués, selon la spécification de la règle : `pass` (transmettre) ou `block` (bloquer).

- **Vérification du pare-feu**

  Les règles d'entrée et de sortie peuvent être configurées séparément, afin d'autoriser ou non la transmission d'un paquet, via IP Filter, vers les routines TCP/IP du noyau ou vers le réseau.

- **Groupes**

  Les groupes permettent d'écrire des ensembles de règles selon une structure arborescente.

- **Fonction**

  Une fonction correspond à l'action à réaliser. Les fonctions sont, par exemple, `block` (bloquer), `pass` (transmettre), `literal` (littéral) et `send ICMP response` (envoyer une réponse ICMP).

- **FastRoute**

  FastRoute indique à IP Filter de ne pas transmettre le paquet vers la pile UNIX IP pour le routage, ce qui entraîne une réduction TTL.

- **Authentification IP**

  Les paquets authentifiés ne sont transmis via les boucles du pare-feu qu'une seule fois, afin d'éviter le traitement multiple de certains paquets.

Recommandations relatives à l'utilisation d'IP Filter

- IP Filter est géré par les services SMF svc:/network/pfil et svc:/network/ipfilter. Pour une présentation complète de l'utilitaire SMF, reportez-vous au Chapitre 18, “Gestion des services (présentation) ” du *Guide d'administration système : administration de base*. Pour une présentation pas à pas des procédures associées à SMF, reportez-vous au Chapitre 19, “Gestion des services (tâches) ” du *Guide d'administration système : administration de base*.
- IP Filter requiert la modification directe des fichiers de configuration.
- IP Filter est installé en tant que composant d'Oracle Solaris. Par défaut, IP Filter n'est pas activé lorsque vous venez de procéder à l'installation. Pour configurer le filtrage, vous devez modifier les fichiers de configuration et activer manuellement IP Filter. Pour activer le filtrage, réinitialisez le système ou montez les interfaces à l'aide de la commande `ifconfig`. Pour de plus amples informations, reportez-vous à la page de manuel `ifconfig(1M)` Pour obtenir la description des tâches associées à l'activation d'IP Filter, reportez-vous à la section “Configuration d'IP Filter” à la page 663.
- Pour gérer IP Filter, connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter. Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “Configuring RBAC (Task Map)” du *System Administration Guide: Security Services*.
- IPMP (IP Network Multipathing, multiacheminement sur réseau IP) ne prend en charge que le filtrage sans état.
- Les configurations Sun Cluster ne prennent pas en charge le filtrage à l'aide d'IP Filter.
- Actuellement, le filtrage entre les zones n'est pas pris en charge par IP Filter.

Utilisation des fichiers de configuration IP Filter

IP Filter peut assurer des services de pare-feu ou de translation d'adresse réseau (NAT, Network Address Translation). Vous pouvez implémenter IP Filter à l'aide de fichiers de configuration chargeables. IP Filter contient un répertoire appelé `/etc/ipf`. Vous pouvez créer et enregistrer les fichiers de configuration `ipf.conf`, `ipnat.conf` et `ippool.conf` dans le répertoire `/etc/ipf`. Si ces fichiers existent dans le répertoire `/etc/ipf`, ils sont automatiquement chargés à l'initialisation. Il est également possible d'enregistrer les fichiers de configuration à un autre emplacement, puis de les charger manuellement. Pour obtenir des exemple de fichiers de configuration, reportez-vous à la section “Création et modification des fichiers de configuration IP Filter” à la page 695.

Utilisation des ensembles de règles IP Filter

Pour gérer le pare-feu, vous devez spécifier des ensembles de règles à l'aide d'IP Filter, puis filtrer le trafic réseau en fonction de ces ensembles de règles. Les types d'ensembles de règles suivants sont disponibles :

- ensembles de règles de filtrage de paquets ;
- ensembles de règles NAT (Network Address Translation, translation d'adresse réseau).

Par ailleurs, il est possible de créer des pools d'adresses pour référencer des groupes d'adresses IP. Ensuite, ces pools peuvent être utilisés dans un ensemble de règles. Les pools d'adresses permettent d'accélérer le traitement des règles. En outre, ils facilitent la gestion des grands groupes d'adresses.

Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter

Vous pouvez configurer le filtrage de paquets à l'aide des ensembles de règles de filtrage de paquets. La commande `ipf` permet d'utiliser les ensembles de règles de filtrage de paquets. Pour plus d'informations sur la commande `ipf`, reportez-vous à la page de manuel `ipf(1M)`.

Vous pouvez créer des règles de filtrage de paquets via la ligne de commande, à l'aide de la commande `ipf` ou dans un fichier de configuration de filtrage de paquets. Si vous souhaitez charger les règles de filtrage de paquets à l'initialisation, créez le fichier de configuration `/etc/ipf/ipf.conf` pour y insérer les règles de filtrage de paquets. Dans le cas contraire, placez le fichier `ipf.conf` à un autre endroit, puis activez manuellement le filtrage de paquets à l'aide de la commande `ipf`.

Avec IP Filter, deux ensembles de règles de filtrage de paquets peuvent coexister : l'ensemble de règles actif et l'ensemble de règles inactif. Dans la plupart des cas, vous utiliserez l'ensemble de règles actif. Toutefois, la commande `ipf -I` permet d'appliquer une commande à la liste de règles inactives. La liste de règles inactives n'est pas employée par IP Filter, sauf si vous la sélectionnez. La liste de règles inactives constitue l'emplacement auquel vous pouvez enregistrer des règles sans affecter le filtrage de paquets actif.

IP Filter traite les règles de la liste de règles du début à la fin de la liste de règles configurée, puis transmet ou bloque le paquet. Un indicateur permet à IP Filter de déterminer si un paquet doit être transmis ou non. Il parcourt l'intégralité de l'ensemble de règles et détermine si le paquet doit être transmis ou bloqué, en fonction de la dernière règle correspondante.

Il existe deux exceptions à ce processus. D'une part, si le paquet correspondant à une règle contenant le mot-clé `quick`, Si une règle inclut le mot-clé `quick`, l'action associée à cette règle est exécutée et les règles suivantes sont ignorées. D'autre part, si le paquet correspond à une règle contenant le mot-clé `group`, seules les règles portant l'indicateur de ce group sont vérifiées.

Configuration des règles de filtrage de paquets

Appliquez la syntaxe suivante pour créer des règles de filtrage de paquets :

action `[in|out]` *option mot-clé, mot-clé...*

1. Chaque règle commence par une action. IP Filter applique l'action au paquet si celui-ci correspond à la règle. Les actions habituellement appliquées aux paquets sont répertoriées ci-dessous.

`block`	Empêche le paquet de traverser le filtre.
`pass`	Permet au paquet de traverser le filtre.
`log`	Consigne le paquet sans déterminer s'il est bloqué ou transmis. Exécutez la commande `ipmon` pour afficher le journal.
`count`	Inclut le paquet dans les statistiques du filtre. Exécutez la commande `ipfstat` pour afficher les statistiques.
`skip` *nombre*	Le filtre saute *nombre* règles de filtrage.
`auth`	Le paquet est authentifié par un programme utilisateur qui valide les informations qu'il contient. Le programme détermine si le paquet est transmis ou bloqué.

2. Le mot suivant est `in` ou `out`. Votre choix détermine si la règle de filtrage de paquets est appliquée à un paquet entrant (in) ou à un paquet sortant (out).
3. Ensuite, vous pouvez insérer toute une liste d'options. Si vous en utilisez plusieurs, elles doivent être dans l'ordre indiqué ci-dessous.

`log`	Consigne le paquet si la règle constitue la dernière règle correspondante. Exécutez la commande `ipmon` pour afficher le journal.
`quick`	Exécute la règle contenant l'option `quick` si un paquet lui correspond. Toute vérification de règle subséquente est interrompue.
`on` *nom-interface*	Applique la règle uniquement si le paquet entre ou sort via l'interface spécifiée.
`dup-to` *nom-interface*	Copie le paquet et envoie la copie sur *nom-interface* vers une adresse IP éventuellement spécifiée.
`to` *nom-interface*	Déplace le paquet vers une file d'attente sortante sur *nom-interface*.

4. Une fois les options spécifiées, vous avez le choix entre plusieurs mots-clés afin de déterminer si le paquet correspond à la règle. Les mots-clés doivent être utilisés dans l'ordre indiqué ci-dessous.

Remarque – Par défaut, le filtre autorise la transmission de tout paquet ne correspondant à aucune règle du fichier de configuration.

`tos`	Filtre les paquets en fonction de leur type de service, exprimé sous forme d'entier décimal ou hexadécimal.
`ttl`	Filtre les paquets en fonction de leur durée de vie. La durée de vie d'un paquet est une valeur enregistrée dans celui-ci qui indique la durée pendant laquelle le paquet peut se trouver sur le réseau avant d'être abandonné.
`proto`	Les paquets correspondant à la règle sont déterminés en fonction d'un protocole spécifique. Vous pouvez employer l'un des noms de protocole spécifiés dans le fichier `/etc/protocols` ou un nombre décimal représentant le protocole. Le mot-clé `tcp/udp` peut être utilisé pour filtrer les paquets TCP ou UDP.
`from/to/all/ any`	Filtre les paquets en fonction des éléments suivants : l'adresse IP source, l'adresse IP de destination et le numéro de port. Le mot-clé `all` permet d'accepter tous les paquets, quelles que soient leur source et leur destination.
`with`	Les paquets correspondant à la règle sont ceux qui sont associés à des attributs spécifiques. Insérez le mot `not` ou `no` devant le mot-clé pour indiquer qu'un paquet ne correspond à la règle qu'en l'absence de l'option.
`flags`	Employé pour TCP afin de filtrer les paquets en fonction des indicateurs TCP définis. Pour plus d'informations sur les indicateurs TCP, reportez-vous à la page de manuel `ipf(4)`.
`icmp-type`	Filtre les paquets en fonction du type d'ICMP. Ce mot-clé n'est employé que si l'option `proto` est définie sur `icmp` et que l'option `flags` n'est pas utilisée.
`keep` *options-keep*	Détermine les informations conservées pour le paquet. Les options `state` et `frags` sont disponibles comme *options-keep*. L'option `state` conserve les informations relatives à la session et peuvent être conservées sur les paquets TCP, UDP et ICMP. L'option `frags` permet de conserver les informations sur les fragments de paquets et d'appliquer les informations aux fragments suivants. Les *options-keep* permettent la transmission des paquets correspondant à la règle sans passer par la liste de contrôle d'accès.
`head` *numéro*	Crée un groupe pour les règles de filtrage, désigné par le numéro *numéro*.

`group` *numéro* Ajoute la règle au groupe de numéro *numéro* au lieu du groupe par défaut. Toutes les règles de filtrage sont placées dans le groupe 0 si aucun autre groupe n'est spécifié.

L'exemple suivant illustre la constitution d'une syntaxe de règle de filtrage de paquets pour créer une règle. Pour bloquer le trafic entrant à partir de l'adresse IP `192.168.0.0/16`, ajoutez la règle suivante à la liste de règles :

```
block in quick from 192.168.0.0/16 to any
```

Pour obtenir la syntaxe et la grammaire complètes utilisées pour écrire des règles de filtrage de paquets, reportez-vous à la page de manuel `ipf(4)` Pour une description des tâches associées au filtrage de paquets, reportez-vous à la section "Gérez les ensembles de règles de filtrage de paquets d'IP Filter" à la page 677. Pour une explication du schéma d'adresse IP (`192.168.0.0/16`) de l'exemple, reportez-vous au Chapitre 2, "Planification de votre réseau TCP/IP (tâches)".

Utilisation de la fonctionnalité NAT d'IP Filter

NAT configure des règles de mappage qui réalisent la translation des adresses IP source et de destination vers d'autres adresses Internet ou intranet. Ces règles modifient les adresses source et de destination des paquets IP entrants et sortants et envoient les paquets. Vous pouvez également utiliser NAT pour rediriger le trafic d'un port à un autre. NAT assure l'intégrité du paquet en cas de modification ou de redirection de celui-ci.

Exécutez la commande `ipnat` pour utiliser les listes de règles NAT. Pour plus d'informations sur la commande `ipnat`, reportez-vous à la page de manuel `ipnat(1M)`.

Vous pouvez créer des règles NAT à la ligne de commande, à l'aide de la commande `ipnat` ou dans un fichier de configuration NAT. Les règles de configuration NAT résident dans le fichier `ipnat.conf`. Si vous souhaitez charger les règles NAT à l'initialisation, créez le fichier `/etc/ipf/ipnat.conf` afin d'y insérer les règles NAT. Dans le cas contraire, placez le fichier `ipnat.conf` à un autre endroit, puis activez manuellement le filtrage de paquets à l'aide de la commande `ipnat`.

Les règles NAT peuvent s'appliquer à la fois aux adresses IPv4 et IPv6. Toutefois, vous ne pouvez pas spécifier les deux types d'adresses dans la même règle. Au contraire, vous devez définir des règles distinctes pour chaque type d'adresse. Dans une règle NAT qui inclut les adresses IPv6, vous ne pouvez pas utiliser les commandes NAT `mapproxy` et `rdrproxy` simultanément.

Configuration des règles NAT

Appliquez la syntaxe ci-dessous pour créer des règles NAT :

commande nom-interface paramètres

1. Toute règle commence par l'une des commandes ci-dessous :

   `map` Mappe une adresse IP ou un réseau IP vers une autre adresse IP ou un autre réseau IP selon un processus circulaire non contrôlé.

   `rdr` Redirige les paquets d'un couple port-adresse IP vers un autre couple port-adresse IP.

   `bimap` Établit une translation d'adresse réseau bidirectionnelle entre une adresse IP externe et une adresse IP interne.

   `map-block` Établit la translation basée sur les adresses IP statiques. Cette commande se base sur un algorithme qui force la translation des adresses vers une plage de destination.

2. Le mot suivant correspond au nom de l'interface, par exemple `hme0`.
3. Ensuite, vous avez le choix entre divers paramètres, afin de définir la configuration NAT. Les paramètres suivants sont disponibles :

   `ipmask` Désigne le masque réseau.

   `dstipmask` Désigne l'adresse cible de la translation de `ipmask`.

   `mapport` Désigne les protocoles `tcp`, `udp` ou `tcp/udp`, ainsi qu'une plage de numéros de port.

L'exemple suivant illustre la constitution d'une syntaxe de règle NAT pour créer une règle NAT. Pour réécrire un paquet sortant sur le périphérique `de0` avec l'adresse source `192.168.1.0/24` et pour afficher son adresse source comme étant `10.1.0.0/16`, ajoutez la règle ci-dessous à l'ensemble de règles NAT :

```
map de0 192.168.1.0/24 -> 10.1.0.0/16
```

Les règles suivantes s'appliquent aux adresses IPv6 :

```
map ppp0 fec0:1::/64 -> 2000:1:2::/72 portmap tcp/udp 1025:65000
map-block ppp0 fe80:0:0:209::/64 -> 209:1:2::/72 ports auto
rdr ce0 209::ffff:fe13:e43e port 80 -> fec0:1::e,fec0:1::f port 80 tcp round-robin
```

Pour obtenir la syntaxe et la grammaire complètes utilisées pour écrire des règles NAT, reportez-vous à la page de manuel `ipnat(4)`.

Utilisation de la fonctionnalité de pools d'adresses d'IP Filter

Les pools d'adresses constituent une référence unique pour nommer un groupe de paires adresse/masque de réseau. Les processus fournis pas les pools d'adresses permettent de trouver plus rapidement les adresses IP correspondant aux règles. En outre, ils facilitent la gestion des grands groupes d'adresses.

Les règles de configuration de pool d'adresses sont définies dans le fichier `ippool.conf`. Si vous souhaitez charger le fichier de règles de pool d'adresses à l'initialisation, créez le fichier `/etc/ipf/ippool.conf` afin d'y insérer les règles de pool. Dans le cas contraire, placez le fichier `ippool.conf` à un autre endroit, puis activez manuellement le filtrage de paquets à l'aide de la commande `ippool`.

Configuration des pools d'adresses

Pour créer un pool d'adresses, appliquez la syntaxe suivante :

`table role =` *role-name* `type =` *storage-format* `number =` *reference-number*

`table` Définit la référence des adresses.

`role` Spécifie le rôle du pool dans IP Filter. À ce stade, vous ne pouvez faire référence qu'au rôle `ipf`.

`type` Spécifie le format de stockage du pool.

`numéro` Spécifie le numéro de référence utilisé par la règle de filtrage.

Par exemple, pour faire référence aux groupes d'adresses `10.1.1.1` et `10.1.1.2` et au réseau `192.16.1.0` à l'aide du numéro de pool `13`, insérez la règle suivante dans le fichier de configuration de pool d'adresses :

```
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24 };
```

Ensuite, pour faire référence au numéro de pool `13` dans une règle de filtrage, élaborez une règle similaire à la suivante :

```
pass in from pool/13 to any
```

Vous devez charger le fichier de pool avant de charger les règles contenant une référence au pool. Dans le cas contraire, le pool n'est pas défini, comme indiqué dans la sortie suivante :

```
# ipfstat -io
empty list for ipfilter(out)
block in from pool/13(!) to any
```

Si vous ajoutez le pool par la suite, l'ensemble de règle du noyau n'est pas mis à jour. Vous devez également recharger le fichier de règles faisant référence au pool.

Pour obtenir la syntaxe et la grammaire complètes utilisées pour écrire des règles de filtrage de paquets, reportez-vous à la page de manuel ippool(4).

Crochets de filtre de paquets

À partir de la version Solaris 10 7/07, des crochets de filtre de paquets remplacent le module pfil pour activer IP Filter. Dans les versions précédentes, une étape supplémentaire dédiée à la configuration du module pfil était requise pour configurer Solaris IP Filter. Cette exigence de configuration supplémentaire augmentait les risques d'erreurs entraînant le dysfonctionnement d'IP Filter. L'insertion du module STREAMS pfil entre IP et le pilote de périphérique affectait également les performances. Enfin, le module pfil ne pouvait pas intercepter les paquets entre les zones.

Les crochets de filtre de paquets optimisent la procédure d'activation d'IP Filter. Grâce à ces crochets, IP Filter contrôle les flux de paquet entrants et sortants du système Oracle Solaris à l'aide de seuils de filtre de préroutage (entrants) et de postroutage (sortants).

Avec les crochets de filtre de paquets, le module pfil devient inutile. Par conséquent, les composants suivants associés au module sont également supprimés.

- pilote pfil ;
- démon pfil ;
- service SMF svc:/network/pfil.

Pour obtenir une description des tâches associées à l'activation d'IP Filter, reportez-vous au Chapitre 26, “IP Filter (tâches)”.

IP Filter et le module STREAMS pfil

Remarque – Le module pfil n'est utilisé avec IP Filter que dans les versions Solaris suivantes :

- Solaris 10 3/05 ;
- Solaris 10 1/06 ;
- Solaris 10 6/06 ;
- Solaris 10 11/06.

À partir de la version Solaris 10 7/07, le module pfil a été remplacé par les crochets de filtre de paquets et n'est plus utilisé avec IP Filter.

Le module STREAMS `pfil` est requis pour activer IP Filter. Toutefois, IP Filter ne fournit pas de mécanisme automatique pour empiler le module sur chaque interface. Au lieu de cela, le module STREAMS `pfil` est géré par le service SMF `svc:/network/pfil`. Pour activer le filtrage sur une interface réseau, vous devez tout d'abord configurer le fichier `pfil.ap`. Ensuite, activez le service `svc:/network/pfil` afin de fournir le module STREAMS `pfil` à l'interface réseau. Pour activer le module STREAMS, réinitialisez le système ou démontez chacune des interfaces réseau sur lesquelles vous souhaitez réaliser le filtrage, puis remontez-les. Pour activer les capacités de filtrage de paquets IPv6, vous devez monter la version `inet6` de l'interface.

Si aucun module `pfil` n'est trouvé pour les interfaces réseau, les services SMF sont placés en état de maintenance. Cette situation est souvent due à un fichier `/etc/ipf/pfil.ap` modifié incorrect. Si le service est placé en mode de maintenance, l'occurrence est consignée dans les fichiers journaux de filtrage.

Pour obtenir la description des tâches associées à l'activation d'IP Filter, reportez-vous à la section "Configuration d'IP Filter" à la page 663.

IPv6 pour filtre IP

À partir de la version 6/06, IPv6 est pris en charge avec Solaris IP Filter. Ce filtrage peut se baser sur l'adresse IPv6 source/de destination, sur les pools contenant des adresses IPv6 et sur les en-têtes d'extension IPv6.

De nombreux aspects d'IPv6 sont similaires à IPv4. Toutefois, les en-têtes et tailles des paquets ne sont pas identiques dans les deux versions d'IP, ce qui constitue une considération de poids pour IP Filter. Les paquets IPv6 appelés *jumbogrammes* contiennent un datagramme de longueur supérieure à 65 535 octets. IP Filter ne prend pas en charge les jumbogrammes IPv6. Pour en savoir plus sur les autres fonctionnalités IPv6, reportez-vous à la section "Fonctions principales d'IPv6" à la page 72.

Remarque – Pour plus d'informations sur les jumbogrammes, reportez-vous au document IPv6 Jumbograms, RFC 2675 de l'IETF (Internet Engineering Task Force, groupe d'étude d'ingénierie Internet). [`http://www.ietf.org/rfc/rfc2675.txt`]

Les tâches IP Filter associées à IPv6 ne sont pas très différentes d'IPv4. La différence la plus notable est l'emploi de l'option `-6` avec certaines commandes. Les commandes `ipf` et `ipfstat` incluent l'option `-6` à utiliser avec le filtrage de paquets IPv6. Appliquez l'option `-6` avec la commande `ipf` pour charger et vider les règles de filtrage de paquets IPv6. Pour afficher les statistiques IPv6, utilisez l'option `-6` avec la commande `ipfstat`. Les commandes `ipmon` et `ippool` prennent également en charge IPv6, même si aucune option n'est associée à la prise en charge d'IPv6. La commande `ipmon` a été optimisée pour autoriser la journalisation des paquets

IPv6. La commande `ippool` prend en charge les pools avec les adresses IPv6. Vous pouvez créer des pools d'adresses IPv4, des pools d'adresses IPv6 et des pools contenant à la fois des adresses IPv4 et IPv6.

Vous pouvez utiliser le fichier `ipf6.conf` pour créer des jeux de règles de filtrage de paquets pour IPv6. Par défaut, le fichier de configuration `ipf6.conf` figure dans le répertoire `/etc/ipf`. Comme pour les autres fichiers de configuration de filtrage, le fichier `ipf6.conf` se charge automatiquement au cours du processus d'initialisation s'il est stocké dans le répertoire `/etc/ipf` . Vous pouvez également créer un fichier de configuration IPv6, le conserver à un autre emplacement et le charger manuellement.

Une fois les règles de filtrage de paquets pour IPv6 configurées, activez les capacités de filtrage de paquets IPv6 en montant la version `inet6` de l'interface.

Pour plus d'informations sur IPv6, reportez-vous au Chapitre 3, “Présentation d'IPv6”. Pour obtenir une description des tâches associées à IP Filter, reportez-vous au Chapitre 26, “IP Filter (tâches)”.

Pages de manuel IP Filter

Le tableau ci-dessous répertorie les pages de manuel applicables à IP Filter.

Page de manuel	Description
`ipf`(1M)	Exécutez la commande `ipf` pour effectuer les tâches suivantes : ■ utiliser les ensembles de règles de filtrage de paquets ; ■ désactiver et activer le filtrage ; ■ réinitialiser les statistiques et resynchroniser la liste d'interface du noyau avec la liste de statut d'interface actuelle.
`ipf`(4)	Contient la grammaire et la syntaxe de création des règles de filtrage de paquets IP Filter.
`ipfilter`(5)	Fournit les informations d'octroi de licence du logiciel Open Source IP Filter.
`ipfs`(1M)	Exécutez la commande `ipfs` pour enregistrer et restaurer les informations NAT et les informations de table d'état lors des réinitialisations.
`ipfstat`(1M)	Exécutez la commande `ipfstat` pour récupérer et afficher les statistiques relatives au traitement des paquets.

Page de manuel	Description
ipmon(1M)	Exécutez la commande `ipmon` pour ouvrir le périphérique du journal et afficher les paquets consignés pour le filtrage de paquets et pour NAT.
ipnat(1M)	Exécutez la commande `ipnat` pour effectuer les tâches suivantes : ■ utiliser les règles NAT ; ■ récupérer et afficher les statistiques NAT.
ipnat(4)	Contient la grammaire et la syntaxe pour la création de règles NAT.
ippool(1M)	Exécutez la commande `ippool` pour créer et gérer les pools d'adresses.
ippool(4)	Contient la grammaire et la syntaxe de création des pools d'adresses IP Filter.
ndd(1M)	Affiche les paramètres de filtrage actuels du module STREAMS `pfil` et les valeurs courantes des paramètres réglables.

◆ ◆ ◆ CHAPITRE 26

IP Filter (tâches)

Ce chapitre fournit les instructions relatives à chaque étape des tâches. Pour obtenir des informations générales sur IP Filter, reportez-vous au Chapitre 25, “IP Filter dans Oracle Solaris (présentation) ”.

Le présent chapitre contient les informations suivantes :

Configuration d'IP Filter

La liste des tâches ci-dessous identifie les procédures associées à la configuration d'IP Filter.

TABLEAU 26–1 Configuration d'IP Filter (liste des tâches)

Tâche	Description	Voir
Activation initiale d'IP Filter	IP Filter n'est pas activé par défaut. Activez-le manuellement ou à l'aide des fichiers de configuration disponibles dans le répertoire `/etc/ipf/`, puis réinitialisez le système. À partir de la version Solaris 10 7/07, des crochets de filtre de paquets remplacent le module `pfil` pour activer IP Filter.	“Activation d'IP Filter” à la page 664

TABLEAU 26–1 Configuration d'IP Filter (liste des tâches) *(Suite)*

Tâche	Description	Voir
Réactivation d'IP Filter	Si IP Filter est désactivé, vous pouvez le réactiver soit en réinitialisant le système, soit en exécutant la commande `ipf`.	"Réactivation d'IP Filter" à la page 665
Activation du filtrage de loopback	Disponible en option, le filtrage de loopback permet, par exemple, de filtrer le trafic entre les zones.	"Activation du filtrage de loopback" à la page 666

▼ Activation d'IP Filter

Cette procédure permet d'activer IP Filter sur un système exécutant le SE Solaris 10 7/07 ou une version plus récente. Si le système exécute une version Oracle Solaris 10 antérieure à la version Solaris 10 7/07, reportez-vous à la section "Utilisation du module `pfil`" à la page 669 pour activer IP Filter.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Créez un ensemble de règles de filtrage de paquets.

L'ensemble de règles de filtrage de paquets contient les règles de filtrage de paquets utilisées par IP Filter. Pour charger les règles de filtrage de paquets à l'initialisation, modifiez le fichier `/etc/ipf/ipf.conf` afin d'implémenter le filtrage de paquets IPv4. Utilisez le fichier `/etc/ipf/ipf6.conf` pour les règles de filtrage de paquets IPv6. Si vous ne souhaitez pas charger les règles de filtrage de paquets à l'initialisation, insérez-les dans le fichier de votre choix, puis activez manuellement le filtrage de paquets. Pour plus d'informations sur le filtrage de paquets, reportez-vous à la section "Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter" à la page 653. Pour plus d'informations sur l'utilisation des fichiers de configuration, reportez-vous à la section "Création et modification des fichiers de configuration IP Filter" à la page 695.

3 (Facultatif) Créez un fichier de configuration NAT (Network Address Translation, translation d'adresse réseau).

Remarque – NAT ne prend pas en charge IPv6.

Créez le fichier `ipnat.conf` si vous souhaitez utiliser la translation d'adresse réseau. Si vous souhaitez charger les règles NAT à l'initialisation, créez le fichier `/etc/ipf/ipnat.conf` afin d'y

insérer les règles NAT. Si vous ne souhaitez pas charger les règles NAT à l'initialisation, placez le fichier `ipnat.conf` dans le répertoire de votre choix, puis activez manuellement les règles NAT.

Pour de plus amples informations sur NAT, reportez-vous à la section "Utilisation de la fonctionnalité NAT d'IP Filter" à la page 656.

4 **(Facultatif) Créez un fichier de configuration de pool d'adresses.**

Créez un fichier `ipool.conf` si vous souhaitez référencer un groupe d'adresses sous la forme d'un pool d'adresses unique. Pour charger le fichier de configuration de pool d'adresses à l'initialisation, créez le fichier `/etc/ipf/ippool.conf` afin d'y insérer le pool d'adresses. Si vous ne souhaitez pas charger le fichier de configuration de pool d'adresses à l'initialisation, placez le fichier `ippool.conf` dans le répertoire de votre choix, puis activez manuellement les règles.

Un pool d'adresses peut contenir exclusivement des adresses IPv4 ou exclusivement des adresses IPv6. Il peut également contenir à la fois des adresses IPv4 et des adresses IPv6.

Pour de plus amples informations sur les pools d'adresses, reportez-vous à la section "Utilisation de la fonctionnalité de pools d'adresses d'IP Filter" à la page 658.

5 **(Facultatif) Activez le filtrage de trafic en loopback.**

Pour filtrer le trafic entre les zones configurées sur le système, le cas échéant, activez le filtrage de loopback. Reportez-vous à la section "Activation du filtrage de loopback" à la page 666. Vous devez également définir les ensembles de règles adéquats applicables aux zones.

6 **Activez IP Filter.**

```
# svcadm enable network/ipfilter
```

▼ Réactivation d'IP Filter

Si le filtrage de paquets a été temporairement désactivé, vous pouvez le réactiver.

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Activez IP Filter et le filtrage selon l'une des méthodes ci-dessous :**

- Redémarrez l'ordinateur.

```
# reboot
```

Remarque – Lorsque IP Filter est activé, les fichiers suivants sont chargés après une réinitialisation s'ils sont présents : le fichier `/etc/ipf/ipf.conf`, le fichier `/etc/ipf/ipf6.conf` en cas d'utilisation d'IPv6 ou le fichier `/etc/ipf/ipnat.conf`.

- Exécutez les commandes suivantes pour activer IP Filter et le filtrage :
  a. Activez IP Filter.

     ```
     # ipf -E
     ```

  b. Activez le filtrage de paquets.

     ```
     # ipf -f filename
     ```

  c. (Facultatif) Activez NAT.

     ```
     # ipnat -f filename
     ```

     Remarque – NAT ne prend pas en charge IPv6.

▼ Activation du filtrage de loopback

Remarque – Vous pouvez filtrer le trafic de loopback uniquement si vous exécutez la version Solaris 10 7/07&; ou une version ultérieure. Dans les versions antérieures à Oracle Solaris 10, le filtrage de loopback n'était pas pris en charge.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Le cas échéant, arrêtez IP Filter.

```
# svcadm disable network/ipfilter
```

3 Ajoutez la ligne suivante au début du fichier `/etc/ipf.conf` ou `/etc/ipf6.conf` :

```
set intercept_loopback true;
```

Cette ligne doit précéder toutes les règles de filtre IP définies dans le fichier. Toutefois, vous pouvez insérer des commentaires avant la ligne, comme dans l'exemple ci-dessous :

```
#
# Enable loopback filtering to filter between zones
#
```

```
set intercept_loopback true;
#
# Define policy
#
block in all
block out all
<other rules>
...
```

4 **Lancez IP Filter.**

```
# svcadm enable network/ipfilter
```

5 **Pour vérifier le statut du filtrage de loopback, exécutez la commande ci-dessous :**

```
# ipf -T ipf_loopback
ipf_loopback    min 0   max 0x1 current 1
#
```

Si le filtrage de loopback est désactivé, la commande génère la sortie suivante :

```
ipf_loopback    min 0   max 0x1 current 0
```

Désactivation d'IP Filter

Vous pouvez désactiver le filtrage de paquets et NAT pour :

- Réaliser des tests
- Dépanner des problèmes système dont IP Filter semble être à l'origine

La liste des tâches ci-dessous identifie les procédures associées à la désactivation des fonctions IP Filter.

TABLEAU 26–2 Désactivation d'IP Filter (liste des tâches)

Tâche	Description	Voir
Désactivation du filtrage de paquets.	Désactivez le filtrage de paquets à l'aide de la commande `ipf`.	"Désactivation du filtrage de paquets" à la page 667
Désactivation de NAT.	Désactivez NAT à l'aide de la commande `ipnat`.	"Désactivation de NAT" à la page 668
Désactivation du filtrage de paquets et de NAT.	Désactivez le filtrage de paquets et NAT à l'aide de la commande `ipf`.	"Désactivation du filtrage de paquets" à la page 669

▼ Désactivation du filtrage de paquets

La procédure ci-dessous permet de désactiver le filtrage de paquets IP Filter en vidant les règles de filtrage de paquets de l'ensemble de règles de filtrage actif. La procédure ne désactive pas IP Filter. Vous pouvez réactiver IP Filter en ajoutant des règles à l'ensemble de règles.

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Pour désactiver les règles IP Filter, vous avez le choix entre les méthodes suivantes :**

- Supprimez du noyau l'ensemble de règles actif.

```
# ipf -Fa
```

Cette commande désactive toutes les règles de filtrage de paquets.

- Supprimez les règles de filtrage appliquées aux paquets entrants.

```
# ipf -Fi
```

Cette commande désactive les règles de filtrage de paquets appliquées aux paquets entrants.

- Supprimez les règles de filtrage appliquées aux paquets sortants.

```
# ipf -Fo
```

Cette commande désactive les règles de filtrage de paquets appliquées aux paquets sortants.

▼ Désactivation de NAT

La procédure ci-dessous permet de désactiver les règles NAT d'IP Filter en les vidant de l'ensemble de règles NAT actif. La procédure ne désactive pas IP Filter. Vous pouvez réactiver IP Filter en ajoutant des règles à l'ensemble de règles.

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Supprimez NAT du noyau.**

```
# ipnat -FC
```

L'option `-C` permet de supprimer toutes les entrées de la liste de règles NAT actuelle. L'option `-F` permet de supprimer toutes les entrées actives de la table de translation NAT qui indique les mappages NAT actifs.

▼ Désactivation du filtrage de paquets

Lorsque vous exécutez cette procédure, NAT et le filtrage de paquets sont supprimés du noyau. Pour réactiver le filtrage de paquets et NAT après avoir exécuté cette procédure, le cas échéant, vous devez réactiver IP Filter. Pour de plus amples informations, reportez-vous à la section "Réactivation d'IP Filter" à la page 665.

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Désactivez le filtrage de paquets et autorisez la transmission de tous les paquets sur le réseau.**

```
# ipf –D
```

Remarque – La commande `ipf -D` vide les règles de l'ensemble de règles. Lorsque vous réactivez le filtrage, vous devez ajouter des règles à l'ensemble de règles.

Utilisation du module `pfil`

Cette section décrit l'utilisation du module `pfil` STREAMS pour activer ou désactiver IP Filter et afficher les statistiques `pfil`. Les procédures s'appliquent uniquement aux systèmes exécutant l'une des versions Solaris ci-dessous :

- Solaris 10 3/05 ;
- Solaris 10 1/06 ;
- Solaris 10 6/06 ;
- Solaris 10 11/06.

La liste des tâches ci-dessous identifie les procédures associées à la configuration du module `pfil`.

TABLEAU 26–3 Utilisation du module `pfil` (liste des tâches)

Tâche	Description	Voir
Activation d'IP Filter	IP Filter n'est pas activé par défaut. Activez-le manuellement ou à l'aide des fichiers de configuration disponibles dans le répertoire `/etc/ipf/`, puis réinitialisez le système.	"Activation d'IP Filter dans les versions Solaris précédentes" à la page 670

TABLEAU 26–3 Utilisation du module pfil (liste des tâches) *(Suite)*

Tâche	Description	Voir
Activation d'une NIC pour le filtrage de paquets	Configurez le module pfil afin d'activer le filtrage de paquets sur une NIC (Network Interface Card, carte d'interface réseau).	"Activation d'une NIC pour le filtrage de paquets" à la page 672
Désactivation d'IP Filter sur une NIC	Retirez une NIC et autorisez la transmission de tous les paquets via la NIC.	"Désactivation d'IP Filter sur une NIC" à la page 674
Affichage des statistiques pfil	L'affichage des statistiques du module pfil facilite le dépannage d'IP Filter à l'aide de la commande ndd.	"Affichage des statistiques pfil d'IP Filter" à la page 675

▼ Activation d'IP Filter dans les versions Solaris précédentes

IP Filter est installé avec Oracle Solaris. Toutefois, le filtrage de paquets n'est pas activé par défaut. Pour activer IP Filter, suivez la procédure ci-dessous.

Remarque – Si votre système exécute la version Solaris 10 7/07 ou une version ultérieure, suivez la procédure "Activation d'IP Filter" à la page 664 utilisant des crochets de filtre de paquets.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ouvrez le fichier `/etc/ipf/pfil.ap` dans l'éditeur de fichiers de votre choix.

Ce fichier contient les noms des cartes d'interface réseau (NIC, Network Interface Card) présentes sur l'hôte. Par défaut, les noms sont commentés. Annulez le commentaire des noms de périphérique correspondant au trafic réseau que vous souhaitez filtrer. Si la NIC de votre système n'est pas répertoriée, ajoutez une ligne pour la spécifier.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor lastminor modules
```

```
#le     -1      0       pfil
#qe     -1      0       pfil
hme     -1      0       pfil (Device has been uncommented for filtering)
#qfe    -1      0       pfil
#eri    -1      0       pfil
#ce     -1      0       pfil
#bge    -1      0       pfil
#be     -1      0       pfil
#vge    -1      0       pfil
#ge     -1      0       pfil
#nf     -1      0       pfil
#fa     -1      0       pfil
#ci     -1      0       pfil
#el     -1      0       pfil
#ipdptp -1      0       pfil
#lane   -1      0       pfil
#dmfe   -1      0       pfil
```

3 Activez les modifications apportées au fichier `/etc/ipf/pfil.ap` en redémarrant l'instance de service `network/pfil`.

```
# svcadm restart network/pfil
```

4 Créez un ensemble de règles de filtrage de paquets.

L'ensemble de règles de filtrage de paquets contient les règles de filtrage de paquets utilisées par IP Filter. Pour charger les règles de filtrage de paquets à l'initialisation, modifiez le fichier `/etc/ipf/ipf.conf` afin d'implémenter le filtrage de paquets IPv4. Utilisez le fichier `/etc/ipf/ipf6.conf` pour les règles de filtrage de paquets IPv6. Si vous ne souhaitez pas charger les règles de filtrage de paquets à l'initialisation, insérez-les dans le fichier de votre choix, puis activez manuellement le filtrage de paquets. Pour plus d'informations sur le filtrage de paquets, reportez-vous à la section "Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter" à la page 653. Pour plus d'informations sur l'utilisation des fichiers de configuration, reportez-vous à la section "Création et modification des fichiers de configuration IP Filter" à la page 695.

5 (Facultatif) Créez un fichier de configuration NAT (Network Address Translation, translation d'adresse réseau).

Remarque – NAT ne prend pas en charge IPv6.

Créez le fichier `ipnat.conf` si vous souhaitez utiliser la translation d'adresse réseau. Si vous souhaitez charger les règles NAT à l'initialisation, créez le fichier `/etc/ipf/ipnat.conf` afin d'y insérer les règles NAT. Si vous ne souhaitez pas charger les règles NAT à l'initialisation, placez le fichier `ipnat.conf` dans le répertoire de votre choix, puis activez manuellement les règles NAT.

Pour de plus amples informations sur NAT, reportez-vous à la section "Utilisation de la fonctionnalité NAT d'IP Filter" à la page 656.

6 **(Facultatif) Créez un fichier de configuration de pool d'adresses.**

Créez un fichier `ipool.conf` si vous souhaitez référencer un groupe d'adresses sous la forme d'un pool d'adresses unique. Pour charger le fichier de configuration de pool d'adresses à l'initialisation, créez le fichier `/etc/ipf/ippool.conf` afin d'y insérer le pool d'adresses. Si vous ne souhaitez pas charger le fichier de configuration de pool d'adresses à l'initialisation, placez le fichier `ippool.conf` dans le répertoire de votre choix, puis activez manuellement les règles.

Un pool d'adresses peut contenir exclusivement des adresses IPv4 ou exclusivement des adresses IPv6. Il peut également contenir à la fois des adresses IPv4 et des adresses IPv6.

Pour de plus amples informations sur les pools d'adresses, reportez-vous à la section "Utilisation de la fonctionnalité de pools d'adresses d'IP Filter" à la page 658.

7 **Activez IP Filter selon l'une des méthodes ci-dessous :**

- Activez IP Filter et réinitialisez la machine.

```
# svcadm enable network/ipfilter
# reboot
```

Remarque – La réinitialisation est requise si l'exécution des commandes `ifconfig unplumb` et `ifconfig plumb` sur les NIC n'est pas sécurisée.

- Activez les NIC à l'aide des commandes `ifconfig unplumb` et `ifconfig plumb.` Activez ensuite IP Filter. La version `inet6` de l'interface doit être montée afin de permettre l'implémentation du filtrage de paquets IPv6.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20 netmask 255.255.255.0 up
# ifconfig hme0 inte6 unplumb
# ifconfig hme0 inet6 plumb fec3:f849::1/96 up
# svcadm enable network/ipfilter
```

Pour de plus amples informations sur la commande `ifconfig`, reportez-vous à la page de manuel `ifconfig(1M)`.

▼ Activation d'une NIC pour le filtrage de paquets

IP Filter est activé à l'initialisation lorsque le fichier `/etc/ipf/ipf.conf` (ou le fichier `/etc/ipf/ipf6.conf`, si vous utilisez IPv6) existe. Pour activer le filtrage sur une NIC une fois IP Filter activé, le cas échéant, suivez la procédure ci-dessous.

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

   Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Ouvrez le fichier `/etc/ipf/pfil.ap` dans l'éditeur de fichiers de votre choix.**

   Ce fichier contient les noms des NIC présentes sur l'hôte. Par défaut, les noms sont commentés. Annulez le commentaire des noms de périphérique correspondant au trafic réseau que vous souhaitez filtrer. Si la NIC de votre système n'est pas répertoriée, ajoutez une ligne pour la spécifier.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor lastminor modules

#le     -1      0       pfil
#qe     -1      0       pfil
hme     -1      0       pfil (Device has been uncommented for filtering)
#qfe    -1      0       pfil
#eri    -1      0       pfil
#ce     -1      0       pfil
#bge    -1      0       pfil
#be     -1      0       pfil
#vge    -1      0       pfil
#ge     -1      0       pfil
#nf     -1      0       pfil
#fa     -1      0       pfil
#ci     -1      0       pfil
#el     -1      0       pfil
#ipdptp -1      0       pfil
#lane   -1      0       pfil
#dmfe   -1      0       pfil
```

3. **Activez les modifications apportées au fichier `/etc/ipf/pfil.ap` en redémarrant l'instance de service `network/pfil`.**

```
# svcadm restart network/pfil
```

4. **Activez la NIC selon l'une des méthodes ci-dessous :**

   - Redémarrez l'ordinateur.

```
# reboot
```

Remarque – La réinitialisation est requise si l'exécution des commandes `ifconfig unplumb` et `ifconfig plumb` sur les NIC n'est pas sécurisée.

- Activez les NIC à filtrer à l'aide de la commande `ifconfig` avec les options `unplumb` et `plumb`. La version `inet6` de chaque interface doit être montée afin de permettre l'implémentation du filtrage de paquets IPv6.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20  netmask 255.255.255.0  up
# ifconfig hme0 inet6 unplumb
# ifconfig hme0 inet6 plumb fec3:f840::1/96 up
```

  Pour de plus amples informations sur la commande `ifconfig`, reportez-vous à la page de manuel `ifconfig(1M)`.

▼ Désactivation d'IP Filter sur une NIC

Pour arrêter le filtrage des paquets sur une NIC, le cas échéant, suivez la procédure ci-dessous.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ouvrez le fichier `/etc/ipf/pfil.ap` dans l'éditeur de fichiers de votre choix.

Ce fichier contient les noms des NIC présentes sur l'hôte. Le commentaire des NIC utilisées pour filtrer le trafic réseau est annulé. Commentez les noms des périphériques que vous ne souhaitez plus utiliser pour filtrer le trafic réseau.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor lastminor modules

#le     -1      0       pfil
#qe     -1      0       pfil
#hme    -1      0       pfil (Commented-out device no longer filters network traffic)
#qfe    -1      0       pfil
#eri    -1      0       pfil
#ce     -1      0       pfil
#bge    -1      0       pfil
#be     -1      0       pfil
#vge    -1      0       pfil
```

```
#ge     -1      0       pfil
#nf     -1      0       pfil
#fa     -1      0       pfil
#ci     -1      0       pfil
#el     -1      0       pfil
#ipdptp -1      0       pfil
#lane   -1      0       pfil
#dmfe   -1      0       pfil
```

3 Désactivez la NIC selon l'une des méthodes ci-dessous :

- Redémarrez l'ordinateur.

  ```
  # reboot
  ```

  Remarque – La réinitialisation est requise si l'exécution des commandes `ifconfig unplumb` et `ifconfig plumb` sur les NIC n'est pas sécurisée.

- Désactivez les NIC à l'aide de la commande `ifconfig` avec les options `unplumb` et `plumb`. La version `inet6` de chaque interface doit être démontée afin de permettre la désactivation du filtrage de paquets IPv6. Procédez comme suit. Le périphérique système `hme` est utilisé en exemple :

  a. Identifiez le numéro majeur du périphérique à désactiver.

  ```
  # grep hme /etc/name_to_major
  hme 7
  ```

  b. Affichez la configuration `autopush` actuelle pour `hme0`.

  ```
  # autopush -g -M 7 -m 0
     Major     Minor     Lastminor       Modules
         7       ALL           -          pfil
  ```

  c. Supprimez la configuration `autopush`.

  ```
  # autopush -r -M 7 -m 0
  ```

  d. Ouvrez le périphérique et attribuez les adresses IP au périphérique.

  ```
  # ifconfig hme0 unplumb
  # ifconfig hme0 plumb 192.168.1.20  netmask 255.255.255.0  up
  # ifconfig hme0 inet6 unplumb
  # ifconfig hme0 inet6 plumb fec3:f840::1/96 up
  ```

  Pour de plus amples informations sur la commande `ifconfig`, reportez-vous à la page de manuel `ifconfig(1M)`.

▼ Affichage des statistiques `pfil` d'IP Filter

Vous pouvez afficher les statistiques `pfil` lors du dépannage d'IP Filter.

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichage des statistiques `pfil`**

```
# ndd -get /dev/pfil qif_status
```

Exemple 26–1 Affichage des statistiques `pfil` d'IP Filter

L'exemple ci-dessous illustre l'affichage des statistiques **`pfil`**.

```
# ndd -get /dev/pfil qif_status
ifname ill q OTHERQ num sap hl nr nw bad copy copyfail drop notip nodata
   notdata
QIF6 0 300011247b8 300011248b0 6 806 0 4 9 0 0 0 0 0 0 0 0
dmfe1 3000200a018 30002162a50 30002162b48 5 800 14 171 13681 0 0 0 0 0 0 0
```

Utilisation des ensembles de règles IP Filter

La liste des tâches ci-dessous identifie les procédures associées aux ensembles de règles IP Filter.

TABLEAU 26–4 Utilisation des ensembles de règles IP Filter (liste des tâches)

Tâche	Description	Voir
Gestion, affichage et modification des ensembles de règles pour le filtrage de paquets IP Filter		"Gérez les ensembles de règles de filtrage de paquets d'IP Filter" à la page 677
	Affichez un ensemble de règles actif pour le filtrage de paquets.	"Affichage de l'ensemble actif de règles de filtrage de paquets" à la page 678
	Affichez un ensemble de règles inactif pour le filtrage de paquets.	"Affichage de l'ensemble inactif de règles de filtrage de paquets" à la page 678
	Activez un nouvel ensemble de règles actif.	"Activation d'un nouvel ensemble de règles de filtrage de paquets ou d'un ensemble mis à jour" à la page 679
	Supprimez un ensemble de règles.	"Suppression d'un ensemble de règles de filtrage de paquets" à la page 680

TABLEAU 26–4 Utilisation des ensembles de règles IP Filter (liste des tâches) *(Suite)*

Tâche	Description	Voir
	Ajoutez des règles aux ensembles de règles.	"Ajout de règles à l'ensemble actif de règles de filtrage de paquets" à la page 681
		"Ajout de règles à l'ensemble inactif de règles de filtrage de paquets" à la page 682
	Basculez entre les ensembles de règles actif et inactif.	"Basculement entre les ensembles actif et inactif de règles de filtrage de paquets" à la page 682
	Supprimez du noyau un ensemble de règles inactif.	"Suppression d'un ensemble inactif de règles de filtrage de paquets du noyau" à la page 683
Gérez, affichez et modifiez les règles NAT IP Filter		"Gestion des règles NAT d'IP Filter" à la page 684
	Affichez les règles NAT actives.	"Affichage des règles NAT actives" à la page 684
	Supprimez les règles NAT.	"Suppression des règles NAT" à la page 685
	Ajoutez des règles aux règles NAT.	"Ajout de règles aux règles NAT" à la page 685
Gérez, affichez et modifiez les pools d'adresses IP Filter		"Gestion des pools d'adresses d'IP Filter" à la page 686
	Affichez les pools d'adresses actifs.	"Affichage des pools d'adresses actifs" à la page 686
	Supprimez un pool d'adresses.	"Suppression d'un pool d'adresses" à la page 687
	Ajoutez des règles à un pool d'adresses.	"Ajout de règles à un pool d'adresses" à la page 687

Gérez les ensembles de règles de filtrage de paquets d'IP Filter

Lorsque cette option est activée, les ensembles actif et inactif de règles de filtrage de paquets peuvent résider dans le noyau. L'ensemble de règles actif détermine le filtrage appliqué aux paquets entrants et aux paquets sortants. L'ensemble de règles inactif contient également des

règles. Ces règles ne sont pas appliquées, sauf si vous définissez l'ensemble de règles inactif comme l'ensemble de règles actif. Vous pouvez gérer, afficher et modifier les ensembles actif et inactif de règles de filtrage de paquets.

▼ Affichage de l'ensemble actif de règles de filtrage de paquets

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichez l'ensemble actif de règles de filtrage de paquets chargé dans le noyau.**

```
# ipfstat -io
```

Exemple 26–2 Affichage de l'ensemble actif de règles de filtrage de paquets

L'exemple ci-dessous présente la sortie de l'ensemble actif de règles de filtrage de paquets chargé dans le noyau.

```
# 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
```

▼ Affichage de l'ensemble inactif de règles de filtrage de paquets

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichez l'ensemble inactif de règles de filtrage de paquets.**

```
# ipfstat -I -io
```

Exemple 26–3 Affichage de l'ensemble inactif de règles de filtrage de paquets

L'exemple ci-dessous présente la sortie d'un ensemble inactif de règles de filtrage de paquets.

```
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
```

▼ Activation d'un nouvel ensemble de règles de filtrage de paquets ou d'un ensemble mis à jour

Effectuez la procédure ci-dessous pour exécuter l'une ou l'autre des tâches suivantes :

- activation d'un ensemble de règles de filtrage de paquets différent de celui que IP Filter utilise actuellement ;
- rechargement du même ensemble de règles de filtrage mis à jour.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Procédez de l'une des façons suivantes :

- Si vous souhaitez activer un ensemble de règles complètement différent, créez-le dans un fichier distinct.
- Pour mettre à jour l'ensemble de règles actuel, modifiez le fichier de configuration contenant l'ensemble de règles.

3 Supprimez l'ensemble de règles actuel et chargez le nouvel ensemble de règles.

```
# ipf -Fa -f filename
```

La variable *fichier* peut correspondre à un fichier contenant un ensemble de règles complètement différent, ou au fichier contenant l'ensemble de règles actif, mis à jour.

L'ensemble de règles actif est supprimé du noyau. Les règles du *fichier* constituent dorénavant l'ensemble de règles actif.

Remarque – Même si vous rechargez le fichier de configuration actuel, vous devez exécuter la commande. Dans le cas contraire, le système ignore l'ensemble de règles modifié défini dans le fichier de configuration mis à jour et continue d'appliquer l'ancien ensemble de règles.

N'utilisez pas de commandes telles que `ipf -D` ou `svcadm restart` pour charger l'ensemble de règles mis à jour. Ces commandes affectent la sécurité du réseau, car elles désactivent le pare-feu avant de charger le nouvel ensemble de règles.

Exemple 26–4 Activation d'un nouvel ensemble de règles de filtrage de paquets

Dans l'exemple ci-dessous, un ensemble de règles de filtrage de paquets est remplacé par un autre ensemble se trouvant dans un fichier de configuration distinct, `/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
```

Exemple 26–5 Rechargement d'un ensemble de règles de filtrage de paquets mis à jour

Dans l'exemple ci-dessous, un ensemble de règles de filtrage de paquets actuellement actif est rechargé suite à sa mise à jour. Dans cet exemple, le fichier utilisé est `/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
```

▼ Suppression d'un ensemble de règles de filtrage de paquets

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

   Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Supprimez l'ensemble de règles.**

   ```
   # ipf -F [a|i|o]
   ```

   `-a` Supprime toutes les règles de filtrage de l'ensemble de règles.

   `-i` Supprime les règles de filtrage pour les paquets entrants.

   `-o` Supprime les règles de filtrage pour les paquets sortants.

Exemple 26–6 Suppression d'un ensemble de règles de filtrage de paquets

Dans l'exemple ci-dessous, toutes les règles de filtrage sont supprimées de l'ensemble de règles de filtrage actif.

```
# 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)
```

▼ Ajout de règles à l'ensemble actif de règles de filtrage de paquets

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

   Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Appliquez l'une des méthodes ci-dessous pour ajouter des règles à l'ensemble de règles actif :**

   - Pour ajouter des règles à l'ensemble de règles via la ligne de commande, exécutez la commande `ipf -f -`.

     ```
     # echo "block in on dmfe1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
     ```

   - Exécutez les commandes ci-dessous :

     a. Créez un ensemble de règles dans le fichier de votre choix.

     b. Ajoutez ces règles à l'ensemble de règles actif.

        ```
        # ipf -f filename
        ```

        Les règles présentes dans le *fichier* sont ajoutées à la fin de l'ensemble de règles actif. IP Filter utilise un algorithme de type "dernière règle correspondante", de sorte que les nouvelles règles déterminent les priorités de filtrage, sauf si l'utilisateur ajoute le mot-clé `quick`. Si le paquet correspond à une règle contenant le mot-clé `quick`, l'action associée à cette règle est exécutée et les règles suivantes sont ignorées.

Exemple 26–7 Ajout de règles à l'ensemble actif de règles de filtrage de paquets

Dans l'exemple ci-dessous, une règle est ajoutée à l'ensemble actif de règles de filtrage de paquets à partir de la ligne de commande.

```
# 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
```

▼ Ajout de règles à l'ensemble inactif de règles de filtrage de paquets

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Créez un ensemble de règles dans le fichier de votre choix.**

3 **Ajoutez ces règles à l'ensemble de règles inactif.**

```
# ipf -I -f filename
```

Les règles présentes dans le *fichier* sont ajoutées à la fin de l'ensemble de règles inactif. IP Filter utilise un algorithme de type "dernière règle correspondante", de sorte que les nouvelles règles déterminent les priorités de filtrage, sauf si l'utilisateur ajoute le mot-clé `quick`. Si le paquet correspond à une règle contenant le mot-clé `quick`, l'action associée à cette règle est exécutée et les règles suivantes sont ignorées.

Exemple 26–8 Ajout de règles à l'ensemble de règles inactif

Dans l'exemple ci-dessous, une règle est ajoutée à l'ensemble de règles inactif à partir d'un fichier.

```
# 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
```

▼ Basculement entre les ensembles actif et inactif de règles de filtrage de paquets

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Basculez entre les ensembles de règles actif et inactif.**

```
# ipf -s
```

Cette commande permet de basculer entre les ensembles de règles actif et inactif dans le noyau. Si l'ensemble de règles inactif est vide, aucun filtrage de paquets n'est effectué.

Exemple 26–9 Basculement entre les ensembles actif et inactif de règles de filtrage de paquets

Dans l'exemple ci-dessous, la commande `ipf -s` est exécutée. L'ensemble de règles inactif devient alors l'ensemble de règles actif, tandis que l'ensemble de règles actif devient l'ensemble de règles inactif.

- Avant l'exécution de la commande `ipf -s`, la sortie de la commande `ipfstat -I -io` permet d'afficher les règles de l'ensemble de règles inactif. La sortie de la commande `ipfstat -io` affiche les règles de l'ensemble de règles actif.

```
# 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
```

- Une fois la commande `ipf -s` exécutée, les sorties des commandes `ipfstat -I -io` et `ipfstat -io` indiquent que le contenu des deux ensembles de règles a été échangé.

```
# 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
```

▼ Suppression d'un ensemble inactif de règles de filtrage de paquets du noyau

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Spécifiez l'ensemble de règles inactif via la commande "flush all".

```
# ipf -I -Fa
```

Cette commande vide l'ensemble de règles inactif du noyau.

Remarque – Si vous exécutez ensuite la commande `ipf -s`, l'ensemble de règles inactif vide devient l'ensemble de règles actif. Si l'ensemble de règles actif est vide, *aucun* filtrage n'est effectué.

Exemple 26–10 Suppression d'un ensemble inactif de règles de filtrage de paquets du noyau

Dans l'exemple ci-dessous, l'ensemble inactif de règles de filtrage de paquets est vidé afin de supprimer toutes les règles.

```
# 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)
```

Gestion des règles NAT d'IP Filter

Appliquez les procédures ci-dessous pour gérer, afficher et modifier les règles NAT.

▼ Affichage des règles NAT actives

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

   Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Affichez les règles NAT actives.**

   ```
   # ipnat -l
   ```

Exemple 26–11 Affichage des règles NAT actives

L'exemple ci-dessous présente la sortie de l'ensemble de règles NAT actif.

```
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

▼ Suppression des règles NAT

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Supprimez les règles NAT actuelles.**

```
# ipnat -C
```

Exemple 26–12 Suppression des règles NAT

Dans l'exemple ci-dessous, les entrées des règles NAT actuelles sont supprimées.

```
# 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:
```

▼ Ajout de règles aux règles NAT

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Appliquez l'une des méthodes ci-dessous pour ajouter des règles à l'ensemble de règles actif :**

- Pour ajouter des règles à l'ensemble de règles NAT via la ligne de commande, exécutez la commande `ipnat -f -`.

  ```
  # echo "map dmfe0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
  ```

- Exécutez les commandes ci-dessous :

  a. Créez des règles NAT supplémentaires dans le fichier de votre choix.

  b. Ajoutez ces règles aux règles NAT actives.

  ```
  # ipnat -f filename
  ```

Les règles présentes dans le *fichier* sont ajoutées à la fin des règles NAT.

Exemple 26–13 Ajout de règles à l'ensemble de règles NAT

Dans l'exemple ci-dessous, une règle est ajoutée à l'ensemble de règles NAT via la ligne de commande.

```
# 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:
```

Gestion des pools d'adresses d'IP Filter

Appliquez les procédures ci-dessous pour gérer, afficher et modifier les pools d'adresses.

▼ Affichage des pools d'adresses actifs

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

   Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Affichez le pool d'adresses actif.**

   ```
   # ippool -l
   ```

Exemple 26–14 Affichage du pool d'adresses actif

Dans l'exemple ci-dessous, le contenu du pool d'adresses actif est affiché.

```
# ippool -l
table role = ipf type = tree number = 13
        { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

▼ Suppression d'un pool d'adresses

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Supprimez les entrées du pool d'adresses actuel.**

```
# ippool -F
```

Exemple 26–15 Suppression d'un pool d'adresses

Dans l'exemple ci-dessous, un pool d'adresses est supprimé.

```
# 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
```

▼ Ajout de règles à un pool d'adresses

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Appliquez l'une des méthodes ci-dessous pour ajouter des règles à l'ensemble de règles actif :**

- Pour ajouter des règles à l'ensemble de règles via la ligne de commande, exécutez la commande `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 -
  ```

- Exécutez les commandes ci-dessous :

  a. Créez des pools d'adresses supplémentaires dans le fichier de votre choix.

  b. Ajoutez ces règles au pool d'adresses actif.

  ```
  # ippool -f filename
  ```

  Les règles présentes dans le *fichier* sont ajoutées à la fin du pool d'adresses actif.

Exemple 26–16 Ajout de règles à un pool d'adresses

Dans l'exemple ci-dessous, un pool d'adresses est ajouté à l'ensemble de règles de pool d'adresses via la ligne de commande.

```
# 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; };
```

Affichage des statistiques et des informations relatives à IP Filter

TABLEAU 26–5 Affichage des statistiques et informations IP Filter (liste des tâches)

Tâche	Description	Voir
Affichage des tables d'état	Affichez les tables d'état pour obtenir des informations sur le filtrage de paquets à l'aide de la commande `ipfstat`.	"Affichage des tables d'état d'IP Filter" à la page 688
Affichage des statistiques d'état	Affichez les statistiques relatives à l'état des paquets à l'aide de la commande `ipfstat -s`.	"Affichage des statistiques d'état d'IP Filter" à la page 689
Affichage des statistiques NAT	Affichez les statistiques NAT à l'aide de la commande `ipnat -s`.	"Affichage des statistiques NAT d'IP Filter" à la page 690
Affichage des statistiques de pool d'adresses	Affichez les statistiques de pool d'adresses à l'aide de la commande `ippool -s`.	"Affichage des statistiques de pool d'adresses d'IP Filter" à la page 691

▼ Affichage des tables d'état d'IP Filter

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichez la table d'état.**

```
# ipfstat
```

Remarque – L'option `-t` permet d'afficher la table d'état au format de l'utilitaire top.

Exemple 26–17 Affichage des tables d'état d'IP Filter

Dans l'exemple ci-dessous, une table d'état est affichée.

```
# 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
```

▼ Affichage des statistiques d'état d'IP Filter

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichez les statistiques d'état.**

```
# ipfstat -s
```

Exemple 26–18 Affichage des statistiques d'état d'IP Filter

Dans l'exemple ci-dessous, les statistiques d'état sont affichées.

```
# 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
```

▼ Affichage des statistiques NAT d'IP Filter

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichage des statistiques NAT**

```
# ipnat -s
```

Exemple 26–19 Affichage des statistiques NAT d'IP Filter

Dans l'exemple ci-dessous, les statistiques NAT sont affichées.

```
# ipnat -s
mapped  in      0       out     0
added   0       expired 0
no memory       0       bad nat 0
inuse   0
rules   1
wilds   0
```

▼ Affichage des statistiques de pool d'adresses d'IP Filter

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichage des statistiques de pool d'adresses**

```
# ippool -s
```

Exemple 26–20 Affichage des statistiques de pool d'adresses d'IP Filter

Dans l'exemple ci-dessous, les statistiques de pool d'adresses sont affichées.

```
# ippool -s
Pools:  3
Hash Tables:    0
Nodes:  0
```

Utilisation des fichiers journaux IP Filter

TABLEAU 26–6 Utilisation des fichiers journaux IP Filter (liste des tâches)

Tâche	Description	Voir
Création d'un fichier journal	Créez un fichier journal IP distinct.	"Configuration d'un fichier journal d'IP Filter" à la page 692
Affichage des fichiers journaux	Affichez le fichier journal normal et les fichiers journaux d'état et NAT à l'aide de la commande `ipmon`.	"Affichage des fichiers journaux IP Filter" à la page 692
Vidage du tampon de journalisation des paquets	Supprimez le contenu du tampon de journalisation des paquets à l'aide de la commande `ipmon - F`.	"Vidage du fichier journal de paquets" à la page 694
Enregistrement des paquets consignés dans un fichier	Les paquets consignés peuvent être enregistrés dans un fichier afin d'être consultés par la suite.	"Enregistrement dans un fichier des paquets consignés" à la page 694

▼ Configuration d'un fichier journal d'IP Filter

Par défaut, toutes les informations de journal IP Filter sont enregistrées dans le fichier `syslogd`. Configurez un fichier journal afin de séparer les informations de trafic IP Filter enregistrées des autres données susceptibles d'être consignées dans le fichier journal par défaut. Procédez comme suit.

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez les lignes suivantes au fichier `/etc/syslog.conf` :**

```
# Save IPFilter log output to its own file
local0.debug             /var/log/log-name
```

Remarque – Sur la deuxième ligne, séparez `local0.debug` de `/var/log/` *journal* à l'aide de la touche de tabulation (non la barre d'espace).

---

3 **Créez le fichier journal.**

```
# touch /var/log/log-name
```

4 **Redémarrez le service de journal système.**

```
# svcadm restart system-log
```

Exemple 26–21 Création d'un journal IP Filter

Dans l'exemple ci-dessous, le fichier `ipmon.log` est créé pour archiver les informations IP Filter.

Dans `/etc/syslog.conf` :

```
# Save IPFilter log output to its own file
local0.debug             /var/log/ipmon.log
```

Sur la ligne de commande :

```
# touch /var/log/ipmon.log
# svcadm restart system-log
```

▼ Affichage des fichiers journaux IP Filter

Avant de commencer Il est conseillé de créer un fichier journal distinct pour enregistrer les données IP Filter. Reportez-vous à la section "Configuration d'un fichier journal d'IP Filter" à la page 692.

1. **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

   Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Affichez le fichier journal normal, le fichier journal NAT ou le fichier journal d'état. Pour afficher un fichier journal, tapez la commande ci-dessous, conjointement avec l'option adéquate :**

   # ipmon -o [S|N|I] *filename*

   `S` Affiche le fichier journal d'état.

   `N` Affiche le fichier journal NAT.

   `I` Affiche le fichier journal IP normal.

   Pour afficher le fichier journal normal et les fichiers journaux d'état et NAT, appliquez les options :

   # ipmon -o SNI *filename*

   - **Si vous avez arrêté manuellement le démon `ipmon`, vous pouvez également exécuter la commande ci-dessous pour afficher le fichier journal IP Filter et les fichiers journaux d'état et NAT :**

     # ipmon -a *filename*

     Remarque – N'utilisez pas la syntaxe `ipmon -a` si le démon `ipmon` est en cours d'exécution. Normalement, le démon démarre automatiquement à l'initialisation du système. Si vous exécutez la commande `ipmon -a`, une autre copie de `ipmon` s'ouvre également. Dans ce cas, les deux copies lisent les mêmes informations de journal, mais tout message du journal n'est reçu que par l'une d'elles.

   Pour plus d'informations sur l'affichage des fichiers journaux, reportez-vous à la page de manuel `ipmon(1M)`.

Exemple 26–22 Affichage des fichiers journaux IP Filter

L'exemple ci-dessous présente la sortie du fichier `/var/ipmon.log`.

```
# ipmon -o SNI /var/ipmon.log
02/09/2004 15:27:20.606626 hme0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

ou

```
# pkill ipmon
# ipmon -aD /var/ipmon.log
02/09/2004 15:27:20.606626 hme0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

▼ Vidage du fichier journal de paquets

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Videz le tampon de journalisation des paquets.**

```
# ipmon -F
```

Exemple 26–23 Vidage du fichier journal de paquets

L'exemple ci-dessous présente la sortie obtenue en cas de suppression d'un fichier journal. Le système génère un rapport même si le fichier journal est vide, comme dans cet exemple.

```
# ipmon -F
0 bytes flushed from log buffer
0 bytes flushed from log buffer
0 bytes flushed from log buffer
```

▼ Enregistrement dans un fichier des paquets consignés

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Enregistrez dans un fichier les paquets consignés.**

```
# cat /dev/ipl > filename
```

Continuez la journalisation des paquets dans le *fichier* et interrompez la procédure en tapant `Ctrl-C` pour afficher de nouveau l'invite de ligne de commande.

Exemple 26–24 Enregistrement dans un fichier des paquets consignés

L'exemple ci-dessous présente les résultats obtenus lorsque les paquets consignés sont enregistrés dans un fichier.

```
# cat /dev/ipl > /tmp/logfile
^C#

# ipmon -f /tmp/logfile
02/09/2004 15:30:28.708294 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 52 -S IN
02/09/2004 15:30:28.708708 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.792611 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 70 -AP IN
02/09/2004 15:30:28.872000 hme0 @0:1 p 129.146.157.149,33923 ->
 129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872142 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 43 -AP IN
02/09/2004 15:30:28.872808 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872951 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 47 -AP IN
02/09/2004 15:30:28.926792 hme0 @0:1 p 129.146.157.149,33923 ->
  129.146.157.145,23 PR tcp len 20 40 -A IN
.
.
(output truncated)
```

Création et modification des fichiers de configuration IP Filter

Vous devez modifier directement les fichiers de configuration afin de créer et modifier les ensembles de règles et les pools d'adresses. Les fichiers de configuration suivent les règles de syntaxe UNIX standard :

- Le signe dièse (#) indique qu'une ligne contient des commentaires.
- Une ligne peut contenir à la fois des commentaires et des règles.
- Vous pouvez ajouter des espaces supplémentaires afin de faciliter la lecture des règles.
- La définition d'une règle peut s'étaler sur plusieurs lignes. Insérez un backslash (\) à la fin d'une ligne pour indiquer que la règle continue sur la ligne suivante.

▼ Création d'un fichier de configuration d'IP Filter

La procédure ci-dessous décrit la configuration des :

- fichiers de configuration de filtrage de paquets ;
- fichiers de configuration des règles NAT ;

- fichiers de configuration de pool d'adresses.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Lancez l'éditeur de fichiers de votre choix. Créez et modifiez le fichier de configuration de la fonction que vous souhaitez configurer.

- Pour créer un fichier de configuration des règles de filtrage de paquets, modifiez le fichier `ipf.conf`.

  IP Filter utilise les règles de filtrage de paquets spécifiées dans le fichier `ipf.conf`. Si vous placez le fichier de règles de filtrage de paquets dans le fichier `/etc/ipf/ipf.conf`, ce fichier est chargé à l'initialisation du système. Pour empêcher le chargement des règles de filtrage à l'initialisation, le cas échéant, placez-les dans le fichier de votre choix. Vous pouvez ensuite activer les règles à l'aide de la commande `ipf`, comme décrit à la section "Activation d'un nouvel ensemble de règles de filtrage de paquets ou d'un ensemble mis à jour" à la page 679.

  Pour plus d'informations sur la création de règles de filtrage de paquets, reportez-vous à la section "Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter" à la page 653.

  Remarque – Si le fichier `ipf.conf` est vide, aucun filtrage n'est appliqué. Un fichier `ipf.conf` vide correspond à un ensemble de règles défini comme suit :

  ```
  pass in all
  pass out all
  ```

- Pour créer un fichier de configuration des règles NAT, modifiez le fichier `ipnat.conf`.

  IP Filter utilise les règles NAT spécifiées dans le fichier `ipnat.conf`. Si vous placez le fichier de règles NAT dans le fichier `>/etc/ipf/ipnat.conf`, ce fichier est chargé à l'initialisation du système. Pour empêcher le chargement des règles NAT à l'initialisation, le cas échéant, placez le fichier `ipnat.conf` dans le dossier de votre choix. Ensuite, vous pouvez activer les règles NAT à l'aide de la commande `ipnat`.

  Pour plus d'informations sur la création de règles pour NAT, reportez-vous à la section "Utilisation de la fonctionnalité NAT d'IP Filter" à la page 656.

- Pour créer un fichier de configuration des pools d'adresses, modifiez le fichier `ippool.conf`.

  IP Filter utilise le pool d'adresses spécifié dans le fichier `ippool.conf`. Si vous placez le fichier de règles du pool d'adresses dans le fichier `/etc/ipf/ippool.conf`, ce fichier est chargé à l'initialisation du système. Pour empêcher le chargement du pool d'adresses à

l'initialisation, le cas échéant, placez le fichier `ippool.conf` dans le dossier de votre choix. Ensuite, vous pouvez activer le pool d'adresses à l'aide de la commande `ippool`.

Pour plus d'informations sur la création de pools d'adresses, reportez-vous à la section "Utilisation de la fonctionnalité de pools d'adresses d'IP Filter" à la page 658.

Exemples de fichiers de configuration IP Filter

Les exemples ci-dessous illustrent les règles de filtrage de paquets utilisées dans les configurations de filtrage.

EXEMPLE 26–25 Configuration d'un hôte IP Filter

Cet exemple correspond à une configuration définie sur une machine hôte avec une interface réseau `elxl`.

```
# pass and log everything by default
pass in log on bge0 all
pass out log on bge0 all

# block, but don't log, incoming packets from other reserved addresses
block in quick on bge0 from 10.0.0.0/8 to any
block in quick on bge0 from 172.16.0.0/12 to any

# block and log untrusted internal IPs. 0/32 is notation that replaces
# address of the machine running Solaris IP Filter.
block in log quick from 192.168.1.15 to <thishost>
block in log quick from 192.168.1.43 to <thishost>

# block and log X11 (port 6000) and remote procedure call
# and portmapper (port 111) attempts
block in log quick on bge0 proto tcp from any to bge0/32 port = 6000 keep state
block in log quick on bge0 proto tcp/udp from any to bge0/32 port = 111 keep state
```

Cet ensemble de règles commence par deux règles illimitées qui permettent à tout type de données d'entrer et sortir via l'interface `elxl`. Le deuxième ensemble de règles empêche tout paquet entrant issu des espaces d'adresses privées `10.0.0.0` et `172.16.0.0` de traverser la pare-feu. L'ensemble de règles suivant bloque des adresses internes spécifiques de la machine hôte. Enfin, le dernier ensemble de règles empêche l'entrée des paquets via les ports 6000 et 111.

EXEMPLE 26–26 Configuration d'un serveur IP Filter

Cet exemple présente la configuration d'une machine hôte tenant lieu de serveur Web. Cette machine possède une interface réseau `eri`.

```
# web server with an eri interface
# block and log everything by default; then allow specific services
# group 100 - inbound rules
# group 200 - outbound rules
# (0/32) resolves to our IP address)
```

EXEMPLE 26–26 Configuration d'un serveur IP Filter *(Suite)*

```
*** FTP proxy ***


# block short packets which are packets fragmented too short to be real.
block in log quick all with short


# block and log inbound and outbound by default, group by destination
block in log on eri0 from any to any head 100
block out log on eri0 from any to any head 200


# web rules that get hit most often
pass in quick on eri0 proto tcp from any \
to eri0/32 port = http flags S keep state group 100
pass in quick on eri0 proto tcp from any \
to eri0/32 port = https flags S keep state group 100


# inbound traffic - ssh, auth
pass in quick on eri0 proto tcp from any \
to eri0/32 port = 22 flags S keep state group 100
pass in log quick on eri0 proto tcp from any \
to eri0/32 port = 113 flags S keep state group 100
pass in log quick on eri0 proto tcp from any port = 113 \
to eri0/32 flags S keep state group 100


# outbound traffic - DNS, auth, NTP, ssh, WWW, smtp
pass out quick on eri0 proto tcp/udp from eri0/32 \
to any port = domain flags S keep state group 200
pass in quick on eri0 proto udp from any port = domain to eri0/32 group 100

pass out quick on eri0 proto tcp from eri0/32 \
to any port = 113 flags S keep state group 200
pass out quick on eri0 proto tcp from eri0/32 port = 113 \
to any flags S keep state group 200

pass out quick on eri0 proto udp from eri0/32 to any port = ntp group 200
pass in quick on eri0 proto udp from any port = ntp to eri0/32 port = ntp group 100

pass out quick on eri0 proto tcp from eri0/32 \
to any port = ssh flags S keep state group 200

pass out quick on eri0 proto tcp from eri0/32 \
to any port = http flags S keep state group 200
pass out quick on eri0 proto tcp from eri0/32 \
to any port = https flags S keep state group 200

pass out quick on eri0 proto tcp from eri0/32 \
to any port = smtp flags S keep state group 200


# pass icmp packets in and out
pass in quick on eri0 proto icmp from any to eri0/32  keep state group 100
```

EXEMPLE 26–26 Configuration d'un serveur IP Filter *(Suite)*

```
pass out quick on eri0 proto icmp from eri0/32 to any keep state group 200


# block and ignore NETBIOS packets
block in quick on eri0 proto tcp from any \
to any port = 135 flags S keep state group 100

block in quick on eri0 proto tcp from any port = 137 \
to any flags S keep state group 100
block in quick on eri0 proto udp from any to any port = 137 group 100
block in quick on eri0 proto udp from any port = 137 to any group 100

block in quick on eri0 proto tcp from any port = 138 \
to any flags S keep state group 100
block in quick on eri0 proto udp from any port = 138 to any group 100

block in quick on eri0 proto tcp from any port = 139 to any flags S keep state
group 100
block in quick on eri0 proto udp from any port = 139 to any group 100
```

EXEMPLE 26–27 Configuration d'un routeur IP Filter

Cet exemple présente la configuration d'un routeur possédant une interface interne, `ce0`, et une interface externe, `ce1`.

```
# internal interface is ce0 at 192.168.1.1
# external interface is ce1 IP obtained via DHCP
# block all packets and allow specific services
*** NAT ***
*** POOLS ***


# Short packets which are fragmented too short to be real.
block in log quick all with short


# By default, block and log everything.
block in log on ce0 all
block in log on ce1 all
block out log on ce0 all
block out log on ce1 all


# Packets going in/out of network interfaces that aren't on the loopback
# interface should not exist.
block in log quick on ce0 from 127.0.0.0/8 to any
block in log quick on ce0 from any to 127.0.0.0/8
block in log quick on ce1 from 127.0.0.0/8 to any
block in log quick on ce1 from any to 127.0.0.0/8


# Deny reserved addresses.
block in quick on ce1 from 10.0.0.0/8 to any
block in quick on ce1 from 172.16.0.0/12 to any
```

EXEMPLE 26–27 Configuration d'un routeur IP Filter *(Suite)*

```
block in log quick on ce1 from 192.168.1.0/24 to any
block in quick on ce1 from 192.168.0.0/16 to any


# Allow internal traffic
pass in quick on ce0 from 192.168.1.0/24 to 192.168.1.0/24
pass out quick on ce0 from 192.168.1.0/24 to 192.168.1.0/24


# Allow outgoing DNS requests from our servers on .1, .2, and .3
pass out quick on ce1 proto tcp/udp from ce1/32 to any port = domain keep state
pass in quick on ce0 proto tcp/udp from 192.168.1.2 to any port = domain keep state
pass in quick on ce0 proto tcp/udp from 192.168.1.3 to any port = domain keep state


# Allow NTP from any internal hosts to any external NTP server.
pass in quick on ce0 proto udp from 192.168.1.0/24 to any port = 123 keep state
pass out quick on ce1 proto udp from any to any port = 123 keep state


# Allow incoming mail
pass in quick on ce1 proto tcp from any to ce1/32 port = smtp keep state
pass in quick on ce1 proto tcp from any to ce1/32 port = smtp keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = smtp keep state


# Allow outgoing connections: SSH, WWW, NNTP, mail, whois
pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 22 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 22 keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 443 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 443 keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = nntp keep state
block in quick on ce1 proto tcp from any to any port = nntp keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = nntp keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = smtp keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = whois keep state
pass out quick on ce1 proto tcp from any to any port = whois keep state


# Allow ssh from offsite
pass in quick on ce1 proto tcp from any to ce1/32 port = 22 keep state


# Allow ping out
pass in quick on ce0 proto icmp all keep state
pass out quick on ce1 proto icmp all keep state


# allow auth out
```

EXEMPLE 26–27 Configuration d'un routeur IP Filter *(Suite)*

```
pass out quick on ce1 proto tcp from ce1/32 to any port = 113 keep state
pass out quick on ce1 proto tcp from ce1/32 port = 113 to any keep state


# return rst for incoming auth
block return-rst in quick on ce1 proto tcp from any to any port = 113 flags S/SA


# log and return reset for any TCP packets with S/SA
block return-rst in log on ce1 proto tcp from any to any flags S/SA


# return ICMP error packets for invalid UDP packets
block return-icmp(net-unr) in proto udp all
```

PARTIE V

Mobile IP

Cette partie constitue une introduction à Mobile IP (Mobile Internet Protocol, protocole Internet mobile) et répertorie les tâches relatives à l'administration de Mobile IP. L'installation de Mobile IP sur des systèmes d'ordinateurs portables et de communication sans fil leur permet de fonctionner sur des réseaux étrangers.

Remarque – La fonction Mobile IP a été supprimée de toutes les mises à jour Oracle Solaris depuis la version Solaris 10 8/07.

◆ ◆ ◆ CHAPITRE 27

Mobile IP (présentation)

Mobile IP (Internet Protocol) permet de transférer des informations entre ordinateurs portables. Par *ordinateurs portables*, il faut entendre ordinateurs portables et communications sans fil. Un ordinateur portable peut se placer sur un réseau étranger, sans perdre sa capacité à communiquer par le biais de son réseau d'accueil. L'implémentation Solaris de Mobile IP est compatible avec IPv4 uniquement.

Le présent chapitre contient les informations suivantes :

Pour les tâches relatives à Mobile IP, reportez-vous au Chapitre 28, "Administration de Mobile IP (tâches)". Pour obtenir des références sur Mobile IP, reportez-vous au Chapitre 29, "Fichiers et commandes de Mobile IP (références)".

Nouveautés de Mobile IP

La fonction Mobile IP est supprimée des mises à jour Solaris 10 depuis Solaris 10 8/07.

Introduction à Mobile IP

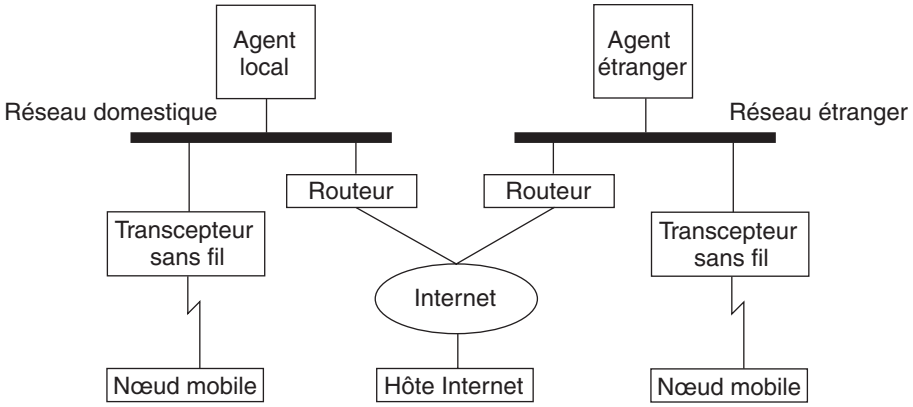
Les versions actuelles de l'IP (Internet Protocol) partent du principe que le point de connexion entre l'ordinateur et Internet ou un réseau est fixe. L'IP part également du principe que l'adresse IP de l'ordinateur permet d'identifier le réseau auquel est connecté l'ordinateur. Les datagrammes envoyés à un ordinateur sont basés sur les informations d'emplacement contenues dans l'adresse IP. Dans le cas de nombreux protocoles Internet, l'adresse IP du nœud n'est pas modifiée. Si l'un de ces protocoles est actif sur un périphérique informatique Mobile IP, cela entraîne un échec de leurs applications. Cela occasionnerait même l'échec du protocole HTTP si les connexions TCP n'étaient pas de nature si courte. La mise à jour d'une adresse IP et l'actualisation de la page Web ne sont pas des tâches complexes.

Si un ordinateur portable ou *nœud mobile* se déplace vers un nouveau réseau alors que son adresse IP ne change pas, l'adresse du nœud mobile ne reflète pas le nouveau point de connexion. Par conséquent, les protocoles de routage existants ne peuvent pas acheminer correctement les datagrammes vers le nœud mobile. Vous devez reconfigurer le nœud mobile avec une adresse IP qui représente le nouvel emplacement. L'attribution d'une adresse IP différente est une tâche fastidieuse. Par conséquent, sous l'IP actuel, si le nœud mobile se déplace sans modifier son adresse, le routage est perdu. Si le nœud mobile modifie son adresse, cela entraîne une perte des connexions.

Mobile IP permet de résoudre ce problème en autorisant le nœud mobile à utiliser deux adresses IP. La première adresse est une *adresse d'accueil* fixe. La seconde est une *adresse d'hébergement* qui change à chaque nouveau point de connexion. Mobile IP permet à un ordinateur de naviguer librement sur Internet. Mobile IP permet également à un ordinateur de naviguer librement sur le réseau d'une entreprise tout en conservant la même adresse d'accueil. Par conséquent, les activités de communication ne sont pas interrompues lorsque l'utilisateur modifie le point de connexion de l'ordinateur. En revanche, le réseau est mis à jour avec le nouvel emplacement du nœud mobile. Reportez-vous au Glossaire pour obtenir les définitions des termes associés à Mobile IP.

La figure suivante illustre la topologie générale de Mobile IP.

FIGURE 27–1 Topologie de Mobile IP



Grâce à l'utilisation de la topologie de Mobile IP de cette figure, le scénario suivant illustre le mode de déplacement d'un datagramme d'un point vers un autre au sein de la structure de Mobile IP :

1. L'hôte Internet envoie un datagramme au nœud mobile à l'aide de l'adresse d'accueil de ce dernier (processus de routage d'IP normal).
2. Si le nœud mobile se trouve dans son réseau d'accueil, le datagramme est livré par le biais du processus IP normal au nœud mobile. Autrement, l'agent d'accueil reçoit le datagramme.
3. Si le nœud mobile se trouve sur un réseau étranger, l'agent d'accueil transfère le datagramme vers ce dernier. L'agent d'accueil doit encapsuler le datagramme dans un datagramme externe de sorte que l'adresse IP de l'agent étranger s'affiche dans l'en-tête de l'IP externe.
4. L'agent étranger livre le datagramme au nœud mobile.
5. Les datagrammes sont envoyés à partir du nœud mobile vers l'hôte Internet selon les procédures de routage IP normales. Si le nœud mobile se trouve sur un réseau étranger, les paquets sont livrés à l'agent étranger. L'agent étranger transfère le datagramme vers l'hôte internet.
6. Dans les situations où le filtrage d'entrée est présent, l'adresse source doit être topologiquement correcte pour le sous-réseau dont provient le datagramme, sinon le routeur ne peut pas transférer le datagramme. Si c'est le cas pour des liens entre le nœud mobile et le nœud correspondant, l'agent étranger doit fournir un support de création de tunnel inverse. L'agent étranger peut ensuite livrer tous les datagrammes que le nœud mobile envoie à son agent d'accueil. L'agent d'accueil transfère ensuite le datagramme via le chemin qu'aurait emprunté ce dernier si le nœud mobile s'était trouvé sur le réseau d'accueil. Ce processus permet de garantir que l'adresse source est correcte pour tous les liens que doit traverser le datagramme.

En ce qui concerne les communications sans fil, la Figure 27–1 illustre l'utilisation de transducteurs pour la transmission des datagrammes vers le nœud mobile. En outre, tous les datagrammes entre l'hôte Internet et le nœud mobile utilisent l'adresse d'accueil du nœud

mobile. L'adresse d'accueil est utilisée même lorsque le nœud mobile se trouve dans le réseau étranger. L'adresse d'hébergement s'utilise uniquement pour communiquer avec les agents de mobilité. L'hôte Internet ne voit pas l'adresse d'hébergement.

Entités fonctionnelles de Mobile IP

Mobile IP présente les nouvelles entités fonctionnelles suivantes :

- **Nœud mobile** – Hôte ou routeur qui change son point de connexion d'un réseau à un autre tout en conservant la totalité des communications existantes à l'aide de son adresse IP d'accueil.
- **Agent d'accueil** – Routeur ou serveur se trouvant sur le réseau d'accueil du nœud mobile. Le routeur intercepte les datagrammes destinés au nœud mobile. Il livre ensuite les datagrammes via l'adresse d'hébergement. L'agent d'accueil gère également les informations actuelles à l'emplacement du nœud mobile.
- **Agent étranger** – Routeur ou serveur situé sur le réseau étranger visité par le nœud mobile. Fournit un service de routage d'hôtes au nœud mobile. L'agent étranger peut également fournir une adresse d'hébergement au nœud mobile pendant l'enregistrement de ce dernier.

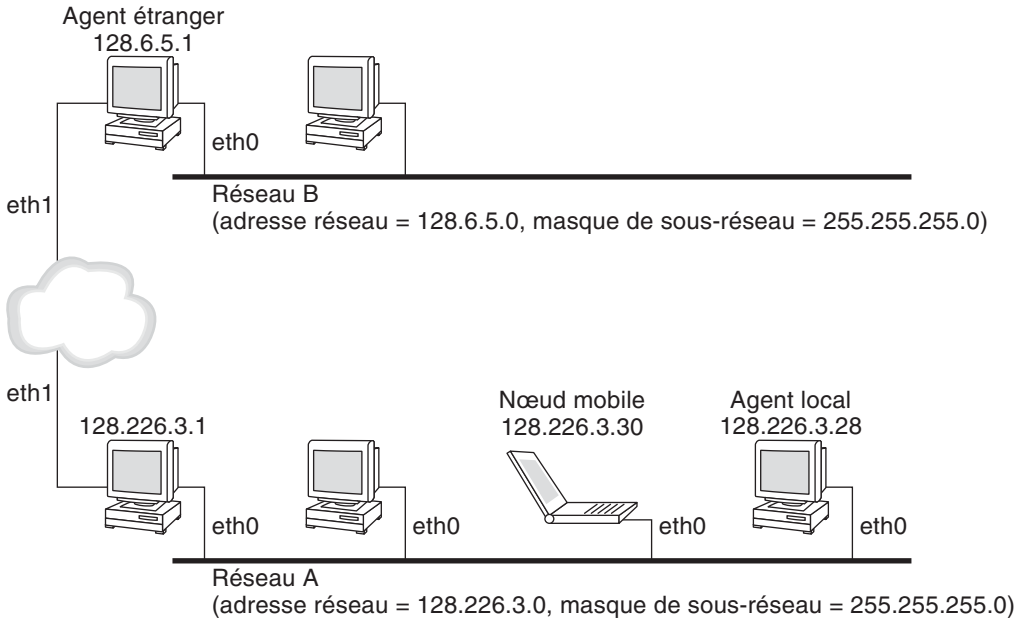
Mode de fonctionnement de Mobile IP

Mobile IP permet d'acheminer des datagrammes IP vers les nœuds mobiles. L'adresse d'accueil du nœud mobile identifie toujours ce dernier, quel que soit son point de connexion. En cas d'absence, une adresse d'hébergement est associée à l'adresse d'accueil du nœud mobile. L'adresse d'hébergement fournit les informations relatives au point de connexion actuel du nœud mobile. Mobile IP utilise un mécanisme d'enregistrement pour enregistrer l'adresse d'hébergement avec un agent d'accueil.

L'agent d'accueil redirige les datagrammes provenant du réseau d'accueil vers l'adresse d'hébergement. L'agent d'accueil construit un nouvel en-tête IP qui contient l'adresse d'hébergement du nœud mobile en tant qu'adresse IP de destination. Ce nouvel en-tête encapsule le datagramme IP d'origine. Par conséquent, l'adresse d'accueil du nœud mobile n'a aucune incidence sur l'acheminement du datagramme encapsulé jusqu'à ce que ce dernier parvienne à l'adresse d'hébergement. Ce type d'encapsulation correspond à la *création de tunnel*. Lorsque le datagramme parvient à l'adresse d'hébergement, il est désencapsulé. Le datagramme est ensuite livré au nœud mobile.

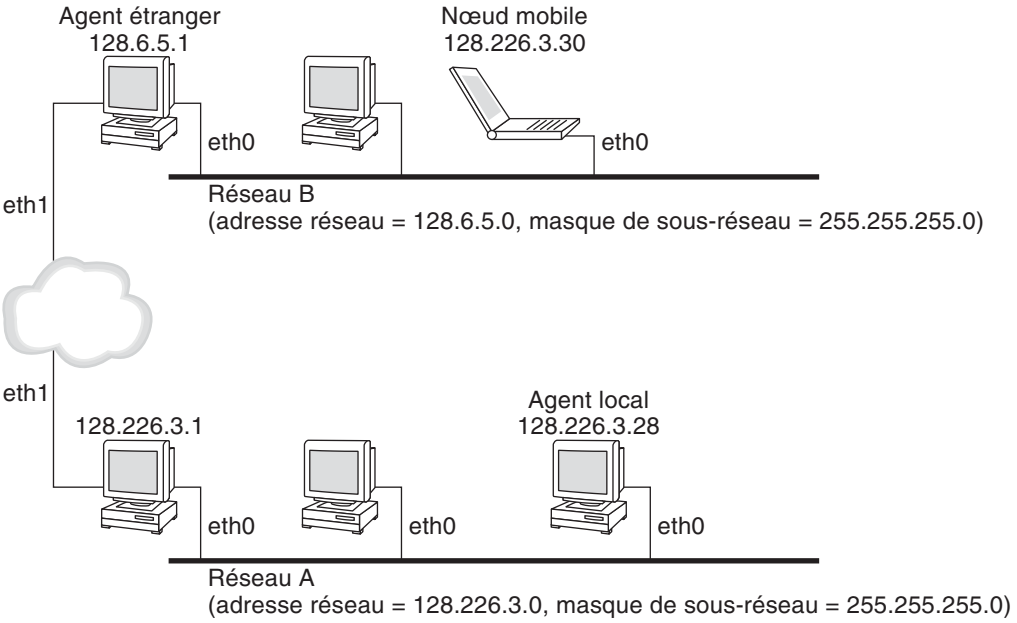
La figure suivante représente un nœud mobile qui réside sur son réseau d'accueil, le réseau A, avant d'être déplacé vers un réseau étranger, le réseau B. Mobile IP est pris en charge par les deux réseaux. Le nœud mobile est toujours associé à son adresse d'accueil, `128.226.3.30`.

FIGURE 27–2 Nœud mobile résidant sur son réseau d'accueil



La figure suivante représente un nœud mobile qui s'est déplacé vers un réseau étranger, le réseau B. Les datagrammes destinés au nœud mobile sont interceptés par l'agent d'accueil du réseau d'accueil, soit le réseau A. Les datagrammes sont encapsulés. Ils sont ensuite envoyés à l'agent étranger du réseau B. L'agent étranger retire ensuite l'en-tête externe. L'agent étranger livre ensuite le datagramme au nœud mobile situé sur le réseau B.

FIGURE 27–3 Nœud mobile se déplaçant vers un réseau étranger



L'adresse d'hébergement peut appartenir à un agent étranger. Le nœud mobile peut obtenir l'adresse d'hébergement par le biais du protocole DHCP (Dynamic Host Configuration Protocol) ou PPP (Point-to-Point Protocol). Dans le deuxième cas, le nœud mobile possède une adresse d'hébergement colocalisée.

Les agents de mobilité (agents d'accueil et étrangers) indiquent leur présence à l'aide de messages *de publication d'agent.* Au besoin, un nœud mobile peut également demander un message de publication d'agent. Le nœud mobile utilise un agent de mobilité connecté localement via un message de *demande d'agent.* Un nœud mobile utilise les publications d'agent afin de déterminer s'il se trouve sur le réseau d'accueil ou sur un réseau étranger.

Le nœud mobile utilise un processus d'enregistrement spécial afin d'informer l'agent d'accueil à propos de l'emplacement actuel du nœud mobile. Le nœud mobile est toujours "à l'écoute" des agents de mobilité au cas où ils l'informeraient de leur présence. Le nœud mobile utilise ces publications afin de déterminer le moment où se déplacer vers un autre sous-réseau. Lorsqu'un nœud mobile détermine qu'il a changé d'emplacement, il utilise le nouvel agent étranger pour transférer un message d'enregistrement vers l'agent d'accueil. Le nœud mobile utilise le même processus lorsqu'il se déplace d'un réseau étranger vers un autre.

Lorsque le nœud mobile détecte qu'il est situé sur le réseau d'accueil, il n'utilise pas les services de mobilité. Lorsque le nœud mobile revient sur le réseau d'accueil, il se *désenregistre* auprès de l'agent d'accueil.

Détection d'un agent

Un nœud mobile emploie la méthode appelée *détection d'agent* afin de déterminer les informations suivantes :

- le moment où le nœud s'est déplacé d'un réseau vers un autre ;
- si le réseau est le réseau d'accueil ou un réseau étranger ;
- l'adresse d'hébergement de l'agent étranger proposée par chaque agent étranger sur ce réseau ;
- les services de mobilité fournis par l'agent de mobilité, publiés en tant qu'indicateurs, ainsi que les extensions supplémentaires dans la publication d'agent.

Les agents de mobilité transmettent les *publications d'agents* afin de publier les services sur un réseau. En l'absence de publication d'agent, un nœud mobile peut demander des publications. Cette capacité est également appelée *demande d'agent*. Si un nœud mobile est capable de prendre en charge sa propre adresse d'hébergement colocalisée, il peut utiliser les publications de routeur habituelles dans le même objectif.

Publication d'agent

Les nœuds mobiles utilisent la publication d'agent afin de déterminer le point actuel de connexion à Internet ou au réseau d'une entreprise. Une publication d'agent correspond à une publication de routeur ICMP (Internet Control Message Protocol) qui a été étendue afin de porter une extension de publication d'agent de mobilité.

Un agent étranger peut être trop occupé pour pouvoir servir des nœuds mobiles supplémentaires. Cependant, un agent étranger doit continuer d'envoyer des publications d'agent. Ensuite, le nœud mobile, qui est déjà enregistré auprès d'un agent étranger, sait qu'il est toujours à la portée de l'agent étranger. Le nœud mobile sait également que l'agent étranger n'a pas échoué. Il est probable qu'un nœud mobile enregistré avec un agent étranger dont il ne reçoit plus de publication d'agents sache qu'il ne peut plus contacter cet agent.

Publication d'agents sur interfaces dynamiques

Vous pouvez configurer l'implémentation de l'agent étranger de sorte qu'il envoie des publications à des interfaces créées de façon dynamique. Vous pouvez également activer ou désactiver les publications non sollicitées limitées par le biais des interfaces ad hoc. Les interfaces créées de manière dynamique sont définies comme étant uniquement les interfaces configurées après le démarrage du démon `mipagent`. La publication sur interface dynamique est utile pour les applications prenant en charge les interfaces de mobilité transitoire. En outre, la limitation des publications non sollicitées permet de réaliser des économies de bande passante de réseau.

Demande d'agent

Chaque nœud mobile doit implémenter la demande d'agent. Pour la demande d'agents, le nœud mobile utilise les procédures, paramètres par défaut et constantes spécifiés par les routeurs ICMP pour les messages de demande.

Le nœud mobile limite la fréquence à laquelle il envoie ses demandes. Il peut envoyer trois demandes initiales à une fréquence maximale d'une demande par seconde pendant qu'il recherche un agent. Une fois le nœud mobile enregistré auprès d'un agent, la fréquence d'envoi des demandes est réduite afin de limiter le temps système du réseau local.

Adresses d'hébergement

Mobile IP propose les autres modes d'acquisition suivants pour l'acquisition d'une adresse d'hébergement :

- Un agent étranger fournit une *adresse d'hébergement d'agent étranger* qui est publiée sur le nœud mobile par le biais de messages de publication d'agent. En règle générale, l'adresse d'hébergement correspond à l'adresse IP de l'agent étranger qui envoie les publications. L'agent étranger constitue le point d'extrémité du tunnel. Lorsque l'agent étranger reçoit des datagrammes par le biais d'un tunnel, il les désencapsule. Ensuite, l'agent étranger livre le datagramme interne au nœud mobile. Par conséquent, de nombreux nœuds mobiles peuvent partager la même adresse d'hébergement. La bande passante est importante pour les liens sans fil. Les liens sans fil sont de bons candidats à partir desquels les agents étrangers peuvent fournir des services Mobile IP à des liens connectés à une bande passante plus importante.
- Un nœud mobile acquiert une *adresse d'hébergement colocalisée* en tant qu'adresse IP locale par des moyens externes. Le nœud mobile s'associe alors à l'une de ses propres interfaces réseau. Le nœud mobile peut acquérir une adresse temporaire via DHCP. L'adresse peut également correspondre à l'adresse à long terme du nœud mobile. Cependant, le nœud mobile peut utiliser l'adresse uniquement en cas de visite dans le sous-réseau auquel appartient l'adresse d'hébergement. En cas d'utilisation d'une adresse d'hébergement colocalisée, le nœud mobile sert de point d'extrémité du tunnel. Le nœud mobile désencapsule les datagrammes acheminés via le tunnel au nœud mobile.

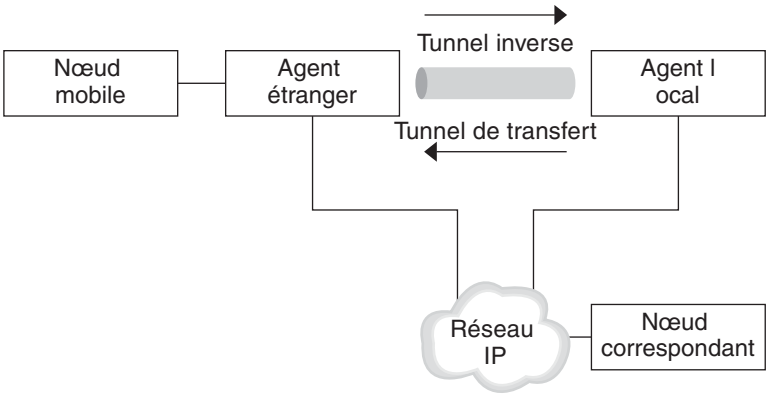
Une adresse d'hébergement colocalisée permet à un nœud mobile de fonctionner sans agent étranger. Par conséquent, un nœud mobile peut utiliser une adresse d'hébergement colocalisée dans des réseaux n'ayant pas déployé d'agent étranger.

S'il utilise une adresse d'hébergement colocalisée, le nœud mobile doit se trouver sur le lien identifié par le préfixe réseau de l'adresse d'hébergement. Autrement, la livraison des datagrammes destinés à l'adresse d'hébergement est impossible.

Mobile IP avec création de tunnel inverse

La section "Mode de fonctionnement de Mobile IP" à la page 708 part du principe que le routage au sein d'Internet est indépendant de l'adresse source du datagramme. Les routeurs intermédiaires peuvent cependant effectuer une vérification pour une adresse source topologiquement correcte. En cas de vérification d'un routeur intermédiaire, le nœud mobile doit définir un tunnel inverse. En configurant un tunnel inverse entre l'adresse d'hébergement et l'agent d'accueil, vous garantissez que l'adresse source du paquet de données IP est correcte au point de vue de la topologie. La prise en charge des tunnels inverses est publiée par les agents étrangers et les agents d'accueil. Un nœud mobile peut émettre une demande de tunnel inverse entre l'agent étranger et l'agent d'accueil lors de son enregistrement. Un tunnel inverse commence à l'adresse d'hébergement du nœud mobile et se termine à l'agent d'accueil. La figure suivante illustre la topologie de Mobile IP utilisant un tunnel inverse.

FIGURE 27–4 Mobile IP avec tunnel inverse



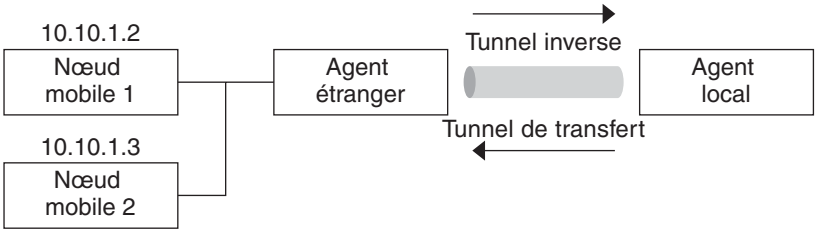
Prise en charge des adresses privées limitées

Les nœuds mobiles dont les adresses privées ne sont pas globalement routables via Internet doivent disposer de tunnels inverses. Mobile IP Solaris assure la prise en charge des nœuds mobiles dont les adresses sont privées. Reportez-vous à "Présentation de l'implémentation de Mobile IP Solaris" à la page 739 pour connaître les fonctions que Mobile IP Solaris ne prend pas en charge.

Les entreprises utilisent des adresses privées lorsque la connectivité externe n'est pas requise. Les adresses privées ne sont pas routables via Internet. Lorsqu'un nœud mobile possède une adresse privée, il ne peut communiquer avec un nœud correspondant que si ses datagrammes sont acheminés vers l'agent d'accueil par le biais du tunnel inverse. L'agent d'accueil livre ensuite le datagramme au nœud correspondant de la manière dont il est normalement livré lorsque le nœud mobile se trouve en accueil. La figure suivante illustre une topologie de réseau

avec deux nœuds mobiles possédant des adresses privées. Les deux nœuds mobiles utilisent la même adresse d'hébergement lorsqu'ils sont enregistrés auprès du même agent étranger.

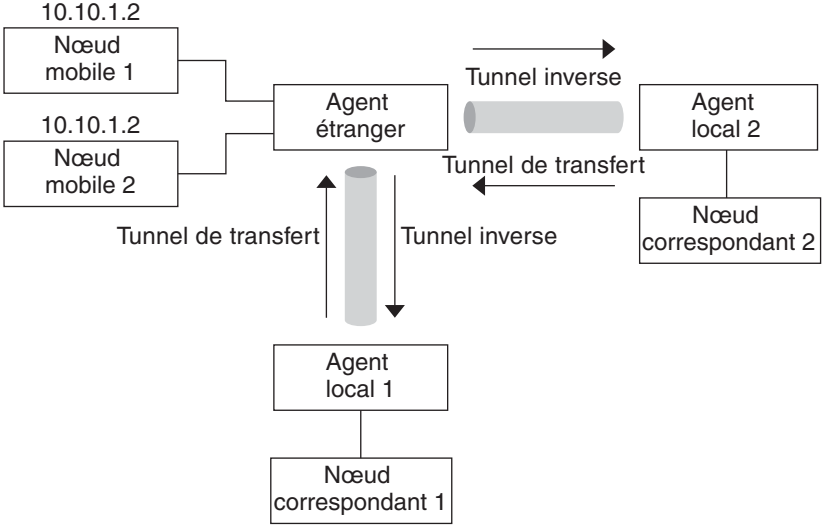
FIGURE 27–5 Nœuds mobiles possédant des adresses privées résidant sur le même réseau étranger



L'adresse d'hébergement et l'adresse de l'agent d'accueil doivent être globalement routables si elles appartiennent à des domaines différents connectés via un Internet public.

Le même réseau étranger peut comprendre deux nœuds mobiles pour lesquels la même adresse IP sert d'adresse privée. Cependant, chaque nœud mobile doit posséder un agent d'accueil différent. En outre, chaque nœud mobile doit se trouver sur un sous-réseau de publication distinct appartenant à un agent étranger unique. La figure suivante illustre une topologie de réseau correspondant à cette situation.

FIGURE 27–6 Nœuds mobiles possédant des adresses privées et résidant sur des réseaux étrangers différents



Enregistrement de Mobile IP

Les nœuds mobiles détectent le moment où ils ont été déplacés d'un sous-réseau vers un autre grâce à la publication d'agent. Lorsqu'il reçoit une publication d'agent indiquant le changement de son emplacement, le nœud mobile s'enregistre par le biais d'un agent étranger. Même s'il est possible que le nœud mobile ait pu acquérir sa propre adresse d'hébergement colocalisée, cette fonction permet de restreindre l'accès aux services de mobilité.

L'enregistrement de Mobile IP fournit un mécanisme flexible permettant aux nœuds mobiles de communiquer les informations relatives à la disponibilité de l'agent d'accueil. Le processus d'enregistrement permet aux nœuds mobiles d'effectuer les tâches suivantes :

- demander des services de transfert lors de la visite d'un réseau étranger ;
- informer l'agent d'accueil de la nouvelle adresse d'hébergement ;
- renouveler une inscription qui est sur le point d'expirer ;
- se désenregister lors du retour du nœud mobile à l'accueil ;
- effectuer une requête pour un tunnel inverse.

Les messages d'enregistrement permettent l'échange d'informations entre un nœud mobile, un agent étranger et l'agent d'accueil. L'enregistrement permet de créer ou de modifier un lien de mobilité au niveau de l'agent d'accueil. L'enregistrement associe l'adresse d'accueil du nœud mobile à l'adresse d'hébergement de ce dernier pour une durée prédéterminée.

Le processus d'enregistrement permet également aux nœuds mobiles d'effectuer les opérations suivantes :

- enregistrement avec plusieurs agents étrangers ;
- désenregistrement d'adresses d'hébergement spécifiques tout en conservant d'autres liens de mobilité ;
- obtention de l'adresse d'un agent d'accueil si le nœud mobile n'est pas configuré avec ces informations.

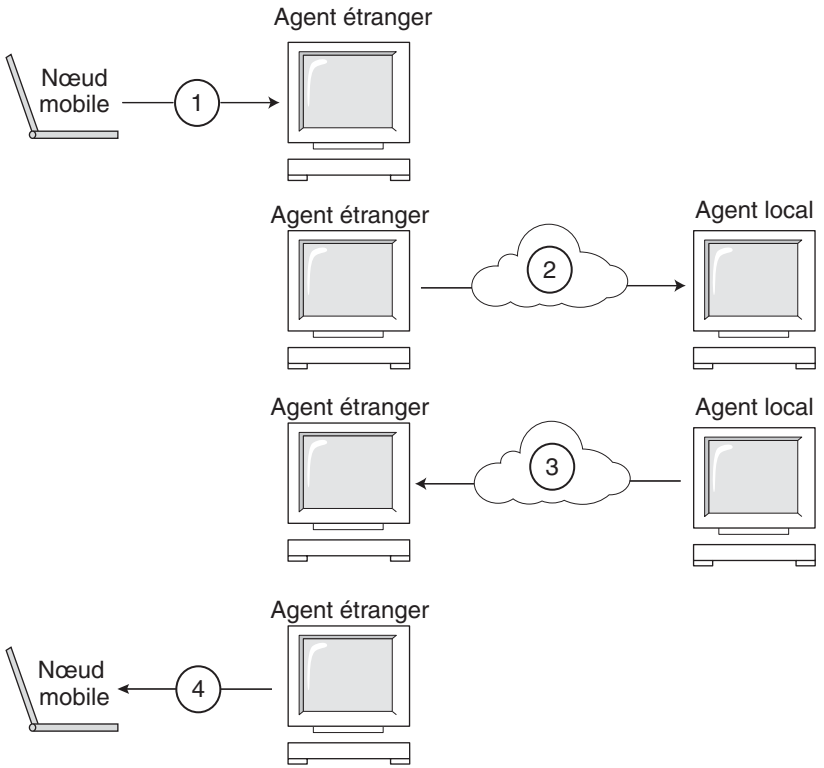
Mobile IP définit les processus d'enregistrement suivants pour un nœud mobile :

- Si un nœud mobile enregistre l'adresse d'hébergement d'un agent étranger, il informe l'agent d'accueil qu'il est accessible par le biais de cet agent étranger.
- Si un nœud mobile reçoit une publication d'agent requérant son enregistrement par le biais d'un agent étranger, il peut tenter d'obtenir une adresse d'hébergement colocalisée. Le nœud mobile peut également s'enregistrer auprès de cet agent étranger ou de tout autre agent étranger situé sur ce lien.
- Si un nœud mobile utilise une adresse d'hébergement colocalisée, il s'enregistre directement auprès de l'agent d'accueil.
- Si un nœud mobile retourne sur le réseau d'accueil, il se désenregistre auprès de l'agent d'accueil.

Ces processus d'enregistrement impliquent un échange de requêtes d'enregistrement et de messages de réponse d'enregistrement. Lorsque le nœud mobile s'enregistre à l'aide d'un agent étranger, le processus d'enregistrement effectue les étapes suivantes, représentées par la figure ci-desous :

1. Le nœud mobile envoie une demande d'enregistrement à l'agent étranger adéquat pour qu'il démarre le processus d'enregistrement.
2. L'agent étranger traite la demande d'enregistrement, puis relaie la demande auprès de l'agent d'accueil.
3. L'agent d'accueil envoie une réponse d'enregistrement à l'agent étranger afin d'accepter ou de refuser la demande.
4. L'agent étranger traite la réponse d'enregistrement, puis la relaie auprès du nœud mobile afin de l'informer du traitement de la demande.

FIGURE 27–7 Processus d'enregistrement de Mobile IP



Lorsque le nœud mobile s'enregistre directement auprès de l'agent d'accueil, le processus d'enregistrement nécessite les étapes suivantes uniquement :

- Le nœud mobile envoie une demande d'enregistrement à l'agent d'accueil.
- L'agent d'accueil envoie une réponse d'enregistrement au nœud mobile qui accepte ou refuse la demande.

De plus, l'agent étranger ou l'agent d'accueil peut nécessiter un tunnel inverse. Si l'agent étranger prend en charge la création de tunnels inverse, le nœud mobile utilise le processus d'enregistrement pour demander un tunnel inverse. Le nœud mobile définit l'indicateur de tunnel inverse dans la demande d'enregistrement de sorte qu'il effectue une demande de tunnel inverse.

NAI (Network Access Identifier, identificateur d'accès au réseau)

Lorsqu'ils sont utilisés sur Internet, les serveurs AAA (Authentication, Autorization, and Accounting ; authentification, autorisation et comptabilisation) offrent des services d'authentification et d'autorisation aux ordinateurs à connexion téléphonique. ll est possible que ces services soient tout aussi importants pour les nœuds mobiles faisant appel à Mobile IP lorsqu'ils essaient de se connecter à des domaines étrangers avec des serveurs AAA. Les NAI permettent aux serveurs AAA d'identifier des clients. Un nœud mobile peut s'identifier en incluant les NAI dans la demande d'enregistrement de Mobile IP.

Dans la mesure où, en règle générale, un NAI identifie le nœud mobile de façon unique, l'adresse d'accueil du nœud mobile n'est pas toujours nécessaire à l'obtention de cette fonction. Par conséquent, un nœud mobile peut s'authentifier lui-même. Ainsi, un nœud mobile peut obtenir une autorisation de connexion à un domaine étranger sans même posséder une adresse d'accueil. Pour demander l'attribution d'une adresse d'accueil, un message contenant l'extension NAI du nœud mobile peut définir le champ d'adresse d'accueil à zéro dans la demande d'enregistrement.

Authentification de message de Mobile IP

Chaque nœud mobile, d'agent étranger et d'agent d'accueil assure la prise en charge d'une association de sécurité de mobilité entre les différents composants de Mobile IP. L'association de sécurité est indexée par le SPI et l'adresse IP. Dans l'instance du nœud mobile, cette adresse correspond à l'adresse d'accueil de ce dernier. Les messages d'enregistrement entre un nœud mobile et l'agent d'accueil sont authentifiés par l'extension d'authentification mobile-accueil. En plus de l'authentification mobile-accueil obligatoire, vous pouvez utiliser les authentifications facultatives agent mobile-étranger et agent d'accueil-étranger.

Demande d'enregistrement de nœud mobile

Un nœud mobile utilise un message de *demande d'enregistrement* pour s'enregistrer auprès de l'agent d'accueil. Ainsi, l'agent d'accueil peut créer ou modifier un lien de mobilité pour ce nœud mobile, en lui attribuant par exemple une nouvelle durée de vie. L'agent étranger peut relayer la demande d'enregistrement vers l'agent d'accueil. Cependant, si le nœud mobile enregistre une adresse d'hébergement colocalisée, il peut alors envoyer la demande d'enregistrement directement à l'agent d'accueil. Si l'agent étranger indique que les messages d'enregistrement doivent être envoyés à l'agent étranger, le nœud mobile doit alors envoyer la demande d'enregistrement à l'agent étranger.

Message de réponse d'enregistrement

Un agent de mobilité renvoie un message de *réponse d'enregistrement* à un nœud mobile ayant envoyé un message de demande d'enregistrement. Si le nœud mobile demande un service venant d'un agent étranger, ce dernier reçoit la réponse de l'agent d'accueil. Par conséquent, l'agent étranger relaie la réponse vers le nœud mobile. Le message de réponse contient les codes nécessaires permettant d'informer le nœud mobile et l'agent étranger du statut de la demande d'enregistrement. Le message contient également la durée de vie accordée à l'agent d'accueil. La durée de vie peut être inférieure à la demande originale. La réponse d'enregistrement peut également contenir une assignation d'adresse d'accueil dynamique.

Considérations relatives aux agents étrangers

La plupart du temps, l'agent étranger joue un rôle passif dans l'enregistrement Mobile IP. L'agent étranger ajoute tous les nœuds mobiles enregistrés dans la table de visiteurs. L'agent étranger relaie les demandes d'enregistrement entre les nœuds mobiles et les agents d'accueil. De plus, lorsque l'agent étranger fournit l'adresse d'hébergement, ce dernier désencapsule les datagrammes en vue d'une livraison au nœud mobile. L'agent étranger envoie également des messages périodiques de publication d'agent pour informer de sa présence.

Si les agents d'accueil et étrangers prennent en charge les tunnels inverses et si le nœud mobile demande un tunnel de retour, l'agent étranger achemine l'ensemble des paquets à partir du nœud mobile vers l'agent d'accueil. L'agent d'accueil envoie alors les paquets au nœud correspondant. Ce processus est l'inverse de celui où l'agent d'accueil achemine tous les paquets du nœud mobile vers l'agent étranger en vue d'une livraison au nœud mobile. Un agent étranger qui prend en charge les tunnels inverses indique que ces derniers sont pris en charge pour l'enregistrement. Selon la stratégie locale, l'agent étranger peut refuser une demande d'enregistrement en l'absence de définition d'indicateur de tunnel inverse. L'agent étranger peut distinguer plusieurs nœuds mobiles avec la même adresse IP (privée) uniquement lorsque ces derniers visitent différentes interfaces sur l'agent étranger. Dans le cas d'un tunnel d'acheminement, l'agent étranger fait la distinction entre plusieurs nœuds mobiles partageant la

même adresse privée en consultant l'interface du tunnel entrant. L'interface du tunnel entrant mappe vers une adresse d'agent d'accueil unique.

Considérations relatives aux agents d'accueil

Les agents d'accueil jouent un rôle actif dans le processus d'enregistrement. L'agent d'accueil reçoit les demandes d'enregistrement provenant du nœud mobile. La demande d'enregistrement peut être transmise à l'agent étranger. L'agent d'accueil met à jour les enregistrements des liens de mobilité pour ce nœud mobile. Il émet une réponse d'enregistrement adaptée à chaque demande. De plus, il transfère les paquets vers le nœud mobile lorsque celui-ci ne se trouve pas dans le réseau d'accueil.

Un agent d'accueil peut ne pas posséder de sous-réseau configuré pour les nœuds mobiles. Cependant, l'agent d'accueil doit reconnaître l'adresse d'accueil du nœud mobile par le biais du fichier `mipagent.conf` ou d'un autre mécanisme lorsqu'il autorise un enregistrement. Pour de plus amples informations sur le fichier `mipagent.conf`, reportez-vous à la section "Création du fichier de configuration de Mobile IP" à la page 724.

Un agent d'accueil peut prendre en charge des nœuds mobiles disposant d'une adresse privée en les configurant dans le fichier `mipagent.conf`. Les adresses d'accueil utilisées par l'agent d'accueil doivent être uniques.

Détection dynamique d'agent d'accueil

Dans certains cas, le nœud mobile peut ne pas connaître l'adresse de l'agent d'accueil lorsqu'il tente de s'enregistrer. Si le nœud mobile ne possède pas l'adresse de l'agent d'accueil, il peut utiliser la résolution dynamique d'adresse d'agent d'accueil pour la connaître. Dans ce cas, le nœud mobile définit le champ de l'agent d'accueil de la demande d'enregistrement à l'adresse de diffusion destinée au sous-réseau de son réseau d'accueil. Chaque agent d'accueil qui reçoit une demande d'enregistrement avec une adresse de destination de diffusion refuse l'enregistrement du nœud mobile en envoyant une réponse de refus d'enregistrement. Ce faisant, le nœud mobile peut utiliser l'adresse IP unicast de l'agent d'accueil indiquée dans la réponse négative lors de la prochaine tentative d'enregistrement.

Routage de datagrammes vers et à partir de nœuds mobiles

Cette section décrit le mode de coopération entre les nœuds mobiles, les agents d'accueil et les agents étrangers afin d'acheminer les datagrammes vers les nœuds mobiles connectés à un réseau étranger. Reportez-vous à "Présentation de l'implémentation de Mobile IP Solaris" à la page 739 pour obtenir des informations sur les fonctions de Mobile IP prises en charge par le système d'exploitation Solaris.

Méthodes d'encapsulation

Les agents d'accueil et étrangers utilisent l'une des méthodes d'encapsulation disponibles pour la prise en charge des datagrammes utilisant un tunnel. Les méthodes d'encapsulation définies sont l'encapsulation IP dans IP, l'encapsulation minimale et l'encapsulation de routage générique. Les cas d'agents étrangers et d'accueil, ou de nœuds mobiles indirects colocalisés et d'agents d'accueil, doivent prendre en charge la même méthode d'encapsulation. Toutes les entités de Mobile IP doivent obligatoirement prendre en charge l'encapsulation IP dans IP .

Routage de datagramme de monodiffusion

Lors de son enregistrement sur un réseau étranger, le nœud mobile choisit un routeur par défaut en fonction des règles suivantes :

- Si le nœud mobile est enregistré et utilise l'adresse d'hébergement d'un agent étranger, le processus est relativement simple. Le nœud mobile choisit son routeur par défaut parmi les adresses de routeur publiées dans la partie publication du routeur ICMP de la publication de cet agent. Il peut également considérer l'adresse IP source de la publication d'agent comme un autre choix possible d'adresse IP de routeur par défaut.
- Le nœud mobile peut être enregistré directement auprès de l'agent d'accueil à l'aide d'une adresse d'hébergement colocalisée. Ensuite, le nœud mobile sélectionne son routeur par défaut parmi ceux qui sont publiés dans tout message de publication de routeur ICMP qu'il est susceptible de recevoir. Le préfixe réseau du routeur par défaut sélectionné doit correspondre au préfixe réseau de l'adresse d'hébergement du nœud mobile provenant d'une source externe. L'adresse peut correspondre à l'adresse IP source de la publication d'agent sous le préfixe réseau. Ensuite, le nœud mobile peut également considérer que l'adresse IP source est un autre choix possible pour l'adresse IP d'un routeur par défaut.
- Si le nœud mobile est enregistré, un agent étranger qui prend en charge les tunnels inverses achemine les datagrammes de monodiffusion à partir du nœud mobile vers l'agent d'accueil via le tunnel inverse. S'il est enregistré avec un agent étranger qui assure la prise en charge de tunnel inverse, le nœud mobile doit utiliser cet agent étranger en tant que routeur par défaut.

Datagrammes de diffusion

Lorsqu'un agent d'accueil reçoit un datagramme de diffusion ou de multidiffusion, il le transfère uniquement vers les nœuds mobiles qui ont indiqué spécifiquement qu'ils souhaitent recevoir des datagrammes. Le mode de transmission des datagrammes de diffusion et multidiffusion vers les nœuds mobiles dépend principalement de deux facteurs. Le nœud mobile utilise soit une adresse d'hébergement fournie par un agent étranger, soit sa propre adresse d'hébergement colocalisée. Dans le premier cas, cela signifie qu'une double encapsulation du datagramme est nécessaire. Le premier en-tête IP identifie le nœud mobile auquel le datagramme doit être livré.

Cet en-tête ne se trouve pas dans le datagramme de diffusion ou de multidiffusion. Le second en-tête IP identifie l'adresse d'hébergement et constitue l'en-tête de tunnel habituel. Dans le deuxième cas, le nœud mobile décapsule ses propres datagrammes et il suffit d'envoyer le datagramme via le tunnel habituel.

Routage de datagramme de multidiffusion

Pour recevoir du trafic de multidiffusion lorsqu'il visite un sous-réseau étranger, un nœud mobile peut rejoindre un groupe de multidiffusion de l'une des manières suivantes :

- Si le nœud mobile utilise une adresse d'hébergement colocalisée, il peut utiliser celle-ci en tant qu'adresse IP source de tout message IGMP (Internet Group Management Protocol). Cependant, le sous-réseau visité doit disposer d'un routeur de multidiffusion.
- Si le nœud mobile souhaite rejoindre le groupe ICMP de son sous-réseau d'accueil, il doit utiliser un tunnel inverse pour envoyer des messages IGMP à l'agent d'accueil. Cependant, l'agent d'accueil du nœud mobile doit être un routeur de multidiffusion. L'agent d'accueil transfère ensuite les datagrammes de multidiffusion via le tunnel vers le nœud mobile.
- Si le nœud mobile utilise une adresse d'hébergement colocalisée, il peut utiliser cette adresse en tant qu'adresse IP source de tout message d'adhésion IGMP. Cependant, le sous-réseau visité doit disposer d'un routeur de multidiffusion. Lorsque le nœud mobile a rejoint le groupe, il peut participer en envoyant ses propres paquets de multidiffusion directement sur le réseau visité.
- Effectuer un envoi directement sur le réseau visité.
- Effectuer un envoi vers l'agent d'accueil via un tunnel.

Le routage multidiffusion dépend de l'adresse IP source. Un nœud mobile qui envoie un datagramme de multidiffusion doit l'envoyer à partir d'une adresse source valide sur ce lien. Ainsi, un nœud mobile qui envoie des datagrammes de multidiffusion directement sur le réseau visité doit utiliser une adresse d'hébergement colocalisée en guise d'adresse IP source. De plus, le nœud mobile doit faire partie du groupe de multidiffusion associé à l'adresse. De même, un nœud mobile qui a rejoint un groupe de multidiffusion alors qu'il était sur son sous-réseau d'accueil avant d'effectuer un roaming, ou pendant un roaming dans un tunnel inverse vers son agent d'accueil, doit utiliser son adresse d'accueil en guise d'adresse IP source du datagramme de multidiffusion. Par conséquent, les datagrammes de ce nœud mobile doivent également être acheminés via un tunnel inverse vers son sous-réseau d'accueil, soit à l'aide de son adresse d'hébergement colocalisée, soit par le biais d'un tunnel inverse d'agent étranger.

Bien qu'une adhésion systématique au sous-réseau qu'il visite semble plus efficace, un nœud mobile reste ce qu'il est. Par conséquent, il devrait répéter l'adhésion à chaque fois qu'il change de sous-réseau. Le mode d'adhésion le plus efficace du nœud mobile s'effectue par le biais de son agent d'accueil, ce qui représente une économie de temps système. De plus, des sessions de multidiffusion disponibles uniquement via le sous-réseau d'accueil pourraient être présentes. D'autres considérations peuvent également forcer le nœud mobile à participer d'une façon spécifique.

Considérations relatives à la sécurité de Mobile IP

Dans de nombreux cas, les ordinateurs portables utilisent des liens sans fil pour se connecter au réseau. Les liens sans fil sont particulièrement vulnérables à l'écoute passive, aux attaques de rediffusion active et autres attaques actives.

Dans la mesure où Mobile IP reconnaît son incapacité à réduire ou éliminer cette faiblesse, une forme d'authentification permet de protéger les messages d'enregistrement Mobile IP de ce type d'attaques. L'algorithme par défaut utilisé est MD5 avec une taille de clé de 128 octets. Le mode d'opération par défaut exige que cette clé de 128 octets précède et suive les données à hacher. L'agent étranger utilise MD5 pour la prise en charge de l'authentification. Il utilise également des clés d'une taille minimale de 128 octets, avec distribution de clé manuelle. Mobile IP peut prendre en charge d'autres algorithmes d'authentification, modes d'algorithmes, méthodes de distribution de clé et tailles de clé.

Ces méthodes empêchent les modifications sur les messages d'enregistrement Mobile IP. Cependant, Mobile IP utilise une forme de protection contre la rediffusion afin d'alerter les entités Mobile IP dans le cas où elles recevraient des duplicatas de messages d'enregistrement précédents. Sans cette méthode de protection, le nœud mobile et son agent d'accueil pourraient se désynchroniser si l'un d'entre eux recevait un message d'enregistrement. Ainsi, Mobile IP met son état à jour. Par exemple, un agent d'accueil reçoit le duplicata d'un message de désenregistrement alors que le nœud mobile est enregistré via un agent étranger.

La protection contre la rediffusion est assurée par les méthodes connues sous les noms de *nonce* ou *horodatage*. Les agents d'accueil et les nœuds mobiles échangent les nonces et les horodatages au sein des messages d'enregistrement Mobile IP. Les nonces et les horodatages sont protégés contre les modifications par un mécanisme d'authentification. Par conséquent, si un agent d'accueil ou un nœud mobile reçoit un message dupliqué, ce message peut être rejeté.

L'utilisation de tunnels peut constituer une vulnérabilité importante, tout particulièrement si l'enregistrement n'est pas authentifié. En outre, l'ARP (Address Resolution Protocol) n'est pas authentifié et peut être utilisé pour voler le trafic d'un autre hôte.

◆ ◆ ◆ CHAPITRE 28

Administration de Mobile IP (tâches)

Ce chapitre décrit les procédures permettant de modifier, ajouter, supprimer et afficher les paramètres du fichier de configuration de Mobile IP. Il indique également la méthode à utiliser pour afficher l'état de l'agent de mobilité.

Le présent chapitre contient les informations suivantes :

Pour obtenir une introduction à Mobile IP, consultez le Chapitre 27, "Mobile IP (présentation)". Pour obtenir des informations détaillées à propos de Mobile IP, reportez-vous au Chapitre 29, "Fichiers et commandes de Mobile IP (références)".

Remarque – La fonction Mobile IP est supprimée des mises à jour Solaris 10 depuis Solaris 10 8/07.

Création du fichier de configuration de Mobile IP (liste des tâches)

Tâche	Description	Voir
Création du fichier de configuration de Mobile IP	Créez un fichier `/etc/inet/mipagent.conf` ou copiez l'un des fichiers d'exemple.	"Création du fichier de configuration de Mobile IP " à la page 725

Tâche	Description	Voir
Configuration de la section `General`	Saisissez le numéro de version dans la section `General` du fichier de configuration de Mobile IP.	"Configuration de la section `General`" à la page 725
Configuration de la section `Advertisements`	Ajoutez ou modifiez les étiquettes et les valeurs de la section `Advertisements` du fichier de configuration de Mobile IP.	"Configuration de la section `Advertisements` " à la page 726
Configuration de la section `GlobalSecurityParameters`	Ajoutez ou modifiez les étiquettes et les valeurs de la section `GlobalSecurityParameters` du fichier de configuration de Mobile IP.	"Configuration de la section `GlobalSecurityParameters` " à la page 726
Configuration de la section `Pool`	Ajoutez ou modifiez les étiquettes et les valeurs de la section `Pool` du fichier de configuration de Mobile IP.	"Configuration de la section `Pool`" à la page 727
Configuration de la section `SPI`	Ajoutez ou modifiez les étiquettes et les valeurs de la section `SPI` du fichier de configuration de Mobile IP.	"Configuration de la section `SPI`" à la page 727
Configuration de la section `Address`	Ajoutez ou modifiez les étiquettes et les valeurs de la section `Address` du fichier de configuration de Mobile IP.	"Configuration de la section `Address`" à la page 727

Création du fichier de configuration de Mobile IP

Cette section décrit les procédures de planification relatives à Mobile IP et la méthode de création du fichier `/etc/inet/mipagent.conf` .

▼ Procédure de planification de Mobile IP

Lors de la première configuration du fichier `mipagent.conf` , effectuez les tâches suivantes :

1. **Selon la configuration requise par votre organisation en matière d'hôtes, identifiez les fonctionnalités que doit fournir votre agent Mobile IP :**
   - fonctionnalité d'agent étranger uniquement ;
   - fonctionnalité d'agent d'accueil uniquement ;
   - fonctionnalité d'agent étranger et d'agent d'accueil.

2. **Créez le fichier `/etc/inet/mipagent.conf` et spécifiez les paramètres nécessaires à l'aide des procédures décrites dans cette section. Vous pouvez également copier l'un des fichiers suivants dans le fichier `/etc/inet/mipagent.conf` et le modifier en fonction de vos besoins :**

- Pour la fonctionnalité d'agent étranger, copiez le fichier `/etc/inet/mipagent.conf.fa-sample` .
- Pour la fonctionnalité d'agent d'accueil, copiez le fichier `/etc/inet/mipagent.conf.ha-sample` .
- Pour la fonctionnalité d'agent étranger et d'agent d'accueil, copiez le fichier `/etc/inet/mipagent.conf-sample`.

3 **Vous pouvez réinitialiser votre système afin d'appeler le script d'initialisation qui lance le démon `mipagent` . Vous pouvez également démarrer `mipagent` à l'aide de la commande suivante :**

```
# /etc/inet.d/mipagent start
```

▼ Création du fichier de configuration de Mobile IP

1 **Connectez-vous au système sur lequel vous souhaitez activer Mobile IP en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Créez le fichier `/etc/inet/mipagent.conf` à l'aide de l'une des options suivantes :**

- Dans le répertoire `/etc/inet`, créez un fichier vide nommé `mipagent.conf`.
- À partir de la liste suivante, copiez l'exemple de fichier qui fournit la fonctionnalité que vous souhaitez attribuer au fichier `/etc/inet/mipagent.conf`.
  - `/etc/inet/mipagent.conf.fa-sample`
  - `/etc/inet/mipagent.conf.ha-sample`
  - `/etc/inet/mipagent.conf-sample`

3 **Ajoutez ou modifiez les paramètres de configuration au fichier `/etc/inet/mipagent.conf` en fonction de la configuration requise.**

Les procédures restantes de cette section décrivent les étapes permettant de modifier les sections du fichier `/etc/inet/mipagent.conf`.

▼ Configuration de la section `General`

Si vous avez copié un des exemples de fichiers dans le répertoire `/etc/inet`, vous pouvez omettre cette procédure, car l'exemple de fichier contient cette entrée. “Section `General`” à la page 745 contient les descriptions des étiquettes et valeurs utilisées dans cette section.

- **Modifiez le fichier `/etc/inet/mipagent.conf` et ajoutez les lignes suivantes :**

```
[General]
     Version = 1.0
```

Remarque – Le fichier `/etc/inet/mipagent.conf` doit contenir cette entrée.

▼ Configuration de la section `Advertisements`

"Section `Advertisements`" à la page 745 contient les descriptions des étiquettes et valeurs utilisées dans cette section.

- **Modifiez le fichier `/etc/inet/mipagent.conf` et ajoutez ou modifiez les lignes suivantes avec les valeurs requises pour votre configuration.**

```
[Advertisements interface]
     HomeAgent = <yes/no>
     ForeignAgent = <yes/no>
     PrefixFlags = <yes/no>
     AdvertiseOnBcast = <yes/no>
     RegLifetime = n
     AdvLifetime = n
     AdvFrequency = n
     ReverseTunnel = <yes/no/FA/HA/both>
     ReverseTunnelRequired = <yes/no/FA/HA>
```

Remarque – Vous devez inclure une section `Advertisements` différente pour chaque interface sur l'hôte local qui fournit les services de Mobile IP.

▼ Configuration de la section `GlobalSecurityParameters`

La "Section `GlobalSecurityParameters`" à la page 747 contient les descriptions des étiquettes et valeurs utilisées dans cette section.

- **Modifiez le fichier `/etc/inet/mipagent.conf` et ajoutez ou modifiez les lignes suivantes avec les valeurs requises pour votre configuration :**

```
[GlobalSecurityParameters]
     MaxClockSkew = n
     HA-FAauth = <yes/no>
     MN-FAauth = <yes/no>
     Challenge = <yes/no>
     KeyDistribution = files
```

Configuration de la section `Pool`

La "Section `Pool`" à la page 748 fournit les descriptions des étiquettes et valeurs utilisées dans cette section.

1. **Modifiez le fichier `/etc/inet/mipagent.conf`**

2. **Ajoutez ou modifiez les lignes suivantes avec les valeurs requises pour votre configuration :**

```
[Pool pool-identifier]
     BaseAddress = IP-address
     Size = size
```

Configuration de la section `SPI`

La "Section `SPI`" à la page 749 contient les descriptions des étiquettes et valeurs utilisées dans cette section.

1. **Modifiez le fichier `/etc/inet/mipagent.conf` .**

2. **Ajoutez ou modifiez les lignes suivantes avec les valeurs requises pour votre configuration :**

```
[SPI SPI-identifier]
     ReplayMethod = <none/timestamps>
     Key = key
```

Remarque – Vous devez inclure une section `SPI` différente pour chaque contexte de sécurité déployé.

Configuration de la section `Address`

La "Section `Address`" à la page 749 contient les descriptions des étiquettes et valeurs utilisées dans cette section.

1. **Modifiez le fichier `/etc/inet/mipagent.conf` .**

2. **Ajoutez ou modifiez les lignes suivantes avec les valeurs requises pour votre configuration :**

   - **Pour un nœud mobile, utilisez ce qui suit :**

     ```
     [Address address]
          Type = node
          SPI = SPI-identifier
     ```

   - **Pour un agent, utilisez ce qui suit :**

     ```
     [Address address]
          Type = agent
     ```

```
SPI = SPI-identifier
```

- **Pour un nœud mobile identifié par son NAI (Network Access Identifier, identificateur d'accès à Internet), utilisez les valeurs suivantes :**

```
[Address NAI]
     Type = Node
     SPI = SPI-identifier
     Pool = pool-identifier
```

- **Pour un nœud mobile par défaut, utilisez les valeurs suivantes :**

```
[Address Node-Default]
     Type = Node
     SPI = SPI-identifier
     Pool = pool-identifier
```

Modification du fichier de configuration Mobile IP (liste des tâches)

Tâche	Description	Voir
Modification de la section `General`	Utilisez la commande `mipagentconfig change` afin de modifier la valeur d'une étiquette dans la section `General` du fichier de configuration de Mobile IP.	"Modification de la section `General`" à la page 729
Modification de la section`Advertisements`	Utilisez la commande `mipagentconfig change` afin de modifier la valeur d'une étiquette dans la section `Advertisements` du fichier de configuration Mobile IP.	"Modification de la section `Advertisements`" à la page 730
Modification de la section `GlobalSecurityParameters`	Utilisez la commande `mipagentconfig change` afin de modifier la valeur de l'étiquette de la section `GlobalSecurityParameters` du fichier de configuration de Mobile IP.	"Modification de la section `GlobalSecurityParameters` " à la page 730
Modification de la section `Pool`	Utilisez la commande `mipagentconfig change` afin de modifier la valeur d'une étiquette de la section `Pool` du fichier de configuration de Mobile IP.	"Modification de la section `Pool`" à la page 731
Modification de la section `SPI`	Utilisez la commande `mipagentconfig change` afin de modifier la valeur de l'étiquette de la section `SPI` du fichier de configuration de Mobile IP.	"Modification de la section `SPI`" à la page 732

Modification de la section `Address`	Utilisez la commande `mipagentconfig change` afin de modifier la valeur de l'étiquette de la section `Address` du fichier de configuration de Mobile IP.	"Modification de la section `Address`" à la page 732
Ajout ou suppression de paramètres	Utilisez les commandes `mipagentconfig add` ou `delete` afin d'ajouter ou de supprimer de nouveaux paramètres, étiquettes et valeurs dans toute section du fichier de configuration de Mobile IP.	"Ajout et suppression de paramètres du fichier de configuration" à la page 733
Affichage des paramètres actuels des destinations de paramètres	Utilisez la commande `mipagentconfig get` afin d'afficher les paramètres actuels de toute section du fichier de configuration de Mobile IP.	"Affichage des valeurs de paramètres actuelles dans le fichier de configuration" à la page 734

Modification du fichier de configuration de Mobile IP

Cette section indique comment modifier le fichier de configuration de Mobile IP à l'aide de la commande `mipagentconfig` . Cette section indique également comment afficher les paramètres actuels des destinations de paramètres.

La section "Configuration de l'agent de mobilité IP" à la page 753 fournit une description conceptuelle de l'utilisation de la commande `mipagentconfig.` Reportez-vous également à la page de manuel `mipagentconfig(1M)`.

▼ Modification de la section `General`

1 **Connectez-vous au système sur lequel vous souhaitez activer Mobile IP en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Sur une ligne de commande, saisissez la commande suivante pour chaque étiquette que vous souhaitez modifier dans la section `General`.**

```
# mipagentconfig change <label> <value>
```

Exemple 28–1 Modification d'un paramètre de la section `General`

L'exemple suivant indique comment modifier le numéro de version de la section `General` du fichier de configuration.

```
# mipagentconfig change version 2
```

▼ Modification de la section `Advertisements`

1 **Connectez-vous au système sur lequel vous souhaitez activer Mobile IP en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Saisissez la commande suivante pour chaque étiquette que vous souhaitez modifier dans la section `Advertisements` :**

```
# mipagentconfig change adv device-name <label> <value>
```

Par exemple, si vous modifiez la durée de vie publiée de l'agent à 300 secondes pour le périphérique `hme0`, utilisez la commande suivante :

```
# mipagentconfig change adv hme0 AdvLifetime 300
```

Exemple 28–2 Modification de la section `Advertisements`

L'exemple suivant indique comment modifier d'autres paramètres de la section `Advertisements` du fichier de configuration.

```
# mipagentconfig change adv hme0 HomeAgent yes
# mipagentconfig change adv hme0 ForeignAgent no
# mipagentconfig change adv hme0 PrefixFlags no
# mipagentconfig change adv hme0 RegLifetime 300
# mipagentconfig change adv hme0 AdvFrequency 4
# mipagentconfig change adv hme0 ReverseTunnel yes
```

▼ Modification de la section `GlobalSecurityParameters`

1 **Connectez-vous au système sur lequel vous souhaitez activer Mobile IP en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Saisissez la commande suivante pour chaque étiquette que vous souhaitez modifier dans la section `GlobalSecurityParameters` :**

   ```
   # mipagentconfig change <label> <value>
   ```

   Si vous activez par exemple l'authentification de l'agent d'accueil et de l'agent étranger, utilisez la commande suivante :

   ```
   # mipagentconfig change HA-FAauth yes
   ```

Exemple 28–3 Modification de la section des paramètres de sécurité globale

L'exemple suivant indique comment modifier d'autres paramètres de la section `GlobalSecurityParameters` du fichier de configuration.

```
# mipagentconfig change MaxClockSkew 200
# mipagentconfig change MN-FAauth yes
# mipagentconfig change Challenge yes
# mipagentconfig change KeyDistribution files
```

▼ Modification de la section `Pool`

1. **Connectez-vous au système sur lequel vous souhaitez activer Mobile IP en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Saisissez la commande suivante pour chaque étiquette que vous souhaitez modifier dans la section `Pool` :**

   ```
   # mipagentconfig change Pool pool-identifier <label> <value>
   ```

Exemple 28–4 Modification de la section `Pool`

L'exemple suivant indique les commandes à utiliser pour modifier l'adresse de base en `192.168.1.1`, ainsi que la taille du Pool de `10` à `100`.

```
# mipagentconfig change Pool 10 BaseAddress 192.168.1.1
# mipagentconfig change Pool 10 Size 100
```

▼ Modification de la section `SPI`

1 **Connectez-vous au système sur lequel vous souhaitez activer Mobile IP en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Saisissez la commande suivante pour chaque étiquette que vous souhaitez modifier dans la section `SPI` :**

```
# mipagentconfig change SPI SPI-identifier <label> <value>
```

Si vous modifiez par exemple la clé de `SPI 257` en `5af2aee39ff0b332`, utilisez la commande suivante :

```
# mipagentconfig change SPI 257 Key 5af2aee39ff0b332
```

Exemple 28–5 Modification de la section `SPI`

L'exemple suivant indique comment modifier l'étiquette `ReplayMethod` de la section `SPI` du fichier de configuration.

```
# mipagentconfig change SPI 257 ReplayMethod timestamps
```

▼ Modification de la section `Address`

1 **Connectez-vous au système sur lequel vous souhaitez activer Mobile IP en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Saisissez la commande suivante pour chaque étiquette à modifier dans la section `Address` :**

```
# mipagentconfig change addr [NAI | IPaddr | node-default] <label> <value>
```

Consultez la section “Section `Address`” à la page 749 pour obtenir une description des trois méthodes de configuration (NAI, adresse IP et nœud-défaut).

Si vous modifiez, par exemple, le SPI de l'adresse IP `10.1.1.1` en `258`, utilisez la commande suivante :

```
# mipagentconfig change addr 10.1.1.1 SPI 258
```

Exemple 28–6 Modification de la section `Address`

L'exemple suivant indique comment modifier les autres paramètres fournis dans la section `Address` de l'exemple de fichier de configuration.

```
# mipagentconfig change addr 10.1.1.1 Type agent
# mipagentconfig change addr 10.1.1.1 SPI 259
# mipagentconfig change addr mobilenode@abc.com Type node
# mipagentconfig change addr mobilenode@abc.com SPI 258
# mipagentconfig change addr mobilenode@abc.com Pool 2
# mipagentconfig change addr node-default SPI 259
# mipagentconfig change addr node-default Pool 3
# mipagentconfig change addr 10.68.30.36 Type agent
# mipagentconfig change addr 10.68.30.36 SPI 260
```

▼ Ajout et suppression de paramètres du fichier de configuration

1. **Connectez-vous au système sur lequel vous souhaitez activer Mobile IP en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Saisissez la commande adéquate pour chaque étiquette que vous souhaitez ajouter ou supprimer pour la section donnée :**

   - Pour la section `General`, utilisez la commande suivante :

     ```
     # mipagentconfig [add | delete] <label> <value>
     ```

   - Pour la section `Advertisements`, utilisez la commande suivante :

     ```
     # mipagentconfig [add | delete] adv device-name <label> <value>
     ```

     Remarque – La commande suivante permet d'ajouter une interface :

     ```
     # mipagentconfig add adv device-name
     ```

     Dans cette instance, les valeurs par défaut sont assignées à l'interface (pour l'agent étranger et l'agent d'accueil).

   - Pour la section `GlobalSecurityParameters`, utilisez la commande suivante :

     ```
     # mipagentconfig [add | delete] <label> <value>
     ```

   - Pour la section `Pool`, utilisez la commande suivante :

```
# mipagentconfig [add | delete] Pool pool-identifier <label> <value>
```

- Pour la section `SPI`, utilisez la commande suivante :

```
# mipagentconfig [add | delete] SPI SPI-identifier <label> <value>
```

- Pour la section `Address`, utilisez la commande suivante :

```
# mipagentconfig [add | delete] addr [NAI | IP-address | node-default] \
<label> <value>
```

Remarque – Veillez à ne pas créer des sections `Advertisements`, `Pool` , `SPI` et `Address` identiques.

Exemple 28–7 Modification de paramètres de fichiers

Par exemple, pour créer un pool d'adresses nommé Pool 11, dont l'adresse de base est `192.167.1.1` et la taille est `100`, utilisez les commandes suivantes :

```
# mipagentconfig add Pool 11 BaseAddress 192.167.1.1
# mipagentconfig add Pool 11 size 100
```

Exemple 28–8 Suppression de SPI

L'exemple suivant indique comment supprimer le paramètre de sécurité SPI `SPI 257`.

```
# mipagentconfig delete SPI 257
```

▼ Affichage des valeurs de paramètres actuelles dans le fichier de configuration

La commande `mipagentconfig get` permet d'afficher les paramètres actuels associés aux destinations de paramètres.

1. **Connectez-vous au système sur lequel vous souhaitez activer Mobile IP en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Saisissez la commande suivante pour chaque paramètre dont vous souhaitez afficher les valeurs :**

```
# mipagentconfig get [<parameter> | <label>]
```

Par exemple, pour afficher les paramètres de publication du périphérique `hme0`, utilisez la commande suivante :

```
# mipagentconfig get adv hme0
```

La sortie suivante s'affiche en résultat :

```
[Advertisements hme0]
   HomeAgent = yes
   ForeignAgent = yes
```

Exemple 28–9 Utilisation de la commande `mipagentconfig get` pour l'affichage des valeurs de paramètres

L'exemple suivant illustre le résultat de l'utilisation de la commande `mipagentconfig get` avec d'autres destinations de paramètre.

```
# mipagentconfig get MaxClockSkew
      [GlobalSecurityParameters]
         MaxClockSkew=300

# mipagentconfig get HA-FAauth
      [GlobalSecurityParameters]
         HA-FAauth=no

# mipagentconfig get MN-FAauth
      [GlobalSecurityParameters]
         MN-FAauth=no

# mipagentconfig get Challenge
      [GlobalSecurityParameters]
         Challenge=no

# mipagentconfig get Pool 10
      [Pool 10]
         BaseAddress=192.168.1.1
         Size=100

# mipagentconfig get SPI 257
      [SPI 257]
         Key=11111111111111111111111111111111
         ReplayMethod=none

# mipagentconfig get SPI 258
      [SPI 258]
         Key=15111111111111111111111111111111
         ReplayMethod=none

# mipagentconfig get addr 10.1.1.1
      [Address 10.1.1.1]
         SPI=258
         Type=agent

# mipagentconfig get addr 192.168.1.200
      [Address 192.168.1.200]
```

```
SPI=257
Type=node
```

Affichage de l'état de l'agent de mobilité

La commande `mipagentstat` permet d'afficher la liste des visiteurs de l'agent étranger et la table de liaison de l'agent d'accueil. La section "État de l'agent de mobilité Mobile IP" à la page 754 fournit une description conceptuelle de la commande `mipagentstat`. Vous pouvez également consulter la page de manuel `mipagentstat(1M)`.

▼ Affichage de l'état de l'agent de mobilité

1 **Connectez-vous au système sur lequel vous activez Mobile IP en tant que superutilisateur ou en prenant un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour de plus amples informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichez l'état de l'agent de mobilité.**

`# mipagentstat` *options*

`-f` Affiche la liste des nœuds mobiles actifs dans la liste des visiteurs de l'agent étranger.

`-h` Affiche la liste des nœuds mobiles actifs dans la table de liaisons de l'agent d'accueil.

`-p` Affiche la liste des associations de sécurité avec les homologues d'agent d'un agent de mobilité.

Exemple 28–10 Affichage de l'état de l'agent de mobilité

Cet exemple indique comment afficher la liste de visiteurs de tous les nœuds mobiles enregistrés avec un agent étranger.

```
# mipagentstat -f
```

Une sortie similaire à la suivante s'affiche :

```
Mobile Node     Home Agent     Time (s)     Time (s)  Flags
                               Granted      Remaining
--------------- -------------- ------------ --------- -----
foobar.xyz.com  ha1.xyz.com    600          125       .....T.
10.1.5.23       10.1.5.1       1000         10        .....T.
```

Une sortie similaire à la suivante s'affiche :

```
Foreign                 ..... Security Association(s).....
Agent                   Requests Replies  FTunnel  RTunnel
---------------------   -------- -------- -------- --------
forn-agent.eng.sun.com  AH       AH       ESP      ESP
```

Cet exemple indique comment afficher les associations de sécurité des agents d'accueil.

```
# mipagentstat -fp
```

Une sortie similaire à la suivante s'affiche :

```
Home                    ..... Security Association(s) .....
Agent                   Requests Replies  FTunnel  RTunnel
---------------------   -------- -------- -------- --------
home-agent.eng.sun.com  AH       AH       ESP      ESP
ha1.xyz.com             AH,ESP   AH       AH,ESP   AH,ESP
```

Affichage des routes de mobilité sur un agent de mobilité

La commande `netstat` permet d'afficher des informations supplémentaires à propos des routes spécifiques à la source créées par les tunnels de transmission et de retour. Consultez la page de manuel `netstat` (1M) pour de plus amples informations à propos de cette commande.

▼ Affichage des routes de mobilité sur un agent étranger

1. **Connectez-vous au système sur lequel vous activez Mobile IP en tant que superutilisateur ou en prenant un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour de plus amples informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Affichez les routes de mobilité.**

   ```
   # netstat -rn
   ```

Exemple 28–11 Affichage des routes de mobilité sur un agent de mobilité

L'exemple suivant illustre les routes d'un agent étranger qui utilise un tunnel de retour.

```
Routing Table:   IPv4 Source-Specific
Destination      In If     Source      Gateway Flags  Use  Out If
--------------  ------- ------------ --------- -----  ---- -------
10.6.32.11      ip.tun1      --      10.6.32.97  UH      0 hme1
    --          hme1    10.6.32.11       --      U       0 ip.tun1
```

La première ligne indique que l'adresse IP de destination `10.6.32.11` et l'interface `ip.tun1` sélectionnent l'interface `hme1` pour la transmission de paquets. La ligne suivante indique que les paquets provenant de l'interface `hme1` et de l'adresse source `10.6.32.11` doivent être transférés vers `ip.tun1`.

◆ ◆ ◆ CHAPITRE 29

Fichiers et commandes de Mobile IP (références)

Ce chaptitre décrit les composants fournis avec l'implémentation Solaris de Mobile IP. Pour utiliser Mobile IP, commencez par configurer le fichier de configuration de Mobile IP à l'aide des paramètres et commandes décrits dans ce chapitre.

Le présent chapitre contient les informations suivantes :

Remarque – La fonction Mobile IP est supprimée des mises à jour Solaris 10 depuis Solaris 10 8/07.

Présentation de l'implémentation de Mobile IP Solaris

Le logiciel de l'agent de mobilité contient les fonctionnalités de l'agent d'accueil et de l'agent étranger. Le logiciel Mobile IP Solaris ne fournit pas de nœud de client mobile, mais la fonctionnalité de l'agent uniquement. Tout réseau avec prise en charge de mobilité doit posséder au moins un hôte statique (non mobile) exécutant ce logiciel.

Les fonctions RFC suivantes sont prises en charge par l'implémentation Solaris de Mobile IP :

- RFC 1918, "Address Allocation for Private Internets" (`http://www.ietf.org/rfc/rfc1918.txt?number=1918`)
- RFC 2002, "IP Mobility Support" (Agent only) (`http://www.ietf.org/rfc/rfc2002.txt?number=2002`)

- RFC 2003, "IP Encapsulation Within IP" (`http://www.ietf.org/rfc/rfc2003.txt?number=2003`)
- RFC 2794, "Mobile IP Network Access Identifier Extension for IPv4" (`http://www.ietf.org/rfc/rfc2794.txt?number=2794`)
- RFC 3012, "Mobile IPv4 Challenge/Response Extensions" (`http://www.ietf.org/rfc/rfc3012.txt?number=3012`)
- RFC 3024, "Reverse Tunneling for Mobile IP" (`http://www.ietf.org/rfc/rfc3024.txt?number=3024`)

Le protocole de base de Mobile IP (RFC 2002) ne permet pas de résoudre le problème de distribution de clés évolutives et traite la distribution de clés comme un problème orthogonal. Le logiciel Mobile IP Solaris utilise uniquement des clés configurées manuellement et spécifiées dans un fichier de configuration.

Les fonctions RFC suivantes ne sont pas prises en charge dans l'implémentation Solaris de Mobile IP :

- RFC 1701, "General Routing Encapsulation" (`http://www.ietf.org/rfc/rfc1701.txt?number-1701`)
- RFC 2004, "Minimal Encapsulation Within IP" (`http://www.ietf.org/rfc/rfc2004.txt?number=2004`)

Les fonctions suivantes ne sont pas prises en charge dans l'implémentation Solaris de Mobile IP :

- la transmission de trafic de multidiffusion ou de trafic de diffusion par l'agent d'accueil vers l'agent étranger pour un nœud mobile accédant à un réseau étranger ;
- le routage de datagrammes de diffusion et de multidiffusion par le biais de tunnels inverses ;
- les adresses d'hébergement ou d'agent d'accueil privées.

Pour plus d'informations, consultez la page de manuel `mipagent(1M)`.

Fichier de configuration de Mobile IP

La commande `mipagent` lit les informations de configuration à partir du fichier de configuration `/etc/inet/mipagent.conf` au démarrage. Mobile IP utilise le fichier de configuration `/etc/inet/mipagent.conf` afin d'initialiser son agent de mobilité. Lorsqu'il est configuré et déployé, l'agent de mobilité émet des publications de routeur périodique et répond aux messages de demande de détection de routeur ou d'enregistrement de Mobile IP.

Consultez la page de manuel `mipagent.conf(4)` pour obtenir une description des attributs de fichier. Consultez la page de manuel `mipagent(1M)` pour obtenir une description de l'utilisation de ce fichier.

Format du fichier de configuration

Le fichier de configuration Mobile IP est constitué de sections. Chaque section possède un nom unique et est mise entre crochets. Chaque section contient au moins une étiquette. Le format suivant permet d'assigner des valeurs aux étiquettes :

```
[Section_name]
     Label-name = value-assigned
```

La section "Sections et étiquettes de fichiers de configuration" à la page 744 décrit les noms, étiquettes et valeurs de section possibles.

Exemples de fichiers de configuration

L'installation Solaris fournit les exemples de fichiers de configuration suivants dans le répertoire `/etc/inet` :

- `mipagent.conf-sample` – contient un exemple de configuration pour un agent Mobile IP qui fournit des fonctionnalités d'agent étranger et d'agent d'accueil.
- `mipagent.conf.fa-sample` – contient un exemple de configuration pour un agent Mobile IP qui fournit uniquement une fonctionnalité d'agent étranger.
- `mipagent.conf.ha-sample` – contient un exemple de configuration pour un agent Mobile IP qui fournit uniquement une fonctionnalité d'agent d'accueil.

Ces exemples de fichiers de configuration contiennent des adresses de nœuds mobiles et des paramètres de sécurité. Préalablement à l'implémentation de Mobile IP, vous devez créer un fichier de configuration nommé `mipagent.conf` et le placer dans le répertoire `/etc/inet`. Ce fichier contient les paramètres de configuration répondant aux exigences d'implémentation de Mobile IP. Vous pouvez également choisir l'un des exemples de fichier de configuration, le modifier avec vos adresses et paramètres de sécurité, puis le copier dans le fichier `/etc/inet/mipagent.conf` .

Pour de plus amples informations, reportez-vous à la section "Création du fichier de configuration de Mobile IP " à la page 725.

Fichier `mipagent.conf-sample`

La liste suivante répertorie les sections, étiquettes et valeurs contenues dans le fichier `mipagent.conf-sample`. La section "Sections et étiquettes de fichiers de configuration" à la page 744 décrit la syntaxe, les sections, les étiquettes et les valeurs.

```
[General]
   Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
```

```
   HomeAgent = yes
   ForeignAgent = yes
   PrefixFlags = yes
   AdvertiseOnBcast = yes
   RegLifetime = 200
   AdvLifetime = 200
   AdvFrequency = 5
   ReverseTunnel = no
   ReverseTunnelRequired = no

[GlobalSecurityParameters]
   MaxClockSkew = 300
   HA-FAauth = yes
   MN-FAauth = yes
   Challenge = no
   KeyDistribution = files

[Pool 1]
   BaseAddress = 10.68.30.7
   Size = 4

[SPI 257]
   ReplayMethod = none
   Key = 11111111111111111111111111111111

[SPI 258]
   ReplayMethod = none
   Key = 15111111111111111111111111111111

[Address 10.1.1.1]
   Type = node
   SPI = 258

[Address mobilenode@sun.com]
   Type = node
   SPI = 257
   Pool = 1

[Address Node-Default]
   Type = node
   SPI = 258
   Pool = 1

[Address 10.68.30.36]
   Type = agent
   SPI = 257
```

Fichier `mipagent.conf.fa-sample`

La liste suivante répertorie les sections, étiquettes et valeurs contenues dans le fichier `mipagent.conf.fa-sample`. La section "Sections et étiquettes de fichiers de configuration" à la page 744 décrit la syntaxe, les sections, les étiquettes et les valeurs.

Le fichier `mipagent.conf.fa-sample` propose une configuration qui fournit uniquement une fonctionnalité d'agent étranger. Cet exemple de fichier en contient pas de section `Pool`, car les pools sont utilisés uniquement par les agents d'accueil. Autrement, ce fichier est similaire au fichier `mipagent.conf-sample`.

```
[General]
   Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
   HomeAgent = no
   ForeignAgent = yes
   PrefixFlags = yes
   AdvertiseOnBcast = yes
   RegLifetime = 200
   AdvLifetime = 200
   AdvFrequency = 5
   ReverseTunnel = yes
   ReverseTunnelRequired = no

[GlobalSecurityParameters]
   MaxClockSkew = 300
   HA-FAauth = yes
   MN-FAauth = yes
   Challenge = no
   KeyDistribution = files

[SPI 257]
   ReplayMethod = none
   Key = 11111111111111111111111111111111

[SPI 258]
   ReplayMethod = none
   Key = 15111111111111111111111111111111

[Address 10.1.1.1]
   Type = node
   SPI = 258

[Address 10.68.30.36]
   Type = agent
   SPI = 257
```

Fichier `mipagent.conf.ha-sample`

La liste suivante répertorie les sections, étiquettes et valeurs contenues dans le fichier `mipagent.conf.ha-sample`. La section “Sections et étiquettes de fichiers de configuration” à la page 744 décrit la syntaxe, les sections, les étiquettes et les valeurs.

Le fichier `mipagent.conf.ha-sample` propose une configuration qui fournit uniquement une fonctionnalité d'agent d'accueil. Autrement, ce fichier est similaire au fichier `mipagent.conf-sample`.

```
[General]
   Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
   HomeAgent = yes
   ForeignAgent = no
   PrefixFlags = yes
   AdvertiseOnBcast = yes
   RegLifetime = 200
```

```
   AdvLifetime = 200
   AdvFrequency = 5
   ReverseTunnel = yes
   ReverseTunnelRequired = no

[GlobalSecurityParameters]
   MaxClockSkew = 300
   HA-FAauth = yes
   MN-FAauth = yes
   Challenge = no
   KeyDistribution = files

[Pool 1]
   BaseAddress = 10.68.30.7
   Size = 4

[SPI 257]
   ReplayMethod = none
   Key = 11111111111111111111111111111111

[SPI 258]
   ReplayMethod = none
   Key = 15111111111111111111111111111111

[Address 10.1.1.1]
   Type = node
   SPI = 258

[Address mobilenode@sun.com]
   Type = node
   SPI = 257
   Pool = 1

[Address Node-Default]
   Type = node
   SPI = 258
   Pool = 1
```

Sections et étiquettes de fichiers de configuration

Le fichier de configuration Mobile IP contient les sections suivantes :

- `General` (requis)
- `Advertisements` (requis)
- `GlobalSecurityParameters` (facultatif)
- `Pool` (facultatif)
- `SPI` (facultatif)
- `Address` (facultatif)

Les sections `General` et `GlobalSecurityParameters` contiennent des informations relatives au fonctionnement de l'agent de Mobile IP. Ces sections ne peuvent s'afficher qu'une seule fois dans le fichier de configuration.

Section `General`

La section `General` contient une seule étiquette : le numéro de version du fichier de configuration. La syntaxe de la section `General` est la suivante :

```
[General]
     Version = 1.0
```

Section `Advertisements`

La section `Advertisements` contient les étiquettes `HomeAgent` et `ForeignAgent` ainsi que d'autres étiquettes. Vous devez inclure une section `Advertisements` différente pour chaque interface sur l'hôte local qui fournit les services de Mobile IP. La section `Advertisements` possède la syntaxe suivante :

```
[Advertisements interface]
     HomeAgent = <yes/no>
     ForeignAgent = <yes/no>
     .
     .
```

En règle générale, votre système possède une interface unique, `eri0` ou `hme0` par exemple, et prend en charge les opérations d'agent d'accueil et d'agent étranger. Si c'est le cas pour l'exemple `hme0`, la valeur `yes` est assignée aux étiquettes `HomeAgent` et `ForeignAgent` comme suit :

```
[Advertisements hme0]
     HomeAgent = yes
     ForeignAgent = yes
     .
     .
```

Pour une publication sur les interfaces dynamiques, utilisez '*' (astérisque) en guise d'ID de périphérique. Par exemple, *Nom-interface* ppp* implique en réalité toutes les interfaces PPP configurées après le démarrage du démon `mipagent`. L'ensemble des attributs dans la section de publication d'un type d'interface dynamique ne change pas.

Le tableau suivant décrit les étiquettes et les valeurs que vous pouvez utiliser dans la section `Advertisements`.

TABLEAU 29–1 Étiquettes et valeurs de la section `Advertisements`

Libellé	Valeur	Description
`HomeAgent`	`yes` ou `no`	Détermine si le démon `mipagent` fournit la fonctionnalité d'agent d'accueil.
`ForeignAgent`	`yes` ou `no`	Détermine si le démon `mipagent` fournit la fonctionnalité d'agent étranger.
`PrefixFlags`	`yes` ou `no`	Spécifie si les publications incluent l'extension facultative de longueur de préfixe.

TABLEAU 29–1 Étiquettes et valeurs de la section `Advertisements` *(Suite)*

Libellé	Valeur	Description
`AdvertiseOnBcast`	`yes` ou `no`	Si sa valeur est `yes`, les publications sont envoyées à `255.255.255.255` , plutôt qu'à `224.0.0.1`.
`RegLifetime`	`n`	Valeur maximale de durée de vie acceptée dans les demandes d'enregistrement, exprimée en secondes.
`AdvLifetime`	`n`	Durée maximale pendant laquelle la publication est considérée comme valide en l'absence de publications supplémentaires, exprimée en secondes.
`AdvFrequency`	`n`	Durée entre deux publications consécutives, exprimée en secondes.
`ReverseTunnel`	`yes` ou `noFA` ou `HA` ou `both`	Détermine si le démon `mipagent` fournit une fonctionnalité de tunnel inverse. La valeur `yes` signifie que l'agent étranger et l'agent d'accueil prennent en charge la création de tunnel inverse. La valeur `no` signifie que l'interface ne prend pas en charge la création de tunnel inverse. La valeur `FA` signifie que l'agent étranger prend en charge la création de tunnel inverse. La valeur `HA` signifie que l'agent d'accueil prend en charge la création de tunnels inverses. La valeur `both` signifie que l'agent d'accueil et l'agent étranger prennent tous deux en charge la création de tunnels inverses.
`ReverseTunnelRequired`	`yes` ou `no`	Détermine si le démon `mipagent` requiert la fonctionnalité de tunnel inverse. Détermine par conséquent si un nœud mobile doit demander un tunnel inverse lors de son enregistrement. La valeur `yes` signifie que l'agent étranger et l'agent d'accueil requièrent tous deux un tunnel inverse. La valeur `no` signifie que l'interface ne requiert pas de tunnel inverse. La valeur `FA` signifie que l'agent étranger requiert un tunnel inverse. La valeur `HA` signifie que l'agent d'accueil requiert un tunnel inverse.
`AdvInitCount`	`n`	Détermine le nombre initial de publications non demandées. La valeur par défaut est 1. Cette valeur n'a un sens que si `AdvLimitUnsolicited` est configuré sur `yes`.
`AdvLimitUnsolicited`	`yes` ou `no`	Active ou désactive un nombre limité de publications non demandées sur l'interface de mobilité.

Section `GlobalSecurityParameters`

La section `GlobalSecurityParameters` contient les étiquettes `maxClockSkew`, `HA-FAauth`, `MN-FAauth`, `Challenge` et `KeyDistribution`. La syntaxe de cette section est la suivante :

```
[GlobalSecurityParameters]
     MaxClockSkew = n
     HA-FAauth = <yes/no>
     MN-FAauth = <yes/no>
     Challenge = <yes/no>
     KeyDistribution = files
```

Le protocole Mobile IP fournit une protection contre la rediffusion de messages en autorisant la présence d'un horodatage dans les messages. Si les horloges sont en décalage, l'agent d'accueil renvoie une erreur au nœud mobile avec l'heure actuelle que le nœud mobile peut utiliser pour s'enregistrer à nouveau. Utilisez l'étiquette `MaxClockSkew` afin de configurer le nombre maximum de secondes de différence entre les horloges de l'agent d'accueil et du nœud mobile. La valeur par défaut est 300 secondes.

Les étiquettes `HA-FAauth` et `MN-FAauth` permettent respectivement d'activer ou de désactiver la nécessité d'authentification accueil-étranger et mobile-étranger. La valeur par défaut est désactivée. L'étiquette `challenge` permet à l'agent étranger d'émettre des questions-réponses au nœud mobile dans ses publications. L'étiquette permet d'obtenir une protection contre les rediffusions. La valeur par défaut est également désactivée.

Le tableau suivant décrit les étiquettes et valeurs que vous pouvez utiliser dans la section `GlobalSecurityParameters`.

TABLEAU 29–2 Étiquettes et valeurs de la section `GlobalSecurityParameters`

Libellé	Valeur	Description
`MaxClockSkew`	`n`	Nombre de secondes de différence entre sa propre heure locale et l'heure des demandes d'enregistrement qu'accepte le démon `mipagent`.
`HA-FAauth`	`yes` ou `no`	Spécifie si les extensions d'authentification HA-FA doivent se trouver dans les demandes et les réponses d'enregistrement.
`MN-FAauth`	`yes` ou `no`	Spécifie si les extensions d'authentification MN-FA doivent se trouver dans les demandes et les réponses d'enregistrement.
`Challenge`	`yes` ou `no`	Spécifie si l'agent étranger inclut des questions/réponses dans ses publications de mobilité.
`KeyDistribution`	`files`	Doit être définie sur les fichiers.

Section `Pool`

L'agent d'accueil peut attribuer des adresses dynamiques aux nœuds mobiles. L'attribution d'adresses dynamiques s'effectue au sein du démon `mipagent`, indépendamment du protocole DHCP. Vous pouvez créer un pool d'adresses qui peut être utilisé par les nœuds mobiles en demandant une adresse d'accueil. Les pools d'adresses se configurent par le biais de la section `Pool` du fichier de configuration.

La section `Pool` contient les étiquettes `BaseAddress` et `Size`. La syntaxe de la section `Pool` est la suivante :

```
[Pool pool-identifier]
     BaseAddress = IP-address
     Size = size
```

Remarque – Si vous utilisez un identificateur `Pool`, il doit également exister dans la section `Address` du nœud mobile.

La section `Pool` permet de définir les pools d'adresses qu'il est possible d'assigner aux nœuds mobiles. L'étiquette `BaseAddress` permet de définir la première adresse IP du pool. L'étiquette `Size` permet de spécifier le nombre d'adresses disponibles dans le pool.

Par exemple, si les adresses IP de `192.168.1.1` à `192.168.1.100` sont réservées dans le pool 10, la section `Pool` possède l'entrée suivante :

```
[Pool 10]
     BaseAddress = 192.168.1.1
     Size = 100
```

Remarque – Les plages d'adresses ne doivent pas inclure l'adresse de diffusion. Par exemple, vous ne devez pas assigner `BaseAddress` = `192.168.1.200` et `Size` = `60`, car cette plage inclut l'adresse de diffusion `192.168.1.255`.

Le tableau suivant décrit les étiquettes et valeurs utilisées dans la section `Pool`.

TABLEAU 29–3 Étiquettes et valeurs de la section `Pool`

Libellé	Valeur	Description
`BaseAddress`	`n.n.n.n`	Première adresse du pool d'adresses
`Size`	`n`	Nombre d'adresses dans le pool

Section SPI

Dans la mesure où le protocole Mobile IP requiert une authentification de message, vous devez identifier le contexte de sécurité à l'aide d'un SPI (security parameter index, index de paramètres de sécurité) . Le contexte de sécurité est défini dans la section `SPI`. Vous devez inclure une section `SPI` distincte pour chaque contexte de sécurité défini. Un ID numérique identifie le contexte de sécurité. Le protocole Mobile IP se réserve les 256 premiers SPI. Utilisez pour cette raison des valeurs SPI supérieures à 256 uniquement. La section `SPI` contient des informations sur la sécurité, notamment sur les secrets partagés et la protection contre la rediffusion.

La section `SPI` contient également les étiquettes `ReplayMethod` et `Key`. La syntaxe de la section `SPI` est la suivante :

```
[SPI SPI-identifier]
     ReplayMethod = <none/timestamps>
     Key = key
```

Deux homologues qui communiquent doivent partager le même identificateur SPI. Vous devez les configurer avec la même clé et la même méthode de rediffusion. La clé est spécifiée comme une chaîne de chiffres hexadécimaux. La longueur maximale est de 16 octets. Par exemple, si la longueur de la clé est de 16 octets et si cette dernière contient les valeurs hexadécimales de `0` à `f`, la chaîne de la clé pourrait ressembler à ce qui suit :

```
Key = 0102030405060708090a0b0c0d0e0f10
```

Le nombre de chiffres d'une clé doit être pair et correspondre à la représentation de deux chiffres par octet.

Le tableau suivant décrit les étiquettes et valeurs que vous pouvez utiliser dans la section `SPI`.

TABLEAU 29–4 Étiquettes et valeurs de la section `SPI`

Libellé	Valeur	Description
`ReplayMethod`	`none` ou `timestamps`	Spécifie le type d'authentification de rediffusion utilisé pour le SPI.
`Key`	`x`	Clé d'authentification en hexadécimales

Section Address

L'implémentation Solaris de Mobile IP vous permet de configurer les nœuds mobiles selon trois méthodes différentes. Chaque méthode est configurée dans la section `Address`. La première méthode suit le protocole Mobile IP classique ; chaque nœud mobile doit posséder une adresse d'accueil. La seconde méthode permet à un nœud mobile d'être identifié grâce à son NAI (Network Access Identifier, identificateur d'accès au réseau). La dernière méthode permet de configurer un nœud mobile *par défaut* qui peut être utilisé par tout nœud mobile disposant de la valeur SPI adéquate et du matériel de chiffrement associé.

Nœud mobile

La section `Address` d'un nœud mobile contient les étiquettes `Type` et `SPI` qui définissent le type d'adresse et l'identificateur SPI. La syntaxe de la section `Address` est la suivante :

```
[Address address]
     Type = node
     SPI = SPI-identifier
```

Vous devez inclure une section `Address` dans le fichier de configuration de l'agent d'accueil de chaque nœud mobile pris en charge.

Si l'authentification de message Mobile IP est requise entre l'agent étranger et l'agent d'accueil, vous devez inclure une section `Address` pour chaque homologue avec lequel un agent doit communiquer.

La valeur SPI que vous configurez doit représenter une section `SPI` présente dans le fichier de configuration.

Vous pouvez également configurer des adresses privées pour un nœud mobile.

Le tableau suivant décrit les étiquettes et valeurs que vous pouvez utiliser dans la section `Address` pour un nœud mobile.

TABLEAU 29–5 Étiquettes et valeurs de la section `Address` (nœud mobile)

Libellé	Valeur	Description
`Type`	`nœud`	Spécifie que l'entrée est destinée à un nœud mobile
`SPI`	`n`	Spécifie la valeur SPI de l'entrée associée

Agent de mobilité

La section `Address` pour un agent de mobilité contient les étiquettes `Type` et `SPI` qui définissent le type d'adresse et l'identificateur SPI. La section `Address` d'un agent de mobilité utilise la syntaxe suivante :

```
[Address address]
     Type = agent
     SPI = SPI-identifier
```

Vous devez inclure une section `Address` dans le fichier de configuration de l'agent d'accueil pour chaque agent de mobilité pris en charge.

Si un message d'authentification de Mobile IP est requis entre l'agent étranger et l'agent d'accueil, vous devez inclure une section `Address` pour chaque homologue avec lequel un agent doit communiquer.

La valeur SPI que vous configurez doit représenter une section `SPI` présente dans le fichier de configuration.

Le tableau suivant décrit les étiquettes et valeurs que vous pouvez utiliser dans la section `Address` pour un agent de mobilité.

TABLEAU 29–6 Étiquettes et valeurs de la section `Address` (agent de mobilité)

Libellé	Valeur	Description
`Type`	`agent`	Spécifie que l'entrée est destinée à un agent de mobilité.
`SPI`	`n`	Spécifie la valeur SPI de l'entrée associée.

Nœud mobile identifié par son NAI

La section `Address` d'un nœud mobile identifié par son NAI contient les étiquettes `Type`, `SPI` et `Pool`. Le paramètre NAI vous permet d'identifier les nœuds mobiles à l'aide de leurs NAI. La syntaxe de la section `Address` utilisant le paramètre NAI se présente comme suit :

```
[Address NAI]
     Type = Node
     SPI = SPI-identifier
     Pool = pool-identifier
```

Pour utiliser des pools, vous devez identifier les nœuds mobiles grâce à leurs NAI. La section `Address` vous permet de configurer un NAI et non une adresse d'accueil. Un NAI utilise le format `user@domain`. L'étiquette `Pool` permet de spécifier le pool d'adresses à utiliser afin d'allouer l'adresse d'accueil au nœud mobile.

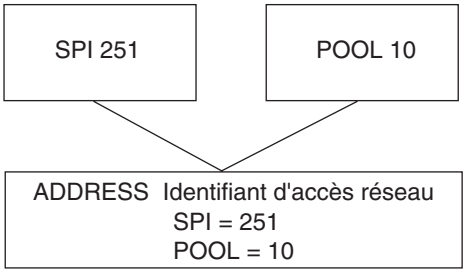
Le tableau suivant décrit les étiquettes et valeurs que vous pouvez utiliser dans la section `Address` pour un nœud mobile identifié par son NAI.

TABLEAU 29–7 Étiquettes et valeurs de la section `Address` (nœud mobile identifié par son NAI)

Libellé	Valeur	Description
`Type`	nœud	Spécifie que l'entrée est destinée à un nœud mobile
`SPI`	`n`	Spécifie la valeur SPI de l'entrée associée
`Pool`	`n`	Alloue le pool à partir duquel une adresse est assignée à un nœud mobile

Vous devez disposer de sections `SPI` et `Pool` correspondantes pour les étiquettes `SPI` et `Pool` définies dans une section `Address` avec un nœud mobile identifié par son NAI, comme illustré dans la figure suivante.

FIGURE 29–1 Sections SPI et Pool correspondantes pour une section Address avec nœud mobile identifié par son NAI



Nœud mobile par défaut

La section Address d'un nœud mobile par défaut contient les étiquettes Type, SPI et Pool. Le paramètre Node-Default permet d'autoriser tous les nœuds mobiles à obtenir du service s'ils possèdent le SPI correct (défini dans cette section). La syntaxe de la section Address utilisant le paramètre Node-Default est la suivante :

```
[Address Node-Default]
     Type = Node
     SPI = SPI-identifier
     Pool = pool-identifier
```

Le paramètre Node-Default permet de réduire la taille du fichier de configuration. Autrement, chaque nœud mobile requiert sa propre section. Cependant, le paramètre Node-Default constitue un risque au niveau de la sécurité. Si, pour quelque raison que ce soit, il devenait impossible de faire confiance à un nœud mobile, vous devez mettre à jour les informations de sécurité de tous les nœuds mobiles de confiance. Cette tâche peut s'avérer très fastidieuse. Vous pouvez cependant utiliser le paramètre Node-Default dans les réseaux qui accordent peu d'importance aux risques de sécurité.

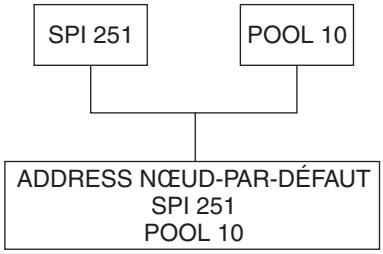
Le tableau suivant décrit les étiquettes et valeurs que vous pouvez utiliser dans la section Address pour un nœud mobile par défaut.

TABLEAU 29–8 Étiquettes et valeurs de la section Address (nœud mobile par défaut)

Libellé	Valeur	Description
Type	nœud	Spécifie que l'entrée est destinée à un nœud mobile
SPI	n	Spécifie la valeur SPI de l'entrée associée
Pool	n	Alloue le pool à partir duquel une adresse est assignée à un nœud mobile

Vous devez disposer de sections SPI et Pool correspondantes pour les étiquettes SPI et Pool définies dans la section Address avec un nœud mobile par défaut, comme illustré dans la figure suivante.

FIGURE 29–2 Sections `SPI` et `Pool` correspondantes pour la section Address avec un nœud mobile par défaut



Configuration de l'agent de mobilité IP

Vous pouvez utiliser la commande `mipagentconfig` afin de configurer l'agent de mobilité. Cette commande permet de créer ou de modifier tout paramètre du fichier de configuration `/etc/inet/mipagent.conf`. Vous pouvez modifier le paramètre de votre choix. Vous pouvez également ajouter ou supprimer les clients de mobilité, les pools et les SPI. La syntaxe de la commande `mipagentconfig` est la suivante :

```
# mipagentconfig <command> <parameter> <value>
```

Le tableau suivant décrit les commandes qu'il est possible d'utiliser conjointement avec `mipagentconfig` pour créer ou modifier les paramètres du fichier de configuration `/etc/inet/mipagent.conf` .

TABLEAU 29–9 Sous-commandes `mipagentconfig`

Commande	Description
`add`	Permet d'ajouter des paramètres de publication, des paramètres de sécurité, des SPI et des adresses au fichier de configuration.
`change`	Permet de modifier les paramètres de publication, les paramètres de sécurité, les SPI et les adresses du fichier de configuration.
`delete`	Permet de supprimer les paramètres de publication, les paramètres de sécurité, les SPI et les adresses du fichier de configuration.
`get`	Permet d'afficher les valeurs actuelles du fichier de configuration.

Consultez la page de manuel `mipagentconfig(1M)` pour obtenir une description des paramètres de commandes et des valeurs acceptables. La section "Modification du fichier de configuration de Mobile IP" à la page 729 décrit les procédures faisant appel à la commande `mipagentconfig`.

État de l'agent de mobilité Mobile IP

La commande `mipagentstat` permet d'afficher la liste de visiteurs de l'agent étranger et la table de liaison d'un agent d'accueil. Vous pouvez également afficher les associations de sécurité avec les homologues d'un agent de mobilité. Pour afficher la liste des visiteurs d'agent étranger, utilisez l'option `-f` de la commande `mipagentstat`. Pour afficher la table de liaison de l'agent d'accueil, utilisez l'option `-h` de la commande `mipagentstat`. Les exemples suivants illustrent la sortie obtenue lorsque vous utilisez la commande `mipagentstat` conjointement avec ces options.

EXEMPLE 29–1 Liste de visiteurs des agents étrangers

```
Mobile Node     Home Agent     Time (s)     Time (s)  Flags
                               Granted      Remaining
--------------- -------------- ------------ --------- -----
foobar.xyz.com  ha1.xyz.com    600          125       .....T.
10.1.5.23       10.1.5.1       1000         10        .....T.
```

EXEMPLE 29–2 Table de liaisons de l'agent d'accueil

```
Mobile Node     Home Agent     Time (s)     Time (s)  Flags
                               Granted      Remaining
--------------- -------------- ------------ --------- -----
foobar.xyz.com  fa1.tuv.com    600          125       .....T.
10.1.5.23       123.2.5.12     1000         10        .....T.
```

Consultez la page de manuel `mipagentstat(1M)` pour obtenir des informations supplémentaires à propos des options de la commande. La section “Affichage de l'état de l'agent de mobilité” à la page 736 décrit les procédures faisant appel à la commande `mipagentstat`.

Informations relatives à l'état de Mobile IP

Lors de l'arrêt, le démon `mipagent` stocke les informations d'état interne dans le fichier `/var/inet/mipagent_state`. Cet événement se produit uniquement lorsque `mipagent` fournit des services en tant qu'agent d'accueil. Ces informations d'état incluent la liste des nœuds mobiles pris en charge en tant qu'agent d'accueil, leurs adresses d'hébergement actuelles et les durées de vie restantes d'enregistrement. Ces informations d'état incluent la configuration d'association de sécurité avec les homologues d'agent de mobilité. Si le démon `mipagent` est interrompu en cas de maintenance et redémarré, le fichier `mipagent_state` permet de recréer autant d'état interne que possible pour l'agent de mobilité. L'objectif est de minimiser les interruptions de service pour les nœuds mobiles qui pourraient visiter d'autres réseaux. Si le fichier `mipagent_state` existe, il est lu immédiatement après le fichier `mipagent.conf` à chaque démarrage ou redémarrage du démon `mipagent`.

Extensions de netstat pour Mobile IP

Les extensions de Mobile IP ont été ajoutées à la commande `netstat` afin d'identifier les routes de transfert de Mobile IP. Vous pouvez, en particulier, utiliser la commande `netstat` pour afficher une nouvelle table de routage dite "spécifique à la source". Consultez la page de manuel `netstat(1M)` pour obtenir des informations supplémentaires.

L'exemple suivant indique la sortie de la commande `netstat` lors de l'utilisation des indicateurs `-nr`.

EXEMPLE 29–3 Sortie Mobile IP à partir la commande `netstat`

```
Routing Table:   IPv4 Source-Specific
Destination      In If     Source      Gateway Flags  Use  Out If
--------------  ------- ------------ --------- -----  ---- -------
10.6.32.11      ip.tun1      --       10.6.32.97  UH      0 hme1
    --          hme1    10.6.32.11       --      U       0 ip.tun1
```

Cet exemple affiche les routes qu'emprunte un agent étranger utilisant un tunnel inverse. La première ligne indique que l'adresse IP de destination `10.6.32.11` et l'interface `ip.tun1` sélectionnent l'interface `hme1` pour la transmission de paquets. La ligne suivante indique que les paquets provenant de l'interface `hme1` et de l'adresse source `10.6.32.11` doivent être transférés vers `ip.tun1`.

Extensions snoop pour Mobile IP

Des extensions de Mobile IP ont été ajoutées à la commande `snoop` afin d'identifier le trafic Mobile IP sur le lien. Pour plus d'informations, reportez-vous à la page de manuel `snoop(1M)`.

L'exemple suivant illustre la sortie de la commande `snoop` exécutée sur le nœud mobile, `mip-mn2`.

EXEMPLE 29–4 Sortie Mobile IP à partir de la commande `snoop`

```
mip-mn2# snoop
Using device /dev/hme (promiscuous mode)
  mip-fa2 -> 224.0.0.1    ICMP Router advertisement (Lifetime 200s [1]:
{mip-fa2-80 2147483648}), (Mobility Agent Extension), (Prefix Lengths),
(Padding)
  mip-mn2 -> mip-fa2   Mobile IP reg rqst
  mip-fa2 -> mip-mn2   Mobile IP reg reply (OK code 0)
```

Cet exemple montre que le nœud mobile a reçu une des publications d'agent de mobilité envoyées périodiquement, en provenance de l'agent étranger `mip-fa2`. Ensuite, `mip-mn2` a envoyé une demande d'enregistrement à `mip-fa2` et reçu une réponse d'enregistrement. La réponse d'enregistrement indique que le nœud mobile s'est enregistré auprès de son agent d'accueil.

PARTIE VI

IPMP

Cette partie décrit le multiacheminement sur réseau IP (IPMP, IP Network Multipathing), ainsi que les tâches relatives à l'administration d'IPMP. IPMP permet de détecter les défaillances, ainsi que d'effectuer le basculement d'interfaces d'un système lorsqu'elles sont connectées à la même liaison.

◆ ◆ ◆ CHAPITRE 30

Présentation d'IPMP

Le multiacheminement sur réseau IP (IPMP, IP Network Multipathing) permet de détecter les défaillances des interfaces physiques et de basculer en transparence l'accès au réseau pour un système présentant plusieurs interfaces sur une même liaison IP. IPMP permet également de répartir la charge des paquets pour les systèmes dotés de plusieurs interfaces.

Le présent chapitre contient les informations suivantes :

Pour les tâches de configuration d'IPMP, reportez-vous au Chapitre 31, "Administration d'IPMP (tâches)".

Avantages d'IPMP

IPMP améliore la fiabilité, la disponibilité et les performances du réseau des systèmes dotés de plusieurs interfaces physiques. Il arrive parfois qu'une interface physique ou le matériel réseau connecté à cette interface présente une défaillance ou requière des opérations de maintenance. Habituellement, il devient alors impossible de contacter le système par le biais de toutes les adresses IP associées à l'interface défaillante. En outre, toute connexion existante vers le système utilisant ces adresses IP est perturbée.

L'utilisation d'IPMP permet de configurer une ou plusieurs interfaces physiques dans un *groupe IPMP*. Une fois la configuration IPMP terminée, le système contrôle automatiquement les interfaces du groupe IPMP. En cas de défaillance ou de retrait pour maintenance d'une interface du groupe, IPMP effectue une migration automatique, ou *basculement*, des adresses IP de

l'interface. Le destinataire de ces adresses est une interface en fonctionnement au sein du groupe IPMP de l'interface défaillante. La fonction de basculement IPMP permet de conserver la connectivité et empêche toute perturbation des connexions existantes. En outre, IPMP répartit le trafic réseau sur l'ensemble des interfaces du groupe IPMP, ce qui permet d'améliorer les performances réseau globales. Ce processus est appelé *répartition de charge*.

Composants IPMP Oracle Solaris

Oracle Solaris IPMP comprend les logiciels suivants :

- le démon `in.mpathd`, dont vous trouverez une description complète à la page de manuel `in.mpathd`(1M) ;
- le fichier de configuration `/etc/default/mpathd` dont vous trouverez également une description à la page de manuel `in.mpathd`(1M) ;
- les options `ifconfig` de la configuration IPMP, telles que décrites à la page de manuel `ifconfig`(1M) ;

Démon de multiacheminement `in.mpathd`

Le démon `in.mpathd` détecte les défaillances d'interface, puis implémente les diverses procédures pour le basculement et le rétablissement. Si `in.mpathd` détecte une défaillance ou une réparation, le démon envoie une commande `ioctl` afin d'effectuer un basculement ou un rétablissement. Le module de noyau `ip` qui implémente la commande `ioctl` effectue le basculement d'accès réseau de manière transparente et automatique.

Remarque – N'utilisez pas l'acheminement secondaire lorsque vous utilisez IPMP sur un même jeu de cartes d'interface réseau. De même, n'utilisez pas IPMP en même temps que l'acheminement secondaire. Vous pouvez utiliser l'acheminement secondaire et IPMP en même temps à condition que cela soit sur des jeux d'interfaces différents. Pour de plus amples informations à propos de l'acheminement alternatif, reportez-vous au *Sun Enterprise Server Alternate Pathing 2.3.1 User Guide*.

Le démon `in.mpathd` détecte les défaillances et les réparations en envoyant des sondes sur toutes les interfaces faisant partie d'un groupe IPMP. Le démon `in.mpathd` détecte également les défaillances et les réparations en contrôlant l'indicateur `RUNNING` sur chaque interface du groupe. Pour obtenir des informations supplémentaires, consultez la page de manuel `in.mpathd`(1M).

Remarque – Le DHCP n'est pas pris en charge pour la gestion des adresses de données IPMP. En cas de tentative d'utilisation de DHCP sur ces adresses, ce protocole finit par cesser de les contrôler. N'utilisez pas le DHCP sur les adresses de données.

Terminologie et concepts IPMP

Cette section présente les termes et concepts utilisés dans les chapitres relatifs à IPMP dans ce manuel.

Liaison IP

Dans la terminologie IPMP, une *liaison IP* correspond à un utilitaire ou moyen de communication à l'aide duquel les nœuds peuvent communiquer dans la couche liaison-données de la suite de protocoles Internet. Les types de liaisons IP comprennent les réseaux Ethernet simples ou avec passerelles, les hubs, ou les réseaux ATM (Asynchronous Transfer Mode). Une liaison IP peut posséder un ou plusieurs numéros de sous-réseau IPv4 et, si applicable, un ou plusieurs préfixes de sous-réseau IPv6. Un même numéro ou préfixe de masque de sous-réseau IPv4 ne peut pas être attribué à plusieurs liaisons IP. Dans le système ATM LANE, une liaison IP est un réseau local (LAN) à émulation simple. Avec le protocole ARP (Address Resolution Protocol, protocole de résolution d'adresse) l'étendue du protocole ARP correspond à une liaison IP unique.

Remarque – D'autres documents relatifs à IP, tel que RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, utilisent le terme *liaison* au lieu de *liaison IP*. Part VI utilise le terme *liaison IP* pour éviter toute confusion avec IEEE 802. Dans IEEE 802, *liaison* se réfère à un seul câble reliant une carte réseau (NIC) Ethernet à un commutateur Ethernet.

Interface physique

L'*interface physique* permet au système de se connecter à une liaison IP. Cette connexion est souvent implémentée comme un pilote de périphérique ou une carte d'interface réseau. Si un système possède plusieurs interfaces connectées à une même liaison, vous pouvez configurer IPMP afin qu'il effectue un basculement en cas de défaillance d'une des interfaces. Pour obtenir des informations supplémentaires sur les interfaces physiques, reportez-vous à la section “Configurations d'interfaces IPMP” à la page 767.

Carte d'interface réseau

Une *carte d'interface réseau* correspond à un adaptateur réseau qu'il est possible d'intégrer au système. La carte d'interface réseau peut également être une carte distincte servant d'interface à partir du système vers une liaison IP. Certaines cartes d'interface réseau possèdent plusieurs interfaces physiques. Par exemple, une carte d'interface réseau `qfe` peut posséder quatre interfaces, de `qfe0` à `qfe3`, et ainsi de suite.

Groupe IPMP

Un groupe de multiacheminement IP, ou groupe *IPMP*, correspond à une ou plusieurs interfaces physiques résidant dans un même système et configurées avec le même nom de groupe IPMP. Toutes les interfaces du groupe IPMP doivent être connectées à la même liaison IP. Le même nom de groupe IPMP sous forme de chaîne de caractères (non-null) identifie la totalité des interfaces du groupe. Vous pouvez placer des interfaces de cartes d'interface réseau de différentes vitesses dans le même groupe IPMP, à condition que les cartes d'interface réseau soient du même type. Par exemple, vous pouvez configurer les interfaces de cartes d'interface réseau Ethernet de 100 Mo et celles de cartes d'interface réseau d'un Go dans un même groupe. Voici un autre exemple : supposons que vous disposez de deux cartes d'interface réseau Ethernet de 100 Mo. Vous pouvez configurer l'une des interfaces de sorte qu'elle soit réduite à 10 Mo, puis placer les deux interfaces dans le même groupe IPMP.

Vous ne pouvez pas placer deux interfaces ayant différents types de média dans un groupe IPMP. Par exemple, vous ne pouvez pas placer une interface ATM dans le même groupe qu'une interface Ethernet.

Détection de défaillance et basculement

La *détection de défaillance* correspond au processus de détection intervenant lorsqu'une interface ou le chemin d'une interface vers un périphérique de couche Internet ne fonctionne plus. IPMP permet aux systèmes de détecter les défaillances d'interface. IPMP détecte les types de défaillance de communication suivants :

- Le chemin de transmission ou de détection de l'interface est défaillant.
- La connexion entre l'interface et la liaison IP a été interrompue.
- Le port sur le commutateur ne reçoit ou ne transmet pas de paquet.
- L'interface physique d'un groupe IPMP n'est pas présente à l'initialisation du système.

Après détection d'une défaillance, IPMP démarre le basculement. Le *basculement* correspond au processus automatique de commutation de l'accès réseau d'une interface défaillante vers une interface physique en état de fonctionnement dans le même groupe. L'accès réseau inclut le trafic IPv4 monodiffusion, multidiffusion et diffusion, ainsi que le trafic IPv6 monodiffusion et multidiffusion. Le basculement n'est possible qu'à condition d'avoir configuré plusieurs interfaces dans le groupe IPMP. Ce processus garantit un accès ininterrompu au réseau.

Détection de réparation et rétablissement

La *détection de réparation* correspond au processus permettant de déterminer le moment auquel une carte d'interface réseau ou le chemin de la carte vers un périphérique de couche 3 est de nouveau fonctionnel après une défaillance. Après avoir détecté la réparation d'une carte d'interface réseau, IPMP effectue un *rétablissement*, qui correspond au processus de restauration de l'accès réseau de l'interface réparée. La détection de réparation suppose que vous avez activé les restaurations automatiques. Reportez-vous à la section “Détection de réparation d'interface physique” à la page 771 pour obtenir des informations supplémentaires.

Système cible

La détection de défaillance basée sur sonde utilise *les systèmes cible* pour déterminer le statut d'une interface. Chaque système cible doit être connecté à la même liaison IP que les membres du groupe IPMP. Le démon `in.mpathd` du système local envoie des messages de sonde IMCP à chaque système cible. Les messages de sonde permettent de déterminer l'état de maintenance de chaque interface du groupe IPMP.

Pour de plus amples informations sur l'utilisation de systèmes cible dans la détection de défaillance basée sur sonde, reportez-vous à la section "Détection de défaillance basée sur sonde" à la page 770.

Répartition de charge sortante

Une fois la configuration d'IPMP terminée, les paquets réseau sortants sont répartis entre plusieurs cartes d'interface réseau, sans incidence sur l'ordre des paquets. On parle de *répartition de charge*. La répartition de charge permet d'augmenter le rendement. Elle ne se produit que lorsque le trafic réseau se dirige vers plusieurs destinations utilisant plusieurs connexions.

Reconfiguration dynamique

La *reconfiguration dynamique* (DR, Dynamic Reconfiguration) correspond à la capacité de reconfiguration d'un système en cours d'exécution en affectant peu ou pas du tout les opérations en cours. La reconfiguration dynamique n'est pas prise en charge par toutes les plates-formes Sun. Certaines plates-formes Sun ne prennent en charge que la reconfiguration dynamique de certains types de matériel. Sur les plates-formes qui prennent en charge la reconfiguration dynamique de cartes d'interface réseau, IPMP peut être utilisé pour basculer de façon transparente l'accès réseau, donnant ainsi au système un accès au réseau ininterrompu.

Pour obtenir des informations supplémentaires sur la prise en charge de la reconfiguration dynamique par IPMP, reportez-vous à la section "IPMP et reconfiguration dynamique" à la page 773.

Exigences de base d'IPMP

Le composant IPMP est intégré à Oracle Solaris et ne nécessite aucun matériel spécial. Toute interface prise en charge par Oracle Solaris peut être utilisée avec IPMP. Cependant, la configuration et la topologie de votre réseau doivent respecter les exigences suivantes relatives à IPMP :

- Toutes les interfaces d'un groupe IPMP doivent disposer d'adresses MAC uniques.

  Notez que par défaut, les interfaces réseau de systèmes SPARC partagent la même adresse MAC. Par conséquent, vous devez modifier explicitement l'adresse par défaut afin d'utiliser IPMP sur des systèmes SPARC. Pour de plus amples informations, reportez-vous à la section "Procédure de planification pour un groupe IPMP" à la page 779.

- Toutes les interfaces d'un groupe IPMP doivent être du même type de média. Pour de plus amples informations, reportez-vous à la section “Groupe IPMP” à la page 762.
- Toutes les interfaces d'un groupe IPMP doivent se trouver sur la même liaison IP. Pour de plus amples informations, reportez-vous à la section “Groupe IPMP” à la page 762.

Remarque – Si plusieurs groupes IPMP appartiennent au même domaine de diffusion (L2 ou couche 2), ces groupes ne sont pas pris en charge. Un domaine de diffusion L2 est généralement mappé à un sous-réseau spécifique. Par conséquent, vous ne devez configurer qu'un seul groupe IPMP par sous-réseau.

- En fonction de vos exigences en matière de détection de défaillance, vous devrez soit utiliser des types spécifiques d'interfaces réseau, soit configurer des adresses IP supplémentaires sur chaque interface réseau. Reportez-vous aux sections “Détection de défaillance basée sur les liaisons” à la page 769 et “Détection de défaillance basée sur sonde” à la page 770.

Adressage IPMP

Vous pouvez configurer la détection de défaillance d'IPMP sur des réseaux IPv4 ainsi que sur des réseaux IPv4 et IPv6 double pile. Les interfaces configurées avec IPMP prennent deux types d'adresses en charge : les adresses de données et les adresses test.

Adresses de données

Les *adresses de données* correspondent aux adresses IPv4 et IPv6 conventionnelles assignées à l'interface d'une carte d'interface réseau au démarrage ou manuellement, à l'aide de la commande `ifconfig`. Le trafic de paquets standard IPv4 et, le cas échéant, IPv6, passant par une interface est considéré comme du *trafic de données*.

Adresses test

Les adresses test sont des adresses spécifiques à IPMP utilisées par le démon `in.mpathd`. Pour pouvoir utiliser la détection de défaillance et de réparation basée sur sonde, une interface doit être configurée avec au moins une adresse test.

Remarque – La configuration des adresses test n'est requise que si vous souhaitez utiliser la détection de défaillance basée sur sonde.

Le démon `in.mpathd` utilise les adresses test afin d'échanger les sondes ICMP avec d'autres cibles sur la liaison IP. C'est ce qu'on appelle le *trafic de sondes*. Le trafic de sondes permet de

déterminer le statut de l'interface et de sa carte d'interface réseau, y compris l'emplacement de la défaillance de l'interface. Les sondes vérifient que le chemin d'envoi et de réception vers l'interface fonctionne correctement.

Il est possible de configurer chaque interface avec une adresse IP test. Dans le cas d'une interface sur un réseau double pile, vous pouvez configurer une adresse test IPv4, une adresse test IPv6 ou les deux.

En cas de défaillance d'une interface, les adresses test restent sur celle-ci de sorte que `in.mpathd` puisse continuer à envoyer des sondes afin de vérifier les réparations ultérieures. Veillez à configurer les adresses test de façon spécifique, de sorte que les applications ne les utilisent pas accidentellement. Pour de plus amples informations, reportez-vous à la section "Empêcher les applications d'utiliser les adresses test" à la page 766.

Pour de plus amples informations sur la détection de défaillance basée sur sonde, reportez-vous à la section "Détection de défaillance basée sur sonde" à la page 770.

Adresses test IPv4

En règle générale, vous pouvez utiliser l'adresse IPv4 de votre choix sur votre sous-réseau en tant qu'adresse test. Il n'est pas nécessaire que les adresses test IPv4 soient acheminables. Dans la mesure où les adresses IPv4 sont une ressource limitée pour de nombreux sites, il est préférable dans certains cas d'utiliser des adresses privées RFC 1918 non acheminables en tant qu'adresses test. Notez que le démon `in.mpathd` n'échange que des sondes ICMP avec d'autres hôtes situés sur le même sous-réseau que l'adresse test. Si vous utilisez des adresses test de type RFC 1918, veillez à configurer d'autres systèmes, des routeurs de préférence, sur la liaison IP avec des adresses situées sur le sous-réseau RFC 1918. Le démon `in.mpathd` peut ensuite échanger les sondes avec des systèmes cible.

Les exemples d'IPMP utilisent les adresses RFC 1918 à partir du réseau `192.168.0/24` en tant qu'adresses test IPv4. Pour plus d'informations sur les adresses privées RFC 1918, reportez-vous au document RFC 1918, Address Allocation for Private Internets (`http://www.ietf.org/rfc/rfc1918.txt?number=1918`) (en anglais).

Pour configurer les adresses test IPv4, reportez-vous à la tâche "Procédure de configuration d'un groupe IPMP avec plusieurs interfaces" à la page 781.

Adresses test IPv6

La seule adresse test IPv6 valide correspond à l'adresse lien-local d'une interface physique. Vous n'avez pas besoin d'utiliser une adresse IPv6 en tant qu'adresse test IPMP. L'adresse IPv6 lien-local est basée sur l'adresse MAC (Media Access Control) de l'interface. Les adresses lien-local sont configurées automatiquement lorsque l'interface devient compatible IPv6 lors du démarrage ou lorsque l'interface est configurée manuellement via `ifconfig`.

Exécutez la commande `ifconfig` *interface* sur un nœud compatible IPv6 afin d'identifier l'adresse lien-local d'une interface. Vérifiez la sortie de l'adresse qui commence par `fe80`, le préfixe lien-local. L'indicateur `NOFAILOVER` dans la sortie de commande `ifconfig` ci-dessous indique que l'adresse lien-local `fe80::a00:20ff:feb9:17fa/10` de l'interface `hme0` est utilisée en tant qu'adresse test.

```
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
          inet6 fe80::a00:20ff:feb9:17fa/10
```

Pour de plus amples informations sur les adresses lien-local, reportez-vous à la section Adresse unicast lien-local.

Lorsque IPv4 et IPv6 sont montés sur la totalité des interfaces d'un groupe IPMP , il est inutile de configurer des adresses test IPv4 distinctes. Le démon `in.mpathd` peut utiliser des adresses IPv6 lien-local en tant qu'adresses test.

Pour créer des adresses test IPv6, reportez-vous à la tâche “Procédure de configuration d'un groupe IPMP avec plusieurs interfaces” à la page 781.

Empêcher les applications d'utiliser les adresses test

Après avoir configuré une adresse test, vous devez vous assurer que cette adresse n'est pas utilisée par les applications. Sinon, en cas de défaillance de l'interface, il devient impossible d'atteindre l'application car les adresses test ne basculent pas lors de l'opération de basculement. Pour vous assurer qu'IP ne sélectionne pas l'adresse test pour des applications normales, marquez l'adresse test comme étant `deprecated`.

IPv4 n'utilise pas d'adresse désapprouvée en tant qu'adresse source pour toute communication, à moins qu'une application ne crée une liaison explicite vers l'adresse. Le démon `in.mpathd` lie de façon explicite à une telle adresse afin d'envoyer et de recevoir du trafic de sondes. Cependant, si une application ne lie pas explicitement à une adresse et que la seule adresse marquée comme `UP` à l'interface est également marquée comme désapprouvée, alors cette adresse est utilisée comme adresse source en dernier recours.

Remarque – En cas de basculement et de rétablissement, tant que la détection d'adresses dupliquées est en cours d'exécution, les applications peuvent recevoir des paquets utilisant des adresses désapprouvées comme adresses source. Ce comportement est attendu. En général, après l'achèvement de la détection d'adresses dupliquées, les adresses désapprouvées ne sont plus traitées par les applications. Toutefois, une exception peut être observée avec les paquets TCP. Une fois qu'une connexion TCP a choisi une adresse source spécifique, l'utilisation de cette adresse ne peut pas être modifiée pendant toute la durée de la connexion. La durée de la connexion peut s'étendre sur une longue période. Dans de tels cas, les applications peuvent néanmoins continuer à utiliser des adresses désapprouvées, même après l'achèvement de la détection d'adresses dupliquées.

Dans la mesure où les adresses IPv6 lien-local sont généralement absentes dans un service de nom, les applications DNS et NIS n'utilisent pas d'adresses lien-local pour la communication. Par conséquent, vous ne devez pas marquer les adresses lien-local IPv6 comme étant `deprecated`.

Les adresses test IPv4 ne doivent pas être placées dans les tables de services de noms DNS et NIS. Dans IPv6, les adresses lien-local ne sont normalement pas placées dans les tables de services de noms.

Configurations d'interfaces IPMP

En règle générale, la configuration d'IPMP se compose d'au moins deux interfaces physiques situées sur le même système et connectées à la même liaison IP. Il n'est pas nécessaire que ces interfaces physiques se trouvent sur la même carte d'interface réseau. Les interfaces sont configurées en tant que membres du même groupe IPMP. Si le système dispose d'interfaces supplémentaires sur une seconde liaison IP, vous devez configurer ces interfaces comme un autre groupe IPMP.

Vous pouvez configurer une interface unique dans son propre groupe IPMP. Le groupe IPMP à interface unique se comporte de la même façon qu'un groupe IPMP avec plusieurs interfaces. Cependant, le basculement et le rétablissement sont impossibles pour un groupe IPMP disposant d'une seule interface.

Vous pouvez également configurer des VLAN en groupe IPMP en procédant de la même manière que pour configurer un groupe à partir d'interfaces IP. Les procédures sont décrites à la section “Configuration de groupes IPMP” à la page 781. Les exigences répertoriées à la section “Exigences de base d'IPMP” à la page 763 s'appliquent également à la configuration de VLAN en groupe IPMP.

Attention – La convention utilisée pour nommer les VLAN peut être à l'origine d'erreurs lorsque vous configurez des VLAN en tant que groupe IPMP. Pour plus de détails sur les noms des réseaux VLAN, reportez-vous à la section "Points de connexions physiques et repères des VLAN" à la page 157 dans le guide *Guide d'administration système : services IP?*. Prenons par exemple quatre VLAN, `bge1000`, `bge1001`, `bge2000` et `bge2001`. L'implémentation IPMP requiert que ces VLAN soient regroupés comme suit : `bge1000` et `bge1001` appartiennent à un seul groupe sur le même VLAN 1, tandis que `bge2000` et `bge2001` appartiennent à un autre groupe sur le même VLAN 2. Du fait des noms VLAN, des VLAN appartenant à différents liens au sein d'un groupe IPMP peuvent facilement être confondus, par exemple `bge1000` et `bge2000`.

Interfaces de réserve d'un groupe IPMP

L'*interface de réserve* d'un groupe IPMP n'est pas utilisée pour le trafic de données, sauf en cas de défaillance d'une autre interface du groupe. En cas de défaillance, les adresses de données de l'interface défaillante migrent vers l'interface de réserve. Ensuite, l'interface de réserve est traitée comme les autres interfaces actives, jusqu'à ce que l'interface défaillante soit réparée. Certains basculements ne choisissent pas l'interface de réserve. Ils choisiront plutôt une interface active disposant d'un nombre moins important d'adresses de données configurées en tant qu'UP.

Sur une interface de réserve, configurez uniquement des adresses test. IPMP ne vous permet pas d'ajouter une adresse de données à une interface configurée par le biais de la commande `ifconfig` comme étant de réserve (option `standby`). Toute tentative de création de ce type de configuration échoue. De même, si vous configurez une interface disposant déjà d'adresses de données comme étant `standby`, ces adresses basculent automatiquement vers une autre interface du groupe IPMP. En raisons de ces restrictions, vous devez utiliser la commande `ifconfig` afin de marquer les adresses test à l'aide des options `deprecated` (désapprouvée) et `-failover` (basculement) avant de configurer l'interface avec l'option `standby`. Pour configurer des interfaces de réserve, reportez-vous à la section "Procédure de configuration d'une interface de réserve pour un groupe IPMP" à la page 788.

Configurations courantes d'interfaces d'IPMP

Comme indiqué dans la section "Adressage IPMP" à la page 764, les interfaces d'un groupe IPMP assurent la gestion du trafic de données et de sondes, en fonction de la configuration des interfaces. Les options IPMP de la commande `ifconfig` permettent de créer la configuration.

Une *interface active* correspond à une interface physique qui transmet le trafic de données et de sondes. Les tâches "Procédure de configuration d'un groupe IPMP avec plusieurs interfaces" à la page 781 et "Procédure de configuration d'un groupe IPMP à interface unique" à la page 790 permettent de configurer l'interface comme étant active.

Vous trouverez ci-dessous deux types courants de configuration IPMP :

Configuration active-active	Groupe IPMP possédant deux interfaces actives. En d'autres termes, elles peuvent transmettre le trafic de sondes et de données à tout moment.
Configuration active-de réserve	Groupe IPMP possédant deux interfaces, dont l'une est configurée en tant qu'interface de réserve.

Vérification du statut d'une interface

L'émission de la commande `ifconfig` *interface* permet de vérifier le statut d'une interface. Pour obtenir des informations générales sur le rapport d'état `ifconfig`, reportez-vous à la section Méthode d'obtention d'informations sur une interface spécifique.

Par exemple, la commande `ifconfig` permet d'obtenir le statut d'une interface de réserve. Lorsque l'interface de réserve n'héberge aucune adresse de données, son statut est signalé par l'indicateur `INACTIVE`. Vous pouvez observer cet indicateur dans les lignes d'état pour l'interface dans la sortie `ifconfig`.

Détection de défaillance d'IPMP et fonctionnalités de reprise

Le démon `in.mpathd` gère les types de détection de défaillance suivants :

- détection de défaillance basée sur les liaisons, si la prise en charge est assurée par le pilote de la carte d'interface réseau ;
- détection de défaillance basée sur sonde, lorsque les adresses test sont configurées ;
- détection d'interfaces manquantes au démarrage.

La page de manuel `in.mpathd(1M)` décrit la méthode de gestion des défaillances d'interface par le démon `in.mpathd`.

Détection de défaillance basée sur les liaisons

La détection de défaillance basée sur les liaisons est toujours activée, à condition que l'interface prenne ce type de détection en charge. Les pilotes de réseau Sun suivants sont pris en charge dans la version actuelle d'Oracle Solaris :

- `hme`
- `eri`
- `ce`
- `ge`
- `bge`
- `qfe`
- `dmfe`

- e1000g
- ixgb
- nge
- nxge
- rge
- xge

Consultez la documentation du fabricant pour savoir si une interface tierce prend en charge la détection de défaillance basée sur les liaisons.

Ces pilotes d'interface réseau contrôlent l'état de la liaison de l'interface et notifient le sous-système de mise en réseau en cas de modification de l'état. En fonction de la situation, le sous-système de mise en réseau définit ou efface alors l'indicateur `RUNNING` de cette interface. Lorsque le démon détecte que l'indicateur `RUNNING` de l'interface a été effacé, il déclenche immédiatement une défaillance de l'interface.

Détection de défaillance basée sur sonde

Le démon `in.mpathd` effectue une détection de défaillance basée sur sonde sur chaque interface possédant une adresse test dans le groupe IPMP. La détection de défaillance basée sur sonde repose sur l'envoi et la réception de messages de sonde ICMP utilisant des adresses test. Ces messages partent de l'interface vers un ou plusieurs systèmes cible sur la même liaison IP. Les adresses test sont décrites à la section “Adresses test” à la page 764. Pour obtenir des informations sur la configuration des adresses test, reportez-vous à la section “Procédure de configuration d'un groupe IPMP avec plusieurs interfaces” à la page 781.

Le démon `in.mpathd` permet de déterminer les systèmes cible à analyser dynamiquement. Les routeurs connectés à la liaison IP sont sélectionnés automatiquement en tant que cibles pour les tests. En l'absence de routeur sur la liaison, `in.mpathd` envoie des sondes aux hôtes voisins sur la liaison. Un paquet multidiffusion envoyé à toutes les adresses d'hôtes multidiffusion, `224.0.0.1` dans IPv4 et `ff02::1` dans IPv6, détermine les hôtes à utiliser en tant que systèmes cible. Les premiers hôtes qui répondent aux paquets d'écho sont sélectionnés en tant que cibles pour les sondes. Si `in.mpathd` ne trouve aucun routeur ou hôte ayant répondu aux paquets d'écho ICMP, `in.mpathd` ne pourra pas détecter les défaillances basées sur sonde.

Vous pouvez utiliser des routes d'hôte afin de configurer de façon explicite une liste de systèmes cible en vue d'une utilisation par `in.mpathd`. Pour obtenir des instructions, reportez-vous à la section “Configuration de systèmes cible” à la page 785.

Afin de garantir le bon fonctionnement de chaque interface du groupe IPMP, `in.mpathd` analyse toutes les cibles séparément via toutes les interfaces du groupe IPMP. Si, après cinq tests consécutifs, aucune réponse n'est obtenue, `in.mpathd` considère que l'interface est défaillante. La fréquence des tests dépend du *temps de détection de défaillance*. Le temps de détection de défaillance par défaut est de 10 secondes. Cependant, vous pouvez régler le temps de détection

de défaillance dans le fichier `/etc/default/mpathd`. Vous trouverez des instructions à la section "Procédure de configuration du fichier `/etc/default/mpathd`" à la page 800.

Pour un temps de détection de réparation de 10 secondes, la fréquence des tests est d'environ une sonde toutes les deux secondes. Le temps de détection de réparation est le double de celui de détection de défaillance, soit 20 secondes par défaut, afin d'assurer la réception de 10 sondes consécutives. Les temps de détection de défaillance et de réparation s'appliquent uniquement à la détection de défaillance basée sur sonde.

Remarque – Dans un groupe IPMP composé de VLAN, la détection de défaillance basée sur lien est implémentée par lien physique et de ce fait, affecte tous les VLAN se trouvant sur ce lien. La détection de défaillance basée sur lien est effectuée par lien VLAN. Par exemple, `bge0/bge1` et `bge1000/bge1001` sont configurés au sein du même groupe. Si le câble de `bge0` est débranché, la détection de défaillance basée sur lien signale la défaillance immédiate de `bge0` et de `bge1000`. Toutefois, si l'accès à toutes les cibles de sondes sur `bge0` est interrompu, seule la défaillance de `bge0` est signalée car `bge1000` dispose de ses propres cibles de sondes sur son VLAN.

Défaillances de groupe

Une *défaillance de groupe* survient lorsque la totalité des interfaces d'un groupe IPMP sont défaillantes au même moment. Le démon `in.mpathd` n'effectue pas de basculement dans le cas d'une défaillance de groupe. En outre, aucun basculement ne se produit lorsque tous les systèmes cible sont défaillants au même moment. Dans ce cas, `in.mpathd` vide la totalité de ses systèmes cible actuels et détecte de nouveaux systèmes cible.

Détection de réparation d'interface physique

Pour que le démon `in.mpathd` considère qu'une interface est réparée, l'indicateur `RUNNING` doit être configuré pour celle-ci. En cas d'utilisation de la détection de défaillance basée sur sonde, le démon `in.mpathd` doit recevoir les réponses de 10 paquets de sonde consécutifs en provenance de l'interface avant qu'elle ne soit considérée comme étant réparée. Lorsqu'une interface est considérée comme étant réparée, toute adresse ayant basculé vers une autre interface bascule à nouveau vers celle-ci. Si l'interface était configurée comme étant active avant sa défaillance, une fois réparée, elle peut reprendre l'envoi et la réception de trafic.

Description du basculement d'interface

Les deux exemples suivants illustrent une configuration typique et sa modification automatique en cas de défaillance d'une interface. En cas de défaillance de l'interface `hme0`, toutes les adresses de données se déplacent de `hme0` à `hme1`.

EXEMPLE 30–1 Configuration d'interface avant une défaillance

```
hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
     mtu 1500 index 2
     inet 192.168.85.19 netmask ffffff00 broadcast 192.168.85.255
     groupname test
hme0:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
     mtu 1500
     index 2 inet 192.168.85.21 netmask ffffff00 broadcast 192.168.85.255
hme1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
8     inet 192.168.85.20 netmask ffffff00 broadcast 192.168.85.255
     groupname test
hme1:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
     mtu 1500
     index 2 inet 192.168.85.22 netmask ffffff00 broadcast 192.168.85.255
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
     inet6 fe80::a00:20ff:feb9:19fa/10
     groupname test
hme1: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
     inet6 fe80::a00:20ff:feb9:1bfc/10
     groupname test
```

EXEMPLE 30–2 Configuration d'interface après une défaillance

```
hme0: flags=19000842<BROADCAST,RUNNING,MULTICAST,IPv4,
      NOFAILOVER,FAILED> mtu 0 index 2
      inet 0.0.0.0 netmask 0
      groupname test
hme0:1: flags=19040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,
      NOFAILOVER,FAILED> mtu 1500 index 2
      inet 192.168.85.21 netmask ffffff00 broadcast 10.0.0.255
hme1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 192.168.85.20 netmask ffffff00 broadcast 192.168.85.255
      groupname test
hme1:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,
      NOFAILOVER> mtu 1500
      index 2 inet 192.168.85.22 netmask ffffff00 broadcast 10.0.0.255
hme1:2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 6
      inet 192.168.85.19 netmask ffffff00 broadcast 192.168.18.255
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER,FAILED> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:19fa/10
      groupname test
hme1: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:1bfc/10
      groupname test
```

Comme vous pouvez l'observer, l'indicateur `FAILED` est défini sur `hme0` afin d'indiquer que cette interface est défaillante. Notez également que `hme1:2` a été créé. `hme1:2` était à l'origine `hme0`. L'adresse `192.168.85.19` devient accessible via `hme1`.

Les appartenances multidiffusion associées à `192.168.85.19` peuvent toujours recevoir des paquets, mais elles les reçoivent à présent via `hme1`. Lors du basculement de l'adresse `192.168.85.19` de `hme0` vers `hme1`, l'adresse fictive `0.0.0.0` a été créée sur `hme0`. Grâce à

l'adresse fictive, il reste possible d'accéder à `hme0`. `hme0:1` ne peut pas exister sans `hme0`. L'adresse fictive est supprimée dès que le basculement s'effectue.

De même, l'adresse IPv6 a basculé de `hme0` vers `hme1`. Dans IPv6, les appartenances multidiffusion sont associées aux index d'interface. Les appartenances multidiffusion basculent également de `hme0` vers `hme1`. Toutes les adresses configurées par `in.ndpd` se déplacent également. Cette action ne figure pas dans les exemples.

Le démon `in.mpathd` poursuit l'analyse de l'interface défaillante `hme0`. Lorsque le démon a reçu 10 réponses consécutives pour une durée de détection de réparation par défaut de 20 secondes, il considère l'interface comme réparée. L'indicateur `RUNNING` étant également défini sur `hme0`, le démon appelle le rétablissement. une fois le rétablissement effectué, la configuration d'origine est restaurée.

Pour obtenir une description des messages d'erreur consignés dans la console lors des défaillances et des réparations, consultez la page de manuel `in.mpathd`(1M).

IPMP et reconfiguration dynamique

La fonctionnalité DR (Dynamic Reconfiguration, reconfiguration dynamique) permet de reconfigurer le matériel système, notamment les interfaces, lorsque le système est en cours d'exécution. Cette section explique le mode d'interopération entre la DR et IPMP.

Dans un système prenant en charge la reconfiguration dynamique des cartes d'interface réseau, IPMP permet de préserver la connectivité et d'éviter toute perturbation des connexions existantes. Vous pouvez connecter, déconnecter ou reconnecter des cartes d'interface réseau en toute sécurité sur un système prenant en charge la DR et utilisant IPMP. Cela est possible car IPMP est intégré à la structure du RCM (Reconfiguration Coordination Manager, gestionnaire de coordination de reconfiguration). Le *RCM* assure la gestion de la reconfiguration dynamique des composants système.

En règle générale, la commande `cfgadm` permet d'effectuer des opérations de reconfiguration dynamique. Cependant, certaines plates-formes fournissent d'autres méthodes. Reportez-vous à la documentation de votre plate-forme pour obtenir des informations supplémentaires. Vous trouverez des informations spécifiques relatives à la DR dans les ressources suivantes.

TABLEAU 30–1 Ressources documentaires sur la DR

Description	Référence
Informations détaillées sur la commande `cfgadm`	Page de manuel `cfgadm`(1M).
Information spécifiques sur la DR dans l'environnement Sun Cluster	*Sun Cluster 3.1 System Administration Guide*

TABLEAU 30–1 Ressources documentaires sur la DR *(Suite)*

Description	Référence
Informations spécifiques sur la DR dans l'environnement Sun Fire	*Sun Fire 880 Dynamic Reconfiguration Guide*
Introduction à la DR et à la commande `cfgadm`	Chapitre 6, "Dynamically Configuring Devices (Tasks)" du *System Administration Guide: Devices and File Systems*
Tâches d'administration de groupes IPMP sur un système prenant en charge la DR	"Remplacement d'une interface physique défaillante sur des systèmes prenant la DR en charge" à la page 795

Connexion de cartes d'interface réseau

Vous pouvez ajouter des interfaces à un groupe IPMP à tout moment à l'aide de la commande `ifconfig`, comme décrit à la section "Procédure de configuration d'un groupe IPMP avec plusieurs interfaces" à la page 781. Par conséquent, toutes les interfaces sur des composants système connectés après l'initialisation du système peuvent être montées et ajoutées à un groupe IPMP existant. Le cas échéant, vous pouvez également configurer les nouvelles interfaces ajoutées dans leur propre groupe IPMP.

Ces interfaces et les adresses de données configurées dessus peuvent immédiatement être utilisées par le groupe IPMP. Cependant, pour que le système configure et utilise les interfaces automatiquement après la réinitialisation, vous devez créer un fichier `/etc/hostname.`*interface* pour chaque nouvelle interface. Pour obtenir des instructions, reportez-vous à la section Configuration d'une interface physique après l'installation du système.

Si un fichier `/etc/hostname.`*interface* existe déjà lors de la connexion de l'interface, le RCM configure l'interface automatiquement, en fonction du contenu du fichier. Par conséquent, la configuration de l'interface est la même que celle qu'elle obtiendrait après l'initialisation du système.

Déconnexion de cartes d'interface réseau

Toutes les requêtes de déconnexion de composants système contenant des cartes d'interface réseau sont d'abord vérifiées afin de garantir un connectivité ininterrompue. Ainsi, par défaut, il est impossible de déconnecter une carte d'interface réseau ne faisant pas partie d'un groupe IPMP. La déconnexion est également impossible dans le cas d'une carte d'interface réseau qui contient les seules interfaces en état de fonctionnement d'un groupe IPMP. Cependant, si vous devez retirer le composant système, l'option `-f` de `cfgadm` permet de contourner ce comportement ; vous trouverez une explication à la page de manuel `cfgadm(1M)`.

Si les vérifications sont réussies, les adresses de données associées à la carte d'interface réseau déconnectée basculent vers une autre carte du même groupe, comme dans le cas d'une défaillance de la carte déconnectée. Une fois la carte d'interface réseau déconnectée, la configuration des adresses test présentes sur ses interfaces est annulée. Ensuite, la carte d'interface réseau est démontée du système. En cas d'échec de l'une de ces étapes, ou de défaillance de la reconfiguration dynamique ou autre matériel sur le même composant système, l'état d'origine de la configuration précédente est restauré. Vous devriez recevoir un message de statut à propos de cet événement. Dans le cas contraire, la demande de déconnexion est traitée. Vous pouvez retirer le composant du système. Aucune connexion existante n'est interrompue.

Reconnexion d'une carte d'interface réseau

Le RCM enregistre les informations de configuration associées à toute carte d'interface réseau déconnectée d'un système en cours d'exécution. Par conséquent, le RCM traite la reconnexion d'une carte d'interface réseau précédemment déconnectée comme il le ferait pour la connexion d'une nouvelle carte d'interface réseau. Le RCM n'effectue que le montage.

Cependant, les cartes réseau reconnectées disposent généralement d'un fichier `/etc/hostname.fichier` *interface*. Dans ce cas, le RCM configure automatiquement l'interface en fonction du contenu du fichier `/etc/hostname. fichier` *interface*. De plus, le RCM informe le démon `in.mpathd` de chaque adresse de données hébergée à l'origine sur l'interface reconnectée. Par conséquent, une fois que l'interface reconnectée fonctionne correctement, toutes ses adresses de données sont rétablies sur l'interface reconnectée, comme si elle avait été reconnectée.

Si la carte d'interface réseau reconnectée ne possède pas de fichier `/etc/hostname.` *interface*, aucune information de configuration n'est disponible. Le RCM ne dispose pas d'informations relatives à la configuration de l'interface. Par conséquent, les adresses basculées vers une autre interface ne sont pas rétablies.

Cartes d'interface réseau manquantes à l'initialisation du système

Les cartes d'interface réseau absentes lors de l'initialisation du système constituent une instance spéciale de détection de défaillance. Lors de l'initialisation, les scripts de démarrage réalisent le suivi de toutes les interfaces possédant des fichiers `/etc/hostname.`*interface* qu'il est impossible de monter. Toute adresse de données se trouvant dans un fichier `/etc/hostname.` *interface* d'une telle interface est automatiquement hébergée sur une autre interface dans le groupe IPMP.

Si cela venait à se produire, vous recevrez un message d'erreur similaire à ce qui suit :

```
moving addresses from failed IPv4 interfaces: hme0 (moved to hme1)
moving addresses from failed IPv6 interfaces: hme0 (moved to hme1)
```

Si aucune autre interface n'existe, vous recevrez un message d'erreur similaire à ce qui suit :

```
moving addresses from failed IPv4 interfaces: hme0 (couldn't move;
   no alternative interface)
 moving addresses from failed IPv6 interfaces: hme0 (couldn't move;
   no alternative interface)
```

Remarque – Dans ce cas de détection de défaillance, seules les adresses de données spécifiées explicitement dans le fichier `/etc/hostname.` *interface* de l'interface manquant sont déplacés vers une autre interface. Toute adresse acquise par d'autres moyens, par exemple via RARP ou DHCP, n'est ni acquise ni déplacée.

Si une interface existante porte le nom d'une autre interface manquante lors de l'initialisation du système et a été reconnectée à l'aide de la reconfiguration dynamique, le RCM monte l'interface automatiquement. Ensuite, le RCM configure l'interface en fonction du contenu de son fichier `/etc/hostname.`*interface.* Enfin, le RCM rétablit toutes les adresses de données, comme si l'interface avait été réparée. Par conséquent, la configuration réseau finale est identique à celle qui aurait été effectuée si l'interface avait été présente lors de l'initialisation du système.

◆ ◆ ◆ CHAPITRE 31

Administration d'IPMP (tâches)

Ce chapitre décrit les tâches relatives à l'administration des groupes d'interfaces avec IPMP (multiacheminement sur réseau IP). Les rubriques traitées sont les suivantes :

Pour obtenir une présentation des concepts relatifs à IPMP, reportez-vous au Chapitre 30, "Présentation d'IPMP".

Configuration d'IPMP (liste des tâches)

Cette section contient des liens vers les tâches décrites dans ce chapitre.

Configuration et administration de groupes IPMP (liste des tâches)

Tâche	Description	Voir
Planification d'un groupe IPMP.	Répertorie la totalité des informations complémentaires et des tâches requises préalables à la configuration d'un groupe IPMP.	"Procédure de planification pour un groupe IPMP" à la page 779

Tâche	Description	Voir
Configuration d'un groupe d'interface IPMP composé de plusieurs interfaces.	Configure plusieurs interfaces en tant que membres d'un groupe IPMP.	"Procédure de configuration d'un groupe IPMP avec plusieurs interfaces" à la page 781
Configuration d'un groupe IPMP où l'une des interfaces est une interface de réserve.	Configure l'une des interfaces d'un groupe d'interfaces IPMP en tant qu'interface de réserve.	"Procédure de configuration d'une interface de réserve pour un groupe IPMP" à la page 788
Configuration d'un groupe IPMP composé d'une interface unique.	Crée un groupe IPMP composé d'une seule interface.	"Procédure de configuration d'un groupe IPMP à interface unique" à la page 790
Affichage du groupe IPMP auquel appartient une interface physique.	Explication sur le mode d'obtention du nom du groupe IPMP d'une interface à partir de la sortie de la commande `ifconfig`.	"Procédure d'affichage de l'appartenance d'une interface à un groupe IPMP" à la page 792
Ajout d'une interface à un groupe IPMP.	Configuration d'une nouvelle interface en tant que membre d'un groupe IPMP existant.	"Procédure d'ajout d'une interface à un groupe IPMP" à la page 792
Retrait d'une interface d'un groupe IPMP.	Fournit des explications sur le retrait d'une interface d'un groupe IPMP.	"Procédure de suppression d'une interface d'un groupe IPMP" à la page 793
Déplacement d'une interface à partir d'un groupe IPMP existant vers un groupe différent.	Déplacement d'interfaces au sein de groupes IPMP.	"Procédure de déplacement d'une interface d'un groupe IPMP vers un autre" à la page 794
Modification de trois paramètres par défaut du démon `in.mpathd`.	Personnalise le temps de détection de défaillance et autres paramètres du démon `in.mpathd` .	"Procédure de configuration du fichier `/etc/default/mpathd`" à la page 800

Administration d'IPMP sur des interfaces prenant en charge la reconfiguration dynamique (liste des tâches)

Tâche	Description	Voir
Retrait d'une interface défaillante.	Retrait du système d'une interface défaillante.	"Procédure de suppression d'une interface physique défaillante (DR puis déconnexion)" à la page 795
Remplacement d'une interface défaillante.	Remplacement d'une interface défaillante.	"Procédure de remplacement d'une interface physique défaillante (DR puis connexion)" à la page 796

Tâche	Description	Voir
Récupération d'une interface non configurée lors de l'initialisation.	Récupération d'une interface défaillante.	"Procédure de récupération d'une interface physique absente lors de l'initialisation du système" à la page 797

Configuration de groupes IPMP

Cette section décrit les procédures pour la configuration de groupes IPMP. Elle propose également une description de la configuration d'une interface en tant qu'interface de réserve.

Planification d'un groupe IPMP

Avant de configurer des interfaces sur un système comme faisant partie d'un groupe IPMP, vous devez effectuer une planification de préconfiguration.

▼ Procédure de planification pour un groupe IPMP

La procédure suivante inclut les tâches de planification et les informations à collecter préalablement à la configuration du groupe IPMP. Il n'est pas obligatoire de réaliser les tâches dans l'ordre dans lequel elles sont décrites.

1 Déterminez les interfaces du système qui feront partie du groupe IPMP.

Un groupe IPMP se compose en règle générale d'au moins deux interfaces physiques connectées à la même liaison IP. Vous pouvez cependant configurer un groupe IPMP à interface unique si nécessaire. Pour une introduction sur les groupes IPMP, reportez-vous à la section "Configurations d'interfaces IPMP" à la page 767. Par exemple, vous pouvez configurer le commutateur Ethernet ou le même sous-réseau IP dans le même groupe IPMP. Vous pouvez configurer le nombre d'interfaces de votre choix dans un même groupe IPMP.

Vous ne pouvez pas utiliser le paramètre `group` de la commande `ifconfig` avec des interfaces logiques. Par exemple, vous pouvez utiliser le paramètre `group` avec `hme0`, mais pas avec `hme0:1` .

2 Assurez-vous que chaque interface du groupe dispose d'une adresse MAC unique.

Pour obtenir des instructions, reportez-vous à la section "SPARC : Garantie de l'unicité de l'adresse MAC d'une interface" à la page 154.

3 Attribuez un nom au groupe IPMP.

Tout nom autre que NULL est approprié pour le groupe. Utilisez un nom qui identifie la liaison IP à laquelle sont connectées les interfaces.

4 Assurez-vous que le même ensemble de modules STREAMS est déplacé et configuré sur toutes les interfaces dans le groupe IPMP.

Toutes les interfaces dans un même groupe doivent disposer de modules STREAMS configurés selon le même ordre.

a. Vérifiez l'ordre des modules STREAMS sur toutes les interfaces du groupe IPMP futur.

Vous pouvez imprimer une liste de modules STREAMS à l'aide de la commande `ifconfig` *interface* `modlist`. Voici un exemple de sortie de la commande `ifconfig` pour une interface `hme0` interface :

```
# ifconfig hme0 modlist
    0 arp
    1 ip
    2 hme
```

Les interfaces existent normalement en tant que pilotes réseau directement sous le module IP, tel qu'illustré dans la sortie de `ifconfig hme0 modlist`. Aucune configuration supplémentaire ne devrait être nécessaire.

Cependant, certaines technologies comme NCA ou IP Filter, s'insèrent en tant que modules STREAMS entre le module IP et le pilote de réseau. Des problèmes peuvent se produire dans le comportement des interfaces dans un même groupe IPMP.

Dans le cas d'un module STREAMS avec état, des comportements inattendus peuvent être observés lors du basculement, même en cas de déplacement d'un même module sur toutes les interfaces d'un groupe. Cependant, vous pouvez utiliser des modules STREAMS sans état, à condition que vous les déplaciez selon le même ordre sur toutes les interfaces du groupe IPMP.

b. Déplacez les modules d'une interface selon l'ordre standard pour le groupe IPMP.

`ifconfig` *interface* **`modinsert`** *module-name*

```
ifconfig hme0 modinsert ip
```

5 Utilisez le même format d'adressage IP sur toutes les interfaces du groupe IPMP.

Si une interface est configurée pour IPv4, toutes les interfaces du groupe doivent être configurées pour IPv4. Admettons que vous disposez d'un groupe IPMP composé d'interfaces provenant de plusieurs cartes d'interface réseau. Si vous ajoutez l'adressage IPv6 aux interfaces d'un NIC, toutes les interfaces du groupe IPMP doivent être configurées pour la prise en charge d'IPv6.

6 Assurez-vous que toutes les interfaces du groupe IPMP sont connectées au même lien IP.

7 Assurez-vous que le groupe IPMP ne contient pas d'interfaces avec différents types de média réseau.

Les interfaces regroupées doivent être du même type, comme défini dans `/usr/include/net/if_types.h` . Par exemple, vous ne pouvez pas combiner les interfaces

Ethernet et Token ring dans un groupe IPMP. En outre, vous ne pouvez pas combiner un bus d'interfaces Token avec des interfaces ATM (Asynchronous Transfer Mode, mode de transfert asynchrone) dans le même groupe IPMP.

8 **En cas d'IPMP avec interfaces ATM, configurez les interfaces ATM en mode d'émulation LAN.**

IPMP n'est pas pris en charge par les interfaces préférant l'IP classique à l'ATM.

Configuration de groupes IPMP

Cette section décrit les tâches relatives à la configuration pour un groupe IPMP classique contenant au moins deux interfaces physiques.

- Les groupes IPMP à plusieurs interfaces sont décrits à la section "Groupe IPMP" à la page 762.
- Pour la planification de tâches, reportez-vous à la section "Planification d'un groupe IPMP" à la page 779.
- Pour configurer un groupe IPMP avec une seule interface physique, reportez-vous à la section "Configuration de groupes IPMP avec une interface physique unique" à la page 790.

▼ Procédure de configuration d'un groupe IPMP avec plusieurs interfaces

Les étapes suivantes permettent de configurer un groupe IPMP et s'appliquent également à la configuration de réseaux VLAN dans un groupe IPMP.

Avant de commencer Configurez au préalable les adresses IPv4 et , le cas échéant, les adresses IPv6 de toutes les interfaces du futur groupe IPMP.

Attention – Vous ne devez configurer qu'un seul groupe IPMP pour chaque sous-réseau ou domaine de diffusion L2. Pour plus d'informations, reportez-vous à la section "Exigences de base d'IPMP" à la page 763.

1 **Sur le système sur lequel vous devez configurer les interfaces, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Placez chaque interface physique dans un groupe IPMP.**

```
# ifconfig interface group group-name
```

Par exemple, pour placer `hme0` et `hme1` sous le groupe `testgroup1`, saisissez les commandes suivantes :

```
# ifconfig hme0 group testgroup1
# ifconfig hme1 group testgroup1
```

Évitez l'utilisation d'espaces dans les noms de groupes. L'affichage du statut `ifconfig` n'affiche pas les espaces. Par conséquent, n'utilisez pas deux noms de groupes similaires dont la seule différence est un espace. Si l'un des noms de groupe contient un espace, ces noms s'afficheront de la même façon dans l'affichage de statut.

Dans un environnement à double pile, si l'on place l'instance IPv4 d'une interface dans un groupe particulier, l'instance IPv6 est automatiquement placée dans ce même groupe.

3 (Facultatif) Configurez une adresse test IPv4 sur une ou plusieurs interfaces physiques.

La configuration d'une adresse test est nécessaire uniquement si vous souhaitez utiliser la détection de défaillance basée sur sonde sur une interface spécifique. Les adresses test sont configurées en tant qu'interfaces logiques de l'interface physique spécifiée à la commande `ifconfig`.

Si une interface du groupe est destinée à devenir l'interface de réserve, ne configurez pas d'adresse test pour celle-ci à cette étape. La configuration de l'adresse test de l'interface de réserve fait partie de la tâche décrite à la section "Procédure de configuration d'une interface de réserve pour un groupe IPMP" à la page 788.

Utilisez la syntaxe de la commande `ifconfig` pour configurer une adresse test :

 # ifconfig *interface* **addif** *ip-address parameters* **-failover deprecated up**

Par exemple, vous pouvez créer l'adresse test suivante pour l'interface réseau principale `hme0` :

```
# ifconfig hme0 addif 192.168.85.21 netmask + broadcast + -failover deprecated up
```

Cette commande définit les paramètres suivants pour l'interface réseau principale `hme0` :

- adresse définie sur `192.168.85.21` ;
- masque de réseau et adresse de diffusion définie sur la valeur par défaut ;
- options `-failover` et `deprecated` définies.

Remarque – Marquez une adresse test IPv4 comme étant désapprouvée (`deprecated`) afin d'empêcher les applications d'utiliser cette adresse test.

---

4 Vérifiez la configuration IPv4 pour une interface spécifique.

A tout moment, pour afficher le statut actuel d'une interface, saisissez la commande `ifconfig` *interface*. Pour de plus amples informations sur l'affichage du statut d'une interface, reportez-vous à la section Méthode d'obtention d'informations sur une interface spécifique.

Vous pouvez obtenir des informations à propos de la configuration de l'adresse test d'une interface physique en spécifiant l'interface logique attribuée à l'adresse test.

```
# ifconfig hme0:1
    hme0:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
    mtu 1500 index 2
    inet 192.168.85.21 netmask ffffff00 broadcast 192.168.85.255
```

5 (Facultatif) Le cas échéant, configurez une adresse de test IPv6.

```
# ifconfig interface inet6 -failover
```

Les interfaces physiques disposant d'adresses IPv6 sont placées dans le même groupe IPMP que les adresses IPv4 des interfaces. Cela se produit lorsque vous configurez l'interface physique avec des adresses IPv4 dans un groupe IPMP. Si vous placez des interfaces physiques disposant d'adresses IPv6 dans un groupe IPMP, les interfaces physiques disposant d'adresses IPv4 sont implicitement placées dans un groupe IPMP.

Par exemple, pour configurer `hme0` avec une adresse test IPv6, saisissez ce qui suit :

```
# ifconfig hme0 inet6 -failover
```

Il est inutile de marquer une adresse test IPv6 comme étant désapprouvée afin d'éviter que les applications utilisent l'adresse test.

6 Vérifiez la configuration IPv6.

```
# ifconfig hme0 inet6
    hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
            inet6 fe80::a00:20ff:feb9:17fa/10
            groupname test
```

L'adresse test IPv6 correspond à l'adresse lien-local de l'interface.

7 (Facultatif) Conservation de la configuration du groupe IPMP après réinitialisation.

- Pour IPv4, ajoutez la ligne suivante au fichier `/etc/hostname.` *interface* :

  ```
  interface-address <parameters> group group-name up \
      addif logical-interface -failover deprecated <parameters> up
  ```

  Dans ce cas, l'adresse test IPv4 est configurée uniquement lors de la réinitialisation suivante. Si vous souhaitez que la configuration soit appelée dans la session actuelle, effectuez les étapes 1 et 2 et éventuellement l'étape 3.

- Pour IPv6, ajoutez la ligne suivante au fichier `/etc/hostname6. fichier` *interface* :

  ```
  -failover group group-name up
  ```

  Cette adresse test IPv6 est configurée à la réinitialisation suivante. Si vous souhaitez que la configuration soit appelée dans la session actuelle, effectuez les étapes 1 et 2 et éventuellement l'étape 5.

8 **(Facultatif) Ajoutez des interfaces supplémentaires au groupe IPMP en répétant les étapes 1 à 6.**

Vous pouvez ajouter de nouvelles interfaces à un groupe existant sur un système actif. Cependant, les modifications ne sont pas conservées après réinitialisation.

Exemple 31–1 Configuration d'un groupe IPMP avec deux interfaces

En supposant que vous souhaitez effectuer ce qui suit :

- définir le masque de réseau et l'adresse de réseau sur la valeur par défaut ;
- configurer l'interface avec l'adresse test `192.168.85.21`.

Saisissez la commande suivante :

```
# ifconfig hme0 addif 192.168.85.21 netmask + broadcast + -failover deprecated up
```

Marquez une adresse test IPv4 comme étant désapprouvée (`deprecated`) afin d'empêcher les applications d'utiliser cette adresse test. Reportez-vous à la section “Procédure de configuration d'un groupe IPMP avec plusieurs interfaces” à la page 781.

Pour activer l'attribut de basculement de l'adresse, utilisez l'option `failover` sans le tiret.

Toutes les adresses IP test d'un groupe IPMP doivent utiliser le même préfixe de réseau. Les adresses IP test doivent appartenir à un sous-réseau IP unique.

Exemple 31–2 Conservation de la configuration du groupe IPMP IPv4 après réinitialisation

Supposons que vous souhaitez créer un groupe IPMP appelé `testgroup1` avec la configuration suivante :

- interface physique `hme0` avec adresse de données `192.168.85.19` ;
- interface logique avec adresse test `192.168.85.21` ;

Remarque – Dans cet exemple, l'interface physique et l'adresse de données sont associées. Il en va de même pour l'interface logique et l'adresse test. Cependant, il n'existe aucune relation inhérente entre une interface type et l'adresse type.

- options `deprecated` et `-failover` définies ;
- masque de réseau et adresse de diffusion définie sur la valeur par défaut ;

Vous ajoutez la ligne suivante au fichier `/etc/hostname.hme0` :

```
192.168.85.19 netmask + broadcast + group testgroup1 up \
    addif 192.168.85.21 deprecated -failover netmask + broadcast + up
```

De même, pour placer la seconde interface `hme1` sous le même groupe `testgroup1` et configurer une adresse test, ajoutez la ligne suivante :

```
192.168.85.20 netmask + broadcast + group testgroup1 up \
    addif 192.168.85.22 deprecated -failover netmask + broadcast + up
```

Exemple 31–3 Conservation de la configuration du groupe IPMP IPv6 après réinitialisation

Pour créer un groupe test pour l'interface `hme0` avec une adresse IPv6, ajoutez la ligne suivante au fichier `/etc/hostname6.hme0` :

```
-failover group testgroup1 up
```

De même, pour placer la seconde interface `hme1` dans le groupe `testgroup1` et configurer une adresse test, ajoutez la ligne suivante au fichier `/etc/hostname6.hme1` :

```
-failover group testgroup1 up
```

Erreurs fréquentes

Pendant la configuration du groupe IPMP, `in.mpathd` génère de nombreux messages sur la console système ou dans le fichier `syslog`. Ces messages à caractère informatif indiquent que la configuration IPMP fonctionne correctement.

- Ce message indique que l'interface `hme0` a été ajoutée au groupe IPMP `testgroup1`. Cependant, `hme0` ne possède pas d'adresse test configurée. Pour activer la détection de défaillance basée sur sonde, attribuez une adresse test à l'interface.

  ```
  May 24 14:09:57 host1 in.mpathd[101180]:
  No test address configured on interface hme0;
  disabling probe-based failure detection on it.
  testgroup1
  ```

- Ce message s'affiche pour toutes les interfaces possédant uniquement des adresses IPv4 ajoutées à un groupe IPMP.

  ```
  May 24 14:10:42 host4 in.mpathd[101180]:
  NIC qfe0 of group testgroup1 is not
  plumbed for IPv6 and may affect failover capability
  ```

- Ce message s'affiche après la configuration d'une adresse test pour une interface.

  ```
  Created new logical interface hme0:1
  May 24 14:16:53 host1 in.mpathd[101180]:
  Test address now configured on interface hme0;
   enabling probe-based failure detection on it
  ```

Voir aussi

Pour que la configuration du groupe IPMP soit de type actif-de réserve, reportez-vous à la section “Procédure de configuration d'une interface de réserve pour un groupe IPMP” à la page 788.

Configuration de systèmes cible

La détection de défaillance basée sur sonde nécessite l'utilisation de systèmes cible, comme expliqué dans la section “Détection de défaillance basée sur sonde” à la page 770. Pour certains groupes IPMP, les cibles par défaut utilisées par `in.mpathd` sont suffisantes. Cependant, pour

certains groupes IPMP, il est nécessaire de configurer des cibles spécifiques pour la détection de défaillance basée sur sonde. La détection de défaillance basée sur sonde s'effectue en configurant des routes hôte en tant que cibles de sondes dans la table de routage. Les routes hôte configurées dans la table de routage figurent dans la liste avant le routeur par défaut. Par conséquent, IPMP utilise les routes hôte définies explicitement pour la sélection de cibles. Il existe deux méthodes permettant de spécifier directement les cibles : définition manuelle de routes hôte ou création d'un script shell pouvant devenir un script de démarrage.

Tenez compte des critères suivants lorsque vous devez sélectionner les hôtes de votre réseau les plus adaptés en tant que cibles.

- Assurez-vous que les cibles potentielles sont disponibles et en cours d'exécution. Établissez la liste de leurs adresses IP.
- Assurez-vous que les interfaces cible se trouvent sur le même réseau que le groupe IPMP configuré.
- Le masque de réseau et l'adresse de diffusion des systèmes cible doivent être les mêmes que ceux du groupe IPMP.
- L'hôte cible doit pouvoir répondre aux requêtes ICMP provenant de l'interface qui utilise la détection de défaillance basée sur sonde.

▼ Procédure de spécification manuelle de systèmes cible pour la détection de défaillance basée sur sonde

1 Connectez-vous à l'aide de votre compte utilisateur au système dans lequel vous configurez la détection de défaillance basée sur sonde.

2 Ajoutez une route à un hôte spécifique, à utiliser en tant que cible dans le cadre de la détection de défaillance basée sur sonde.

```
$ route add -host destination-IP gateway-IP -static
```

Remplacez les valeurs de *IP-destination* et *IP-passerelle* par l'adresse IPv4 de l'hôte à utiliser en tant que cible. Par exemple, saisissez ce qui suit afin de spécifier le système cible `192.168.85.137` qui se trouve sur le même sous-réseau que les interfaces du groupe IPMP `testgroup1`.

```
$ route add -host 192.168.85.137 192.168.85.137 -static
```

3 Ajoutez les routes vers les hôtes supplémentaires du réseau à utiliser en tant que systèmes cible.

▼ Procédure de spécification de systèmes cible dans un script shell

1 **Sur le système sur lequel vous avez configuré un groupe IPMP, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Créez un script shell définissant les routes statiques vers les cibles proposées.**

Par exemple, vous pouvez créer un script shell intitulé `ipmp.targets` avec le contenu suivant :

```
TARGETS="192.168.85.117 192.168.85.127 192.168.85.137"

case "$1" in
        'start')
            /usr/bin/echo "Adding static routes for use as IPMP targets"
          for target in $TARGETS; do
       /usr/sbin/route add -host $target $target
          done
                  ;;
          'stop')
                /usr/bin/echo "Removing static routes for use as IPMP targets"
           for target in $TARGETS; do
          /usr/sbin/route delete -host $target $target
           done
                  ;;
  esac
```

3 **Copiez le script shell dans le répertoire du script de démarrage.**

```
# cp ipmp.targets /etc/init.d
```

4 **Modifiez les permissions dans le nouveau script de démarrage.**

```
# chmod 744 /etc/init.d/ipmp.targets
```

5 **Modifiez la propriété du nouveau script de démarrage.**

```
# chown root:sys /etc/init.d/ipmp.targets
```

6 **Créez une liaison pour le script de démarrage dans le répertoire `/etc/init.d`.**

```
# ln /etc/init.d/ipmp.targets /etc/rc2.d/S70ipmp.targets
```

Le préfixe S70 dans le nom de fichier `S70ipmp.targets` ordonne le nouveau script correctement en fonction des autres scripts de démarrage.

Configuration d'interfaces de réserve

Cette procédure permet d'attribuer une configuration active-de réserve au groupe IPMP. Pour obtenir des informations supplémentaires sur ce type de configuration, reportez-vous à la section "Configurations d'interfaces IPMP" à la page 767.

▼ Procédure de configuration d'une interface de réserve pour un groupe IPMP

Avant de commencer

- Toutes les interfaces doivent être configurées en tant que membres du groupe IPMP.
- Ne configurez pas d'adresse test sur l'interface pour la définir en tant qu'interface de réserve.

Pour obtenir des informations sur la configuration d'un groupe IPMP et l'attribution d'adresses test, reportez-vous à la section "Procédure de configuration d'un groupe IPMP avec plusieurs interfaces" à la page 781.

1 Sur le système sur lequel vous devez configurer les interfaces de réserve, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Configurez une interface en tant qu'interface de réserve et attribuez l'adresse test.

```
# ifconfig interface plumb \
ip-address other-parameters deprecated -failover standby up
```

Une interface de réserve ne peut disposer que d'une adresse IP, l'adresse test. Définissez l'option `-failover` avant l'option `standby up`. Pour `<other-parameters>`, utilisez les paramètres requis par votre configuration, tels que décrits dans la page de manuel `ifconfig(1M)`.

- Par exemple, la commande suivante permet de créer une adresse test IPv4 :

```
# ifconfig hme1 plumb 192.168.85.22 netmask + broadcast + deprecated -failover standby up
```

`hme1`	Définit `hme1` comme étant l'interface physique à configurer en tant qu'interface de réserve.
`192.168.85.22`	Atrtibue cette adresse test à l'interface de réserve.
`deprecated`	Indique que l'adresse test n'est pas utilisée pour les paquets sortants.
`-failover`	Indique que l'adresse test ne bascule pas en cas de défaillance de l'interface.
`standby`	Marque l'interface comme étant l'interface de réserve.

- Par exemple, la commande suivante permet de créer une adresse test IPv6 :

```
# ifconfig hme1 plumb -failover standby up
```

3 Vérifiez les résultats de la configuration de l'interface de réserve.

```
# ifconfig hme1
hme1: flags=69040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER,
      STANDBY,INACTIVE mtu 1500
```

```
index 4 inet 192.168.85.22 netmask ffffff00 broadcast 19.16.85.255
groupname test
```

L'indicateur `INACTIVE` indique que cette interface n'est pas utilisée pour les paquets sortants. En cas de basculement vers cette interface de réserve, l'indicateur `INACTIVE` est effacé.

Remarque – La commande `ifconfig` *interface* permet de vérifier le statut d'une interface. Pour de plus amples informations sur l'affichage du statut d'une interface, reportez-vous à la section "Méthode d'obtention d'informations sur une interface spécifique" à la page 209 .

---

4 (Facultatif) Conservez l'interface de réserve IPv4 après réinitialisation.

Attribuez l'interface au même groupe IPMP et configurez une adresse test pour l'interface de réserve.

Par exemple, pour configurer `hme1` en tant qu'interface de réserve, ajoutez la ligne suivante au fichier `/etc/hostname.hme1` :

```
192.168.85.22 netmask + broadcast + deprecated group test -failover standby up
```

5 (Facultatif) Conservez l'interface de réserve IPv6 après réinitialisation.

Attribuez l'interface au même groupe IPMP et configurez une adresse test pour l'interface de réserve.

Par exemple, pour configurer `hme1` en tant qu'interface de réserve, ajoutez la ligne suivante au fichier `/etc/hostname6.hme1` :

```
-failover group test standby up
```

Exemple 31–4 Configuration d'une interface de réserve pour un groupe IPMP

En supposant que vous souhaitez créer une adresse test avec la configuration suivante :

- interface physique `hme2` en tant qu'interface de réserve ;
- adresse test de `192.168.85.22` ;
- options `deprecated` et `-failover` définies ;
- masque de réseau et adresse de diffusion définie sur la valeur par défaut ;

Vous devez taper ce qui suit :

```
# ifconfig hme2 plumb 192.168.85.22 netmask + broadcast + \
deprecated -failover standby up
```

L'interface est marquée comme interface de réserve une fois que l'adresse est marquée comme étant sans basculement (`NOFAILOVER`).

Saisissez ce qui suit afin de supprimer le statut d'interface de réserve d'une interface :

```
# ifconfig interface -standby
```

Configuration de groupes IPMP avec une interface physique unique

Le basculement est impossible lorsqu'un groupe IPMP dispose d'une seule interface. Cependant, vous pouvez activer la détection de défaillance sur cette interface en l'attribuant à un groupe IPMP. Il est inutile de configurer une adresse IP test dédiée afin d'établir la détection de défaillance pour un groupe IPMP à interface unique. Vous pouvez utiliser une adresse IP unique pour l'envoi de données et la détection de défaillance.

▼ Procédure de configuration d'un groupe IPMP à interface unique

1 Sur le système possédant le groupe IPMP à interface unique, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 Pour IPv4, créez le groupe IPMP à interface unique.

La syntaxe suivante permet d'attribuer une interface unique à un groupe IPMP.

 # ifconfig *interface* **group** *group-name*

Dans l'exemple suivant, l'interface `hme0` est attribuée au groupe IPMP `v4test` :

```
# ifconfig hme0 group v4test
```

Une fois cette étape effectuée, IPMP active la détection de défaillance basée sur lien sur l'interface.

En outre, vous pouvez activer la détection de défaillance basée sur sonde à l'aide de la sous-commande `-failover` de `ifconfig`. Dans l'exemple suivant, la détection de défaillance basée sur sonde est activée sur `hme0` à l'aide de l'adresse IP assignée à `hme0`:

```
# ifconfig hme0 -failover
```

Contrairement aux groupes comptant plusieurs interfaces, la même adresse IP peut servir d'adresse de données et d'adresse de test. Pour que l'adresse de test puisse être utilisée comme adresse de données par les applications, elle ne doit jamais être signalée comme `désapprouvée` dans les groupes IPMP à interface unique.

3 Pour IPv6, créez le groupe IPMP à interface unique.

La syntaxe suivante permet d'attribuer une interface unique à un groupe IPMP :

 # ifconfig *interface* **inet6 group** *group-name*

Par exemple, pour ajouter l'interface unique `hme0` dans le groupe IPMP `v6test`, saisissez ce qui suit :

```
# ifconfig hme0 inet6 group v6test
```

Une fois cette étape effectuée, IPMP active la détection de défaillance basée sur lien sur l'interface.

En outre, vous pouvez activer la détection de défaillance basée sur sonde à l'aide de la sous-commande `-failover` de `ifconfig`. Dans l'exemple suivant, la détection de défaillance basée sur sonde est activée sur `hme0` à l'aide de l'adresse IP assignée à `hme0`:

```
# ifconfig hme0 inet6 -failover
```

Contrairement aux groupes comptant plusieurs interfaces, la même adresse IP peut servir d'adresse de données et d'adresse de test. Pour que l'adresse de test puisse être utilisée comme adresse de données par les applications, elle ne doit jamais être signalée comme `désapprouvée` dans les groupes IPMP à interface unique.

Dans une configuration d'interface physique unique, il est impossible de vérifier si la défaillance s'est produite au niveau du système cible analysé ou au niveau de l'interface. Il est possible d'analyser le système cible en passant par une seule interface physique. Si un seul routeur par défaut se trouve sur le sous-réseau, désactivez IPMP si le groupe contient une interface physique unique. Si un routeur IPv4 et IPv6 par défaut distinct existe, ou si plusieurs routeurs par défaut existent, il est nécessaire d'analyser plusieurs systèmes cible. Vous pouvez par conséquent activer IPMP.

Maintenance de groupes IPMP

Cette section décrit les tâches relatives à la maintenance de groupes IPMP existants et des interfaces qui composent ces groupes. Cette tâche suppose que vous avez déjà configuré un groupe IPMP, tel que décrit dans la section "Configuration de groupes IPMP" à la page 779.

▼ Procédure d'affichage de l'appartenance d'une interface à un groupe IPMP

1 **Sur le système sur lequel est configuré le groupe IPMP, connectez-vous en tant que superutilisateur (ou équivalent).**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour de plus amples informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichage d'informations sur l'interface, y compris le groupe auquel appartient l'interface.**

```
# ifconfig interface
```

3 **Le cas échéant, affichez les informations IPv6 de l'interface.**

```
# ifconfig interface inet6
```

Exemple 31–5 Affichage de groupes d'interfaces physiques

Saisissez ce qui suit afin d'afficher le nom de groupe de `hme0` :

```
# ifconfig hme0
    hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
      index 2 inet 192.168.85.19 netmask ffffff00 broadcast 192.168.85.255
      groupname testgroup1
```

Saisissez ce qui suit afin d'afficher le nom de groupe uniquement pour les informations IPv6 :

```
# ifconfig hme0 inet6
    hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
            inet6 fe80::a00:20ff:feb9:19fa/10
            groupname testgroup1
```

▼ Procédure d'ajout d'une interface à un groupe IPMP

1 **Sur le système sur lequel est configuré le groupe IPMP, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Ajoutez l'interface au groupe IPMP.**

```
# ifconfig interface group group-name
```

L'interface spécifiée dans *interface* devient membre du groupe IPMP *nom-groupe*.

Exemple 31–6 Ajout d'une interface à un groupe IPMP

Saisissez la commande suivante afin d'ajouter `hme0` au groupe IPMP `testgroup2` :

```
# ifconfig hme0 group testgroup2
  hme0: flags=9000843<UP ,BROADCAST,RUNNING,MULTICAST,IPv4,NOFAILOVER> mtu 1500 index 2
  inet 192.168.85.19 netmask ff000000 broadcast 10.255.255.255
  groupname testgroup2
  ether 8:0:20:c1:8b:c3
```

▼ Procédure de suppression d'une interface d'un groupe IPMP

Lorsque vous exécutez le paramètre `group` de la commande `ifconfig` avec une chaîne vide, l'interface est supprimée du groupe IPMP actuel. Faites preuve de prudence lors de la suppression d'interfaces à partir d'un groupe. Dans le cas d'une défaillance d'une autre interface du groupe IPMP, un basculement a pu se produire antérieurement. Par exemple, en cas de défaillance antérieure de `hme0`, toutes les adresses basculent vers `hme1`, si `hme1` fait partie du même groupe. En cas de suppression de `hme1` du groupe, le démon `in.mpathd` renvoie toutes les adresses de basculement à une autre interface du groupe. Si aucune autre interface ne fonctionne dans le groupe, le basculement risque de ne pas restaurer la totalité des accès réseau.

De même, lorsqu'une interface dans un groupe doit être démontée, commencez par retirer l'interface du groupe. Vérifiez ensuite que toutes les adresses IP d'origine de l'interface sont configurées. Le démon `in.mpathd` tente de restaurer la configuration d'origine d'une interface supprimée du groupe. Avant de démonter l'interface, assurez-vous que la configuration est restaurée. Reportez-vous à la section “Description du basculement d'interface” à la page 771 afin d'obtenir une description des interfaces avant et après basculement.

1. **Sur le système sur lequel est configuré le groupe IPMP, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2. **Supprimez l'interface du groupe IPMP.**

   ```
   # ifconfig interface group ""
   ```

   Les guillemets indiquent une chaîne vide.

Exemple 31–7 Suppression d'une interface d'un groupe

Saisissez la commande suivante afin de supprimer `hme0` du groupe IPMP `test` :

```
# ifconfig hme0 group ""
    # ifconfig hme0
    hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
    index 2 inet 192.168.85.19 netmask ffffff00 broadcast 192.168.85.255
    # ifconfig hme0 inet6
    hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    inet6 fe80::a00:20ff:feb9:19fa/10
```

▼ Procédure de déplacement d'une interface d'un groupe IPMP vers un autre

Vous pouvez placer une interface dans un nouveau groupe IPMP lorsque l'interface appartient à un groupe IPMP. Il est inutile de supprimer l'interface du groupe IPMP actuel. Lorsque vous placez l'interface dans un nouveau groupe, l'interface est automatiquement retirée de tout groupe IPMP existant.

1 **Sur le système sur lequel est configuré le groupe IPMP, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Déplacez l'interface vers un nouveau groupe IPMP.**

`# ifconfig` *interface* `group` *group-name*

Si vous placez l'interface dans un nouveau groupe, elle est automatiquement retirée de tout groupe existant.

Exemple 31–8 Déplacement d'une interface vers un autre groupe IPMP

Pour modifier le groupe IPMP de l'interface `hme0`, saisissez ce qui suit :

```
# ifconfig hme0 group cs-link
```

Cette commande permet de supprimer l'interface `hme0` du groupe IPMP `test`, puis de placer l'interface dans le groupe `cs-link`.

Remplacement d'une interface physique défaillante sur des systèmes prenant la DR en charge

Cette section décrit les procédures relatives à l'administration de systèmes prenant en charge la reconfiguration dynamique (DR).

Remarque – Les tâches ne s'appliquent qu'aux couches IP configurées à l'aide de la commande `ifconfig`. Les couches avant ou après la couche IP, comme l'ATM ou autres services, requièrent des étapes manuelles si les couches ne sont pas automatisées. Les étapes des procédures suivantes permettent d'annuler la configuration des interfaces lors de la préconnexion et de configurer une interface après la postconnexion.

▼ Procédure de suppression d'une interface physique défaillante (DR puis déconnexion)

Cette procédure indique la méthode de retrait d'une interface physique d'un système prenant la reconfiguration dynamique en charge. Elle part du principe que les conditions suivantes existent déjà :

- Les interfaces physiques `hme0` et `hme1` sont les interfaces d'exemple.
- Les interfaces se trouvent dans le même groupe IPMP.
- `hme0` est défaillante.
- L'interface logique `hme0:1` possède l'adresse test.
- Le nom de l'interface défaillante est remplacé par le même nom d'interface physique, par exemple, `hme0` par `hme0`.

Remarque – Vous pouvez ignorer l'étape 2 si l'adresse test est montée à l'aide du fichier `/etc/hostname.hme0`.

---

1 Sur le système sur lequel est configuré le groupe IPMP, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Affichez la configuration d'adresse test.**

```
# ifconfig hme0:1

hme0:1:
flags=9040842<BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER>
mtu 1500 index 3
inet 192.168.233.250 netmask ffffff00 broadcast 192.168.233.255
```

Ces informations sont nécessaires afin de remonter l'adresse test lors du remplacement de l'interface physique.

3 **Supprimez l'interface physique.**

Reportez-vous aux sources suivantes pour obtenir une description complète de la méthode de suppression de l'interface physique :

- Page de manuel `cfgadm(1M)`.
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*
- *Sun Enterprise 10000 DR Configuration Guide*

▼ Procédure de remplacement d'une interface physique défaillante (DR puis connexion)

Cette procédure correspond à la méthode de remplacement d'une interface physique d'un système prenant la DR en charge.

1 **Sur le système sur lequel est configuré le groupe IPMP, connectez-vous en tant qu'administrateur principal ou superutilisateur.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, “Utilisation de la console de gestion Solaris (tâches) ” du *Guide d'administration système : administration de base*.

2 **Remplacez l'interface physique.**

Vous pouvez consulter les sources suivantes pour obtenir des instructions :

- Page de manuel `cfgadm(1M)`.
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*
- *Sun Enterprise 10000 DR Configuration Guide* ou *Sun Fire 880 Dynamic Reconfiguration User's Guide*

Récupération d'une interface physique absente à l'initialisation du système

Remarque – La procédure suivante s'applique uniquement aux couches IP configurées à l'aide de la commande `ifconfig`. Les couches avant ou après la couche IP, comme l'ATM ou autres services, requièrent des étapes manuelles si les couches ne sont pas automatisées. Les étapes spécifiques de la procédure suivante permettent d'annuler la configuration d'interface lors de la prédéconnexion et de configurer les interfaces après la postconnexion.

La reprise après reconfiguration dynamique est automatique pour une interface faisant partie de la carte E/S d'une plate-forme Sun Fire™. Si la carte d'interface réseau est une carte Sun Crypto Accelerator I - cPCI, la récupération est également automatique. Par conséquent, les étapes suivantes ne sont pas nécessaires dans le cas d'une interface récupérée lors d'une opération de reconfiguration dynamique. Pour de plus amples informations sur les systèmes Sun Fire x800 et Sun Fire 15000, consultez la page de manuel `cfgadm_sbd`(1M) L'interface physique est rétablie selon la configuration spécifiée dans le fichier `/etc/hostname.` `fichier` *interface*. Reportez-vous à la section "Configuration de groupes IPMP" à la page 779 pour obtenir des informations supplémentaires sur la configuration d'interfaces afin de conserver la configuration après réinitialisation.

Remarque – Dans les systèmes Sun Fire legacy (Exx00), les connexions de reconfiguration dynamique requièrent encore des procédures manuelles. Cependant, les connexions de reconfiguration dynamique sont automatiques.

▼ Procédure de récupération d'une interface physique absente lors de l'initialisation du système

Avant de récupérer une interface physique absente lors de l'initialisation du système, vous devez effectuer les procédures suivantes. Dans l'exemple de cette procédure, la configuration est la suivante :

- Les interfaces physiques `hme0` et `hme1` sont les interfaces.
- Les interfaces se trouvent dans le même groupe IPMP.
- `hme0` n'était pas installé lors de l'initialisation du système.

Remarque – Le rétablissement d'adresses IP lors de la réparation d'une interface physique défaillante peut prendre jusqu'à trois minutes. Cette durée varie en fonction du trafic réseau. Elle dépend également de la stabilité de l'interface entrante afin de rétablir les interfaces basculées par le démon `in.mpathd`.

1 Sur le système sur lequel est configuré le groupe IPMP, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Les informations relatives au réseau défaillant sont indiquées dans le message d'erreur du journal de la console.

Consultez la page de manuel `syslog(3C)` Le message d'erreur est similaire à ce qui suit :

```
moving addresses from failed IPv4 interfaces:
hme1 (moved to hme0)
```

Ce message indique que les adresses IPv4 de l'interface défaillante `hme1` ont basculé vers l'interface `hme0`.

Vous pouvez également recevoir le message suivant :

```
moving addresses from failed IPv4 interfaces:
hme1 (couldn't move, no alternative interface)
```

Ce message indique qu'aucune interface active n'a pu être trouvée dans le groupe de l'interface défaillante `hme1`. Par conséquent, le basculement des adresses IPv4 vers `hme1` ne s'est pas effectué.

3 Connectez l'interface physique au système.

Reportez-vous aux sources suivantes pour obtenir des instructions sur le remplacement de l'interface physique :

- Page de manuel `cfgadm(1M)`.
- *Sun Enterprise 10000 DR Configuration Guide*
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*

4 Reportez-vous au contenu du message de l'étape 2. Si les adresses n'ont pu être déplacées, passez à l'étape 6. Si les adresses ont été déplacées, passez à l'étape 5.

5 **Démontez les interfaces logiques configurées au cours du processus de basculement.**

a. **Consultez le contenu du fichier `/etc/hostname.` *déplacé-de-interface*, afin de connaître les interfaces logiques configurées en tant qu'élément du processus de basculement.**

b. **Démontez chaque adresse IP de basculement.**

```
# ifconfig moved-to-interface removeif moved-ip-address
```

Remarque – Les adresses de basculement sont marquées à l'aide du paramètre `failover` ou ne sont pas marquées avec le paramètre `-failover`. Il est inutile de démonter les adresses IP marquées à l'aide du paramètre `-failover`.

Par exemple, si l'on admet que le fichier `/etc/hostname.hme0` contient les lignes suivantes :

```
inet 10.0.0.4 -failover up group one
addif 10.0.0.5 failover up
addif 10.0.0.6 failover up
```

Pour démonter l'adresse IP de basculement, vous devez saisir la commande suivante :

```
# ifconfig hme0 removeif 10.0.0.5
# ifconfig hme0 removeif 10.0.0.6
```

6 **Reconfigurez les informations IPv4 de l'interface physique remplacée en saisissant la commande suivante pour chaque interface supprimée :**

```
# ifconfig removed-from-NIC <parameters>
```

Vous pouvez par exemple saisir les commandes suivantes :

```
# ifconfig hme1 inet plumb
# ifconfig hme1 inet 10.0.0.4 -failover up group one
# ifconfig hme1 addif 10.0.0.5 failover up
# ifconfig hme1 addif 10.0.0.6 failover up
```

Modification des configurations IPMP

Le fichier de configuration IPMP `/etc/default/mpathd` permet de configurer les paramètres système suivants des groupes IPMP.

- `FAILURE_DETECTION_TIME`
- `TRACK_INTERFACES_ONLY_WITH_GROUPS`
- `FAILBACK`

▼ Procédure de configuration du fichier `/etc/default/mpathd`

1 Sur le système sur lequel est configuré le groupe IPMP, connectez-vous en tant qu'administrateur principal ou superutilisateur.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Modifiez le fichier `/etc/default/mpathd`.

Modifiez la valeur par défaut d'au moins un des trois paramètres.

a. Saisissez la nouvelle valeur du paramètre `FAILURE_DETECTION_TIME`.

```
FAILURE_DETECTION_TIME=n
```

où *n* correspond à la durée en secondes nécessaire aux sondes ICMP pour la détection d'une éventuelle défaillance d'interface. La valeur par défaut est de 10 secondes.

b. Saisissez la nouvelle valeur du paramètre `FAILBACK`.

```
FAILBACK=[yes | no]
```

- *yes*- La valeur *yes* correspond au comportement de basculement par défaut d'IPMP. En cas de détection de réparation d'une interface défaillante, l'accès réseau est rétabli à l'aide de l'interface réparée, tel que décrit dans la section "Détection de défaillance d'IPMP et fonctionnalités de reprise" à la page 769.
- *no* - La valeur *no* indique que le trafic de données n'est pas rétabli sur une interface réparée. En cas de détection d'une interface réparée, l'indicateur *INACTIVE* est défini pour celle-ci. L'indicateur indique qu'il est actuellement impossible d'utiliser l'interface pour le trafic de données. Il est cependant possible de l'utiliser pour le trafic de sondes.

  Supposons par exemple qu'un groupe IPMP se compose de deux interfaces, ce0 et ce1. Supposons ensuite que la valeur *FAILBACK=no* est définie dans `/etc/default/mpathd`. En cas de défaillance de ce0 son trafic bascule vers ce1, ce qui correspond au comportement attendu d'IPMP. Cependant, si IPMP détecte que l'interface ce0 est réparée, le trafic n'est par rétabli à partir de ce1, en raison du paramètre *FAILBACK=no* dans `/etc/default/mpathd`. L'interface ce0 conserve le statut `INACTIVE` et n'est pas utilisée pour le trafic, sauf en cas de défaillance de l'interface ce1. En cas de défaillance de l'interface ce1, les adresses sur ce1 sont déplacées vers ce0, dont l'indicateur INACTIVE est alors effacé. Ce déplacement se produit à condition que ce0 soit la seule interface INACTIVE du groupe. Si c'est le cas d'autres interfaces du groupe, les adresses risquent d'être déplacées vers une interface INACTIVE différente de ce0.

c. Saisissez la nouvelle valeur du paramètre `TRACK_INTERFACES_ONLY_WITH_GROUPS` .

```
TRACK_INTERFACES_ONLY_WITH_GROUPS=[yes | no]
```

- *yes*- La valeur *yes* correspond au comportement par défaut d'IPMP. Ce paramètre permet à IPMP d'ignorer les interfaces réseau qui ne sont pas configurées dans un groupe IPMP.
- *no* - La valeur *no* définit la détection de défaillance et de réparation pour *toutes* les interfaces réseau, qu'elles soient configurées ou non dans un groupe IPMP. Cependant, lorsqu'une défaillance ou une réparation est détectée sur une interface non configurée dans un groupe IPMP, aucun basculement ni rétablissement ne se produit. Par conséquent, la valeur *no* est utile uniquement pour les rapports de défaillances et n'améliore pas directement la disponibilité du réseau.

3 Redémarrez le démon `in.mpathd`.

```
# pkill -HUP in.mpathd
```

PARTIE VII

Qualité de service IP (IPQoS)

Cette partie décrit les tâches et les informations concernant la qualité de service IP (IPQoS) et l'implémentation des services différenciés d'Oracle Solaris.

◆ ◆ ◆ CHAPITRE 32

Présentation d'IPQoS (généralités)

La qualité de service IP (IPQoS) permet de hiérarchiser, de contrôler et de recueillir les statistiques comptables. À l'aide d'IPQoS, vous pouvez fournir des niveaux de service homogènes aux utilisateurs de votre réseau. Cela permet également de gérer le trafic pour éviter la congestion du réseau.

Voici la liste des sujets abordés dans ce chapitre :

Principes de base d'IPQoS

IPQoS active l'architecture de services différenciés (Diffserv) qui est défini par le groupe de travail de l'IETF, The Differentiated Services Working Group. Dans Oracle Solaris, le composant IPQoS est implémenté au niveau de l'IP de la pile du protocole TCP/IP.

Quels sont les services différenciés ?

En activant IPQoS, vous fournissez différents niveaux de service réseau aux clients et aux applications sélectionnés. Les différents niveaux de service sont collectivement désignés sous l'appellation de *services différenciés*. Les services différenciés fournis aux clients peuvent se baser sur la structure des niveaux de service offerts par l'entreprise à ses clients. Vous pouvez également fournir des services différenciés en fonction des priorités définies pour les applications ou les utilisateurs de votre réseau.

Offrir une qualité de service implique les activités suivantes :

- déléguer des niveaux de service à différents groupes (clients ou services d'une entreprise, par exemple) ;
- définir la priorité des services réseau attribuée à certains groupes ou applications ;
- discerner et éliminer les goulets d'étranglement ou toute autre forme de congestion ;
- contrôler les performances réseau et fournir des statistiques sur les performances ;
- réguler la bande passante au vu des ressources réseau.

Fonctions IPQoS

IPQoS possède les fonctions suivantes :

- `ipqosconf`, outil au niveau de la ligne de commande pour configurer la stratégie QoS ;
- classificateur sélectionnant les actions, selon les filtres configurant la stratégie QoS de votre organisation ;
- module de mesure du trafic réseau conformé au modèle Diffserv ;
- différenciation des services basée sur la possibilité de marquer un en-tête IP de paquet avec des informations de transmission ;
- module de comptabilisation des flux rassemblant les statistiques des flux de trafic ;
- statistiques sur les classes de trafic, via la commande UNIX® `kstat` ;
- prise en charge de l'architecture SPARC® et x86 ;
- prise en charge des adresses IPv4 et IPv6 ;
- interopérabilité avec l'architecture de sécurité IP (IPsec) ;
- prise en charge des marquages de priorité utilisateur 802.1D dans les réseaux locaux virtuels (VLAN).

Sources d'informations sur la théorie de la qualité de service et les techniques

Vous trouverez des informations sur les services différenciés et la qualité de service dans la documentation papier ou en ligne.

Ouvrages sur la qualité de service

Pour plus d'informations sur la théorie de la qualité de service et ses applications, reportez-vous aux publications suivantes :

- Ferguson, Paul et Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Kilkki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.

Documents RFC (Request For Comments) sur la qualité de service

IPQoS se conforme aux spécifications décrites dans les RFC et les documents de travail Internet suivants :

- Le document 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`) (en anglais) décrit une amélioration du champ de type de service (ToS) ou champ DS des en-têtes de paquet IPv4 et IPv6 pour la prise en charge des services différenciés
- Le document RFC 2475, An Architecture for Differentiated Services (`http://www.ietf.org/rfc/rfc2475.txt?number=2475`) (en anglais) décrit en détail l'organisation et les modules de l'architecture Diffserv
- Le document RFC 2597, Assured Forwarding PHB Group (`http://www.ietf.org/rfc/rfc2597.txt?number=2597`) (en anglais) décrit le fonctionnement du comportement AF (Assured Forwarding, transfert assuré) par saut
- Le document RFC 2598, An Expedited Forwarding PHB (`http://www.ietf.org/rfc/rfc2598.txt?number=2598`) (en anglais) décrit le fonctionnement du comportement EF (Expedited Forwarding, transfert accéléré) par saut
- Document de travail Internet, *An Informal Management Model for Diffserv Routers* – Présente un modèle pour l'implémentation de l'architecture Diffserv sur les routeurs.

Sites Web donnant des informations sur la qualité de service

Le groupe de travail The Differentiated Services Working Group de l'IETF gère un site Web comportant des liens renvoyant vers des documents de travail Internet Diffserv à l'adresse `http://www.ietf.org/html.charters/diffserv-charter.html`.

Les fabricants de routeur tels que Cisco Systems et Juniper Networks fournissent des informations sur leur sites Web ; ces derniers décrivent la manière dont les services différenciés sont implémentés dans leurs produits.

Pages de manuel IPQoS

Documentation IPQoS inclut les pages de manuel suivantes :

- `ipqosconf(1M)` - décrit la commande permettant de paramétrer le fichier de configuration IPQoS ;
- `ipqos(7ipp)` – décrit l'implémentation IPQoS du modèle d'architecture Diffserv ;
- `ipgpc(7ipp)` – décrit l'implémentation IPQoS d'un classificateur Diffserv ;
- `tokenmt(7ipp)` – décrit le module de mesure `tokenmt` d' IPQoS ;
- `tswtclmt(7ipp)` – décrit le module de mesure `tswtclmt` d' IPQoS ;
- `dscpmk(7ipp)` – décrit le module de marquage DSCP ;
- `dlcosmk(7ipp)` – décrit le module de marquage de priorité utilisateur IPQoS 802.1D ;

- `flowacct(7ipp)`– décrit le module de comptabilisation des flux IPQoS ;
- `acctadm(1M)` – décrit la commande permettant de configurer les fonctions de comptabilité étendues d'Oracle Solaris. La commande `acctadm` inclut des extensions IPQoS.

Livraison d'une qualité de service avec IPQoS

Les fonctions IPQoS permettent aux fournisseurs d'accès Internet (FAI) ainsi qu'aux fournisseurs de services d'applications (ASP) d'offrir différents niveaux de service réseau à leurs clients. Ces fonctions permettent à des sociétés et à des organismes d'éducation ou de formation de hiérarchiser les services pour des organisations internes ou pour les applications principales.

Implémentation des accords de niveau de service

Si votre organisation est un FAI ou un fournisseur de services d'applications, vous pouvez baser votre configuration IPQoS sur l'*accord de niveau de service* que votre entreprise propose à ses clients. Dans le cadre d'un accord de niveau de service, un fournisseur de service garantit à un client un certain niveau de service réseau basé sur une hiérarchie de prix. Par exemple, un accord de type premium implique que le client reçoive la plus haute priorité pour tous les types de trafic réseau 24 h/24h 7j/7. Inversement, un accord facturé à un prix moyen indique que le client bénéficie d'une haute priorité pour la transmission des messages électroniques uniquement pendant les heures d'ouverture de bureau. Tout autre trafic se voit appliquer une priorité moyenne 24 h/24h.

Garantie d'une qualité de service pour une organisation

Si votre organisation est une entreprise ou une institution, vous pouvez également utiliser différentes fonctions liées à la qualité de service pour votre réseau. Ainsi, il est possible d'appliquer un degré de service plus ou moins élevé au trafic d'un groupe ou d'une application spécifique.

Introduction à la stratégie de qualité de service

Vous implémentez la qualité de service en définissant une *stratégie de qualité de service (QoS)*. La stratégie de qualité de service spécifie plusieurs attributs de réseau comme la priorité des clients ou des applications et les actions pour le traitement de différentes catégories de trafic. Vous implémentez la stratégie de qualité de service de votre organisation dans un fichier de configuration IPQoS. Ce fichier configure les modules IPQoS se trouvant dans le noyau Oracle Solaris. Un hôte auquel une stratégie IPQoS est appliquée est considéré comme un *système IPQoS*.

Votre stratégie QoS définit les éléments suivants :

- Des groupes discrets de trafic réseau appelés *classes de service*.
- Des mesures de régulation du volume du trafic réseau de chaque classe. Elles régissent le processus de contrôle du trafic appelé *mesure*.
- Une action qu'un système IPQoS et un routeur Diffserv doivent appliquer à un flux de paquets. Ce type d'action est désigné comme le *PHB* (per-hop behavior ou comportement par pas).
- Toute collecte de statistiques dont votre organisation a besoin sur une classe de service. Citons par exemple, le trafic généré par un client ou une application spécifique.

Lorsque les paquets arrivent sur le réseau, le système IPQoS évalue les en-têtes de paquets. L'action que le système IPQoS réalise est déterminée par votre stratégie QoS.

Les tâches pour élaborer la conception de la stratégie QoS sont décrites dans la section "Planification de la stratégie de qualité de service" à la page 825.

Amélioration de l'efficacité du réseau dans IPQoS

IPQoS contient des fonctions qui contribuent à augmenter l'efficacité des performances réseau lors de l'implémentation de la qualité de service. Au fur et à mesure que le réseau d'ordinateurs s'étend, la nécessité de gérer le trafic réseau engendré par un nombre croissant d'utilisateurs et des processeurs plus puissants se fait plus grande. Un réseau surexploité peut manifester certains signes, par exemple, des pertes de données ou une congestion du trafic. Ces signes se traduisent par des délais de réponse très lents.

Par le passé, les administrateurs système géraient les problèmes de trafic réseau en augmentant la bande passante. Souvent, le niveau du trafic des liaisons variait considérablement. Grâce à IPQoS, il est possible de gérer le trafic sur le réseau existant et d'évaluer si une extension s'avère nécessaire et, le cas échéant, les zones visées.

Par exemple, dans le cadre d'une entreprise ou d'une institution, il est indispensable de maintenir un réseau performant afin d'éviter les goulets d'étranglement. Vous devez également veiller à ce qu'un groupe ou une application ne consomme pas plus de bande passante que le volume alloué. Pour un FAI ou un ASP, vous devez gérer les performances du réseau pour assurer que les clients reçoivent le service réseau correspondant à l'abonnement souscrit.

Impact de la bande passante sur le trafic réseau

Vous pouvez utiliser IPQoS pour réguler la *bande passante* du réseau correspondant au volume maximal de données qu'une liaison réseau ou un périphérique intégralement exploité peut transférer. Votre stratégie QoS doit déterminer la priorité de l'utilisation de la bande passante

afin de fournir la qualité de service aux clients ou utilisateurs. Les modules de mesure IPQoS permettent de mesurer et de contrôler l'allocation de la bande passante aux classes de trafic sur un hôte IPQoS.

Avant de pouvoir gérer efficacement le trafic sur un réseau, vous devez répondre aux questions relatives à l'utilisation de la bande passante suivantes :

- Quelles sont les zones de votre réseau local associées à un problème de trafic ?
- Que devez vous faire pour atteindre l'utilisation optimale de la bande passante disponible ?
- Quelles sont les applications critiques de votre site auxquelles une priorité élevée doit être attribuée ?
- Quelles sont les applications sensibles à une éventuelle congestion ?
- Quelles sont, parmi vos applications, les applications les moins critiques compatibles avec une priorité la plus faible ?

Utilisation des classes de service pour hiérarchiser le trafic

Pour implémenter la qualité de service, vous analysez le trafic du réseau afin de déterminer les groupes plus larges dans lesquels le trafic peut être réparti. Organisez ensuite les groupes en classes de service dotées de caractéristiques et de priorités spécifiques. Ces classes forment les catégories fondamentales sur lesquelles vous basez la stratégie QoS de votre organisation. Les classes de service représentent les groupes de trafic à contrôler.

Par exemple, un fournisseur peut offre des accords de niveau de service platinum, gold, silver et bronze disponibles selon une échelle de prix. Un accord de niveau de service platinum accorde la priorité la plus haute au trafic entrant d'un site Web que le FAI héberge au nom du client. Ainsi, le trafic entrant du site Web du client peut correspondre à une classe de trafic.

Pour une entreprise, il est possible de créer des classes de service en fonction des besoins propres aux services. Une autre option consiste à créer des classes selon la prépondérance d'une application donnée dans le trafic réseau. Voici quelques exemples de classes de trafic pour une entreprise :

- Les applications courantes comme la messagerie électronique et le trafic FTP sortant vers un serveur particulier peuvent constituer l'un ou l'autre une classe. Puisque les employés font constamment appel à ces applications, votre stratégie QoS garantit aux courriers électroniques et au trafic FTP sortant une petite partie de la bande passante et une priorité plus faible.
- Une base de données d'entrées correspondant à des commandes devant fonctionner 24 h/24. Selon l'importance de l'application de la base de données pour l'entreprise, il est possible d'accorder à la base de données une grande partie de la bande passante et une priorité élevée.

- Un service qui réalise des tâches importantes ou confidentielle, comme le service de paie. L'importance du service pour l'organisation détermine la priorité et la largeur de bande passante accordée à un tel service.
- Les appels entrants du site Web externe d'une entreprise. Vous pouvez donner à cette classe une largeur de bande passante moyenne qui s'exécute à basse priorité.

Modèle de services différenciés

IPQoS inclut les modules suivants qui font partie de l'architecture des *services différenciés (Diffserv)* définie dans le document RFC 2475.

- classificateur ;
- compteur ;
- marqueur.

IPQoS apporte les améliorations suivantes au modèle Diffserv :

- module de comptabilisation des flux ;
- marqueur de datagramme 802.1D ;

Cette section présente les modules Diffserv tel qu'ils sont utilisés par IPQoS. Il est nécessaire de posséder des informations sur ces modules et de connaître notamment leur nom ainsi que leur utilisation en vue de la configuration de la stratégie QoS. Pour plus d'informations détaillées sur chaque module, reportez-vous à la section "Architecture IPQoS et modèle Diffserv" à la page 885.

Présentation du classificateur (`ipgpc`)

Dans le modèle Diffserv, le *classificateur* sélectionne des paquets à partir d'un flux de trafic réseau. Un *flux de trafic* consiste en un groupe de paquets avec des informations identiques dans les champs d'en-tête IP suivants :

- adresse source ;
- adresse de destination ;
- port source ;
- port de destination ;
- Numéro de protocole.

Dans IPQoS, ces champs sont désignés *5-uplet*.

Le module de classification IPQoS s'appelle `ipgpc`. Le classificateur `ipgpc` organise les flux de trafic en classes selon les caractéristiques configurées dans le fichier de configuration IPQoS.

Pour des informations détaillées sur `ipgpc`, reportez-vous à la section "Module de classification" à la page 885.

Classes IPQoS

Une *classe* représente un groupe de flux de réseau qui partage des caractéristiques similaires. Par exemple, un FAI peut définir des classes visant à représenter des niveaux de service différents proposés aux clients. Un ASP peut définir des accords de niveau de service octroyant des niveaux de service différents à diverses applications. Dans le cadre de la stratégie QoS d'un ASP, une classe peut inclure le trafic FTP sortant associé à une adresse IP de destination spécifique. Le trafic sortant du site Web externe d'une entreprise peut également faire l'objet d'une classe.

L'organisation du trafic en classes constitue une partie primordiale de la planification de votre stratégie QoS. Lorsque vous créez des classes à l'aide de l'utilitaire `ipqosconf`, vous configurez de fait le module de classification `ipgpc`.

Pour obtenir des informations sur la définition des classes, reportez-vous à la section "Définition des classes pour votre stratégie QoS" à la page 828.

Filtres IPQoS

Les *filtres* sont des jeux de règles qui contiennent des paramètres appelés *sélecteurs*. Chaque filtre doit désigner une classe. IPQoS fait correspondre aux paquets les sélecteurs de chaque filtre afin de déterminer si le paquet appartient à la classe du filtre. Toute une gamme de sélecteurs permet de filtrer un paquet, par exemple, l'uplet à 5 attributs d'IPQoS et d'autres paramètres courants :

- adresses source et de destination ;
- port source et port de destination ;
- numéros de protocole ;
- ID utilisateur ;
- ID de projet ;
- point de code de services différenciés (DSCP) ;
- indice d'interface.

Par exemple, un filtre simple peut comporter le port de destination avec la valeur 80. Le classificateur `ipgpc` sélectionne ensuite tous les paquets liés au port de destination 80 (HTTP) et traite les paquets comme indiqué dans la stratégie QoS.

Pour plus d'informations sur la création de filtres, reportez-vous à la section "Définition de filtres dans la stratégie QoS" à la page 831.

Présentation des compteurs (`tokenmt` et `tswtclmt`)

Dans le modèle Diffserv, le *compteur* étudie le taux de transmission des flux de trafic par classe. Le compteur évalue dans quelle proportion le débit réel du flux se conforme aux débits configurés et définit le résultat qui convient. Selon le résultat obtenu par le flux du trafic, le compteur sélectionne l'action qui s'ensuit. Les actions suivantes peuvent être le transfert du paquet vers une autre action ou le retour du paquet vers le réseau sans traitement supplémentaire.

Les compteurs IPQoS déterminent si un flux de réseau est conforme au débit de transmission défini pour sa classe dans la stratégie QoS. IPQoS comporte deux modules de mesure :

- `tokenmt` – utilise un plan de mesure de seau à deux jetons.
- `tswtclmt` – utilise un plan de mesure se rapportant à une fenêtre (temporelle).

Les deux modules de mesure aboutissent aux trois résultats : rouge, orange et vert. Définissez les actions à réaliser en fonction de chaque résultat dans les paramètres `red_action_name`, `yellow_action_name` et `green_action_name` .

De plus, vous pouvez configurer `tokenmt` de sorte que ses résultats s'affiche sous forme d'un code en couleur. Une instance de mesure couleur utilise la taille du paquet, le DSCP, le débit du trafic et le paramètres configurés pour déterminer le résultat. Le compteur utilise le DSCP de manière à traduire le résultat du paquet en vert, orange ou rouge.

Pour plus d'informations sur la définition des paramètres pour les compteurs IPQoS, reportez-vous à la section “Planification du contrôle de flux” à la page 832.

Généralités des marqueurs (`dscpmk` et `dlcosmk`)

Dans le modèle Diffserv, le *marqueur* donne une valeur au paquet reflétant un comportant de transmission. Le *marquage* est le processus consistant à placer une valeur dans l'en-tête du paquet de façon à signaler le mode de transmission du paquet vers le réseau. IPQoS contient deux modules de marquage :

- `dscpmk` : attribue au champ DS de l'en-tête du paquet IP une valeur numérique appelée *point de code de services différenciés DSCP*. Un routeur Diffserv est alors en mesure d'utiliser le point de code DS pour appliquer le comportement de transmission au paquet.
- `dlcosmk` – spécifie l'étiquette du réseau local virtuel (VLAN) d'un entête de trame Ethernet. Pour cela, il lui attribue une valeur numérique appelée *priorité utilisateur*. La priorité utilisateur indique la *classe de service (CoS)*, définissant le comportement à appliquer au datagramme.

  `dlcosmk` est un extension IPQoS qui ne fait pas partie du modèle Diffserv tel que ce dernier a été conçu par l'IETF.

Pour plus d'informations sur l'implémentation d'une approche utilisant un marqueur dans le cadre de la stratégie QoS, reportez-vous à la section “Planification du comportement de transmission” à la page 835.

Généralités sur la comptabilisation des flux (`flowacct`)

IPQoS ajoute le module de comptabilisation `flowacct` au modèle Diffserv. Vous pouvez utiliser `flowacct` pour collecter des statistiques sur les flux de trafic et facturer les clients en conséquence conformément à l'accord de niveau de service souscrit. La comptabilisation des flux présente également un intérêt dans l'optique de la planification de la capacité et du contrôle du système.

Le module `flowacct` fonctionne avec la commande `acctadm` pour créer un fichier journal de comptabilisation. Un journal standard inclut l'uplet à 5 attributs d'IPQoS et deux attributs supplémentaires comme indiqué dans la liste suivante :

- adresse source ;
- port source ;
- adresse de destination ;
- port de destination ;
- numéro du protocole ;
- nombre de paquets ;
- nombre d'octets.

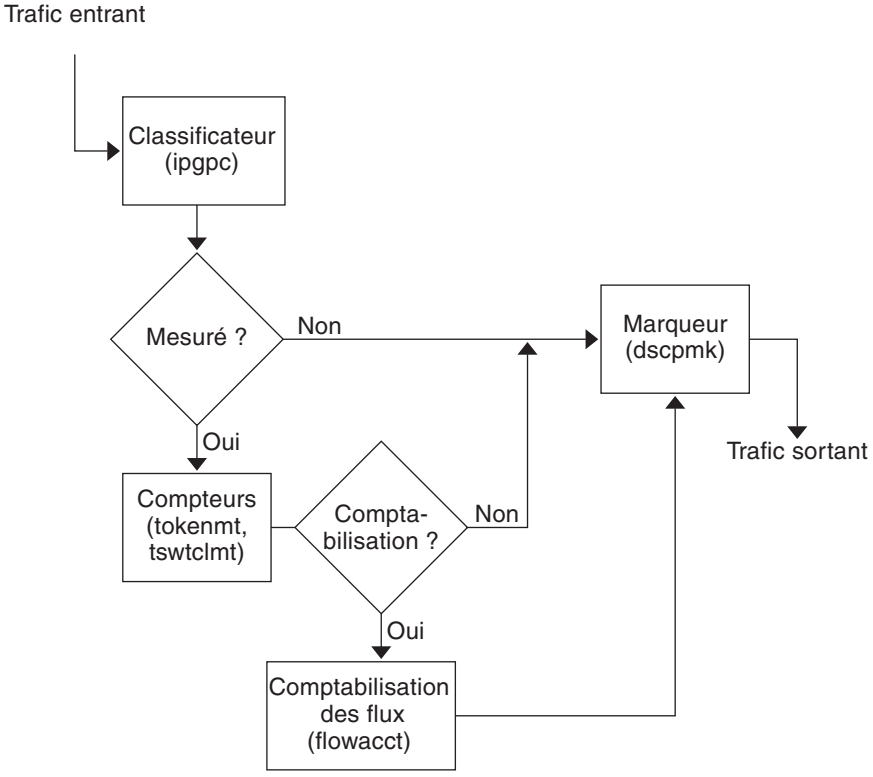
Vous pouvez recueillir les statistiques sur d'autres attributs, comme indiqué à la section "Enregistrement des informations sur les flux de trafic" à la page 880 et dans les pages de manuel `flowacct`(7ipp) et `acctadm`(1M).

Pour plus d'informations sur la planification d'une stratégie de comptabilisation des flux, reportez-vous à la section "Planification de la comptabilisation des flux" à la page 838.

Transit du trafic par les modules IPQoS

La figure suivante présente un itinéraire que le trafic entrant peut suivre en passant par certains modules IPQoS.

FIGURE 32–1 Flux de trafic et implémentation IPQoS du modèle Diffserv



Cette figure illustre une séquence de flux courante sur un ordinateur compatible IPQoS :

1. Le classificateur sélectionne les paquets qui correspondent aux critères de filtre définis pour la stratégie QoS du système dans le flux de paquets.
2. Les paquets sélectionnés sont ensuite évalués en vue de l'action suivante à réaliser.
3. Le classificateur envoie au marqueur le trafic ne nécessitant aucun contrôle de flux.
4. Le trafic à contrôler est transmis au module de mesure.
5. Ce module applique le taux configuré. Il assigne ensuite une valeur de conformité du trafic aux paquets contrôlés.
6. Les paquets dont les flux ont été contrôlés sont ensuite analysés afin de déterminer si des paquets doivent être comptabilisés.
7. Le compteur transmet au marqueur le trafic qui n'exige pas de comptabilisation des flux.
8. Le flux de comptabilisation collecte les statistiques sur les paquets reçus. Le module transmet ensuite les paquets au marqueur.

9. Le marqueur introduit un point de code DS dans l'en-tête du paquet. Ce DSCP signale le traitement, ou PHB, qu'un système Diffserv doit appliquer au paquet.

Trafic sur un réseau compatible IPQoS

Cette section présente les éléments impliqués dans la transmission des paquets sur un réseau IPQoS. Un système IPQoS traite les paquets du réseau en fonction de l'adresse IP du système faisant office de destination. Ce système applique ensuite la stratégie QoS aux paquets afin de fournir des services différenciés.

Point de code DS

Le point de code DS (DSCP) définit, dans l'en-tête du paquet, l'action que le système Diffserv doit appliquer au paquet marqué. L'architecture Diffserv définit un ensemble de points de code DS pour le système IPQoS et le routeur Diffserv à utiliser. L'architecture Diffserv définit également un ensemble d'actions appelées *comportements de transmission* associés aux DSCP. Le système IPQoS marque, à l'aide du DSCP, les bits définissant le niveau de priorité du champ DS dans l'en-tête de paquet. Lorsqu'un routeur reçoit un paquet comportant une valeur DSCP, il applique le comportement associé à ce DSCP. Le paquet est ensuite libéré sur le réseau.

Remarque – Le marqueur `dlcosmk` ne fait pas appel aux valeurs DSCP. À la place, `dlcosmk` marque les en-têtes de trames Ethernet par une valeur CoS (classe de service). Si vous envisagez de configurer IPQoS sur un réseau utilisant des périphériques VLAN, reportez-vous à la section "Module de marquage" à la page 891.

PHB (Per-Hop Behaviors)

Dans la terminologie Diffserv, le comportement assigné à un DSCP est désigné comme le *PHB (per-hop behavior)*. Le PHB définit le niveau de priorité dont bénéficie un paquet marqué par rapport à tout autre trafic sur le système Diffserv. C'est ce niveau de priorité qui détermine si le système IPQoS ou le routeur Diffserv transmet ou rejette le paquet marqué. Tous les routeurs Diffserv rencontrés par le paquet transmis lors de son trajet vers sa destination finale appliquent le même PHB. Une seule exception peut survenir : lorsqu'un autre système Diffserv modifie le DSCP. Pour plus d'informations sur les PHB, reportez-vous à la section "Utilisation du marqueur `dscpmk` pour la transmission des paquets" à la page 891.

L'objectif d'un PHB consiste à fournir le volume de ressources réseau spécifié à une classe de trafic sur le réseau contigu. La stratégie QoS permet d'atteindre cet objectif. Définissez les DSCP chargés de signaler le niveau de priorité des classes de trafic lorsque les flux de trafic quittent le système IPQoS. Les niveaux de priorités varient entre une haute priorité/faible probabilité de rejet et une priorité faible/haute probabilité de rejet.

Votre stratégie QoS peut, par exemple, assigner à une classe de trafic un DSCP garantissant un PHB pour lequel la probabilité de perte des paquets est faible. Cette classe de trafic est donc traitée conformément à un PHB de faible probabilité de rejet par les routeurs Diffserv qui réservent une partie de la bande passante pour les paquets de cette classe. Vous pouvez associer d'autres DSCP à la stratégie QoS, assignant des niveaux variables de priorité à d'autres classes de trafic. La bande passante accordée aux paquets dont le niveau de priorité est le plus faible dépend des priorités spécifiées par les DSCP des paquets.

IPQoS prend en charge deux types de comportements, définis dans l'architecture Diffserv, le traitement accéléré (Expedited Forwarding) et le traitement garanti (Assured Forwarding).

Expedited Forwarding

Le PHB *EF (Expedited forwarding)* garantie à toute classe de trafic de DSCP EF la priorité la plus élevée. Le trafic doté d'un DSCP EF n'est pas placé dans la file d'attente. EF assure des taux de perte, de délai et de gigue faibles. Le code DSCP recommandé pour EF est 101110. Un paquet ainsi marqué se voit garantir une faible probabilité de rejet alors qu'il transite par les réseaux Diffserv pour parvenir à sa destination. Utilisez le DSCP EF lorsque vous définissez la priorité des clients ou des applications bénéficiant d'un accord de niveau de service de type premium.

Assured Forwarding

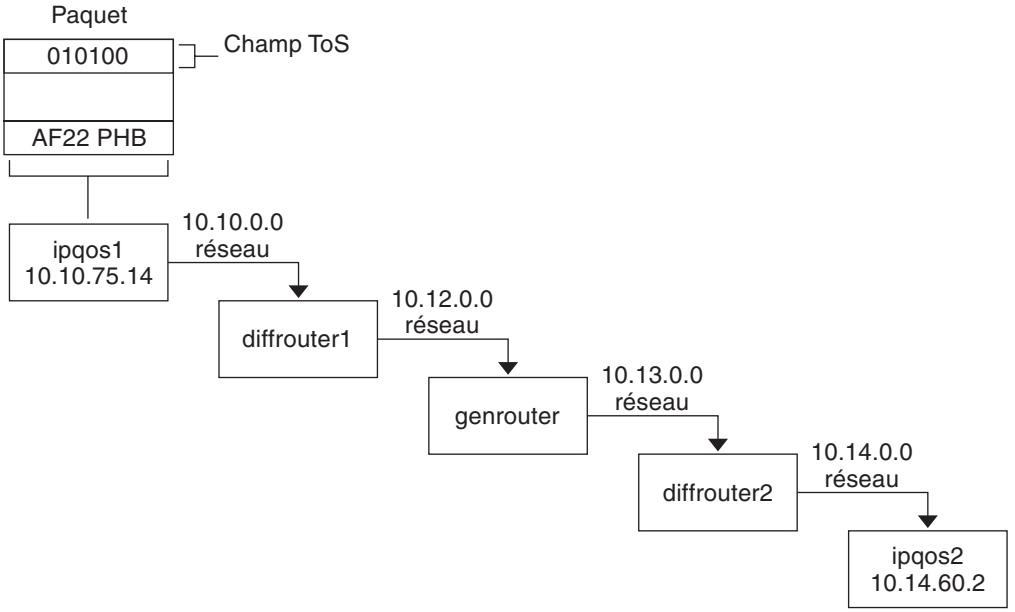
Le PHB *AF (assured forwarding)* comporte quatre classes de transmission différentes susceptibles d'être appliquées à un paquet. Chaque classe fournit, à son tour, trois niveaux de priorité comme indiqué dans le Tableau 37–2.

Les points de codes AF offrent la possibilité d'assigner différents niveaux de service aux clients et aux applications. Dans la stratégie QoS, il est possible de hiérarchiser le trafic et les services de votre réseau lorsque vous planifiez la stratégie QoS. Vous pouvez ensuite assigner différents niveaux AF au trafic auquel la priorité est accordée.

Transmission des paquets dans un environnement Diffserv

La figure suivante illustre une partie de l'intranet d'une entreprise dont l'environnement est partiellement soumis aux règles des services différenciés. Dans cet exemple, tous les hôtes des réseaux `10.10.0.0` et `10.14.0.0` sont compatibles IPQoS et les routeurs locaux sur les deux réseaux reconnaissent Diffserv. Cependant, des réseaux intermédiaires ne sont pas configurés pour prendre en charge les services du modèle Diffserv.

FIGURE 32–2 Transmission des paquets via les nœuds du réseau Diffserv



Les étapes suivantes montre la progression du flux du paquet illustrée dans cette figure. Les étapes présentent le paquet provenant de l'hôte `ipqos1`. Elles se poursuivent par le passage par plusieurs nœuds afin d'atteindre l'hôte `ipqos2`.

1. L'utilisateur au niveau de l'hôte `ipqos1` exécute la commande `ftp` pour accéder à l'hôte `ipqos2`, situé à trois sauts de là.
2. `ipqos1` applique sa stratégie QoS au flux de paquet. `ipqos1` établit la classification du trafic `ftp`.

   L'administrateur système a créé une classe pour l'ensemble du trafic `ftp` sortant émanant du réseau local 10.10.0.0. Le PHB AF22 est assigné au trafic de la classe `ftp` : classe 2, priorité de rejet moyenne. Un débit de 2 Mbits/sec est défini pour la classe `ftp`.
3. `ipqos-1` mesure le flux `ftp` pour déterminer si le flux dépasse le débit garanti de 2 Mbits/sec.
4. Le marqueur sur l'hôte `ipqos1` définit les champs DS des paquets `ftp` sortant à l'aide du DSCP 010100, correspondant au PHB AF22.
5. Le routeur `diffrouter1` reçoit les paquets `ftp. diffrouter1` prend connaissance du DSCP. Si `diffrouter1` est congestionné, les paquets marqués AF22 sont rejetés.
6. Le trafic `ftp` est transféré vers le nœud suivant conformément au PHB défini pour AF22 dans les fichiers de `diffrouter1` .
7. Le trafic `ftp` transite par le réseau `10.12.0.0` pour rejoindre le routeur `genrouter` qui ne reconnaît pas les services différenciés. Un traitement « au mieux » est alors appliqué au trafic.

8. `genrouter` transmet le trafic `ftp` au réseau `10.13.0.0` au sein duquel le trafic est reçu par le routeur `diffrouter2`.
9. `diffrouter2` reconnaît l'architecture Diffserv. Par conséquent, le routeur envoie les paquets `ftp` sur le réseau conformément au PHB défini dans la stratégie du routeur pour les paquets AF22.
10. `ipqos2` reçoit le trafic `ftp. ipqos2` demande à l'utilisateur au niveau de l'hôte `ipqos1` son nom d'utilisateur et son mot de passe.

◆ ◆ ◆ CHAPITRE 33

Planification d'un réseau IPQoS (tâches)

Vous pouvez configurer une architecture IPQoS sur un système qui exécute Oracle Solaris. Le système IPQoS fonctionne alors avec des routeurs Diffserv chargés de fournir des services différenciés et une gestion du trafic sur un intranet.

Ce chapitre décrit les tâches de planification visant à ajouter des systèmes IPQoS sur un réseau compatible avec Diffserv. Ce chapitre contient les sections suivantes.

Planification générale de la configuration IPQoS (liste des tâches)

Implémentation des services différenciés, et notamment IPQoS, sur un réseau nécessitant une planification étendue. Vous devez tenir compte de l'emplacement et de la fonction de chaque système IPQoS, mais également de la relation que chaque système entretient avec le routeur ou le réseau local. La liste des tâches suivante répertorie les principales tâches de planification pour l'implémentation d'une architecture IPQoS sur votre réseau et renvoie vers les procédures permettant d'effectuer ces tâches.

Tâche	Description	Voir
1. Planifiez une topologie de réseau Diffserv qui intègre les systèmes IPQoS.	Étudiez les différentes topologies de réseau Diffserv pour déterminer la solution la plus adaptée à votre site.	"Planification de la topologie de réseau Diffserv" à la page 822.

Tâche	Description	Voir
2. Planifiez les différents types de service qui seront offerts par les systèmes IPQoS.	Organisez les types de service que le réseau fournit dans les accords de niveau de service.	"Planification de la stratégie de qualité de service" à la page 825.
3. Planifiez la stratégie QoS pour chaque système IPQoS.	Identifiez les classes, les fonctions de mesure et de comptabilité nécessaires à l'implémentation de chaque accord de niveau de service.	"Planification de la stratégie de qualité de service" à la page 825.
4. Si nécessaire, planifiez la stratégie du routeur Diffserv.	Élaborez d'éventuelles stratégies de programmation et de mise en file d'attente pour le routeur Diffserv utilisé avec les systèmes IPQoS.	Pour plus d'informations sur ces stratégies, reportez-vous à la documentation du routeur.

Planification de la topologie de réseau Diffserv

Pour faire bénéficier votre réseau de services différenciés, vous devez disposer d'au moins un système IPQoS et d'un routeur compatible Diffserv. Vous pouvez intégrer ce scénario de base à une multitude de variantes, comme expliqué dans cette section.

Stratégies matérielles pour le réseau Diffserv

En général, les clients exécutent IPQoS sur les serveurs et les consolidations de serveurs comme le serveur Sun Enterprise™ 0000. Inversement, vous pouvez également exécuter IPQoS sur des ordinateurs de bureau tels que les systèmes UltraSPARC®, en fonction des besoins du réseau utilisé. La liste suivante décrit les systèmes possibles pour une configuration IPQoS :

- Systèmes Oracle Solaris offrant des services variés (serveurs Web et serveurs de base de données)
- Serveurs d'application proposant des applications de messagerie électronique, FTP ou d'autres applications réseau courantes
- Serveurs de cache Web ou serveurs proxy
- Réseau de batteries de serveurs IPQoS gérées par des équilibreurs de charge compatibles Diffserv
- Pare-feux gérant le trafic d'un seul réseau hétérogène
- Systèmes IPQoS faisant partie d'un réseau local virtuel

Vous pouvez insérer des systèmes IPQoS dans une topologie de réseau comportant des routeurs compatibles Diffserv. Si votre routeur n'inclut pas Diffserv, recherchez des solutions Diffserv auprès de Cisco Systems, Juniper Networks ou d'autres fabricants de routeurs. Si le routeur local n'implémente pas Diffserv, le routeur transmet les paquets marqués au nœud suivant sans analyser les marques.

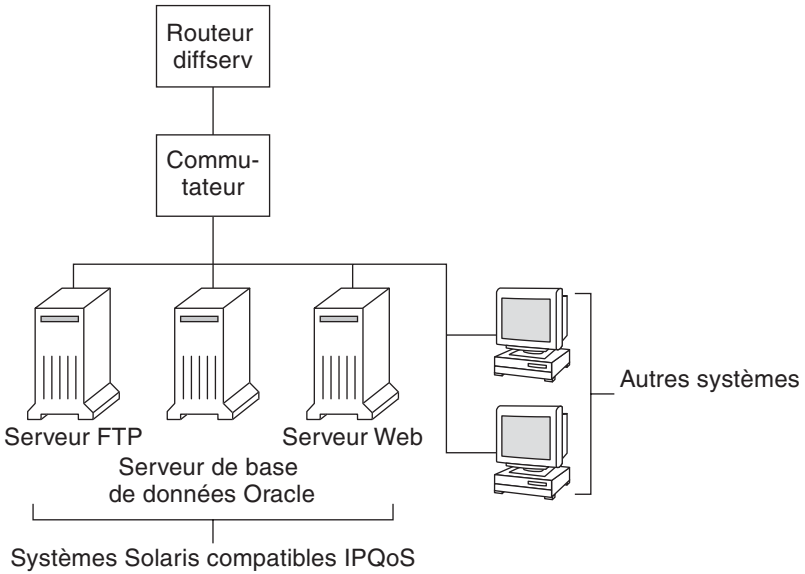
Topologies de réseau IPQoS

Cette section illustre les stratégies IPQoS qui répondent à différentes exigences de réseau.

IPQoS sur des hôtes indépendants

La figure suivante montre un réseau unique pour les systèmes compatibles IPQoS.

FIGURE 33–1 Systèmes IPQoS sur un segment de réseau



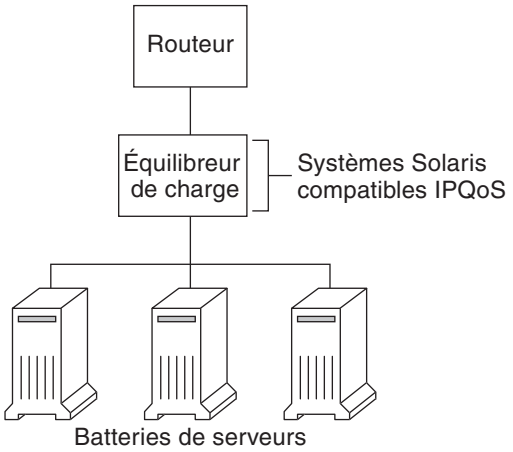
Ce réseau ne représente qu'un seul segment d'un intranet d'entreprise. En activant IPQoS sur les serveurs d'application et les serveurs Web, vous pouvez contrôler le débit auquel chaque système IPQoS libère le trafic sortant. Si le routeur Diffserv est compatible, vous pouvez contrôler davantage le trafic entrant et sortant.

Les exemples du présent guide font appel au scénario « IPQoS sur des hôtes indépendants ». Pour en savoir plus sur la topologie utilisée en guise d'exemple tout au long du guide, reportez-vous à la Figure 33–4.

IPQoS sur une batterie de serveurs réseau

La figure suivante présente un réseau avec des batteries de serveurs hétérogènes.

FIGURE 33–2 Réseau de batteries de serveurs compatibles IPQoS



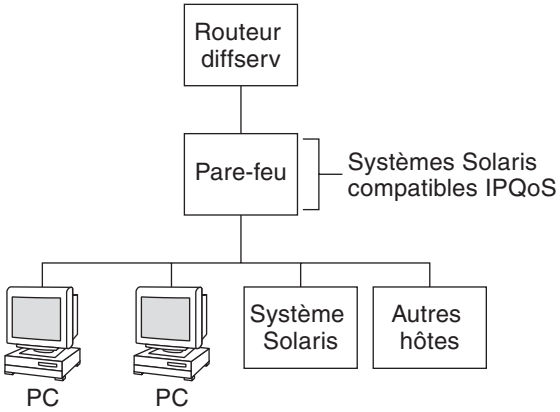
Dans une telle topologie, le routeur est compatible avec Diffserv et peut, à ce titre, mettre en attente et adapter le débit du trafic entrant et sortant. L'équilibreur de charge est également compatible avec Diffserv tandis que les batteries de serveurs reconnaissent le système IPQoS. L'équilibreur de charge peut fournir des fonctions de filtrage supplémentaires au-delà du routeur grâce à des sélecteurs de type ID utilisateur et ID projet. Ces sélecteurs sont inclus dans les données d'application

Ce scénario illustre un contrôle des flux et un transfert du trafic en mesure de gérer une éventuelle congestion du réseau local. Il interdit également au trafic sortant des batteries des serveurs d'encombrer d'autres sections du réseau intranet.

IPQoS sur un pare-feu

La figure suivante montre un segment d'un réseau d'entreprise sécurisé à partir d'autres segments au moyen d'un pare-feu.

FIGURE 33–3 Réseau protégé par un pare-feu compatible IPQoS



Dans l'exemple illustré, le trafic passe par le routeur compatible Diffserv où les paquets sont filtrés et mis en attente. Tout le trafic entrant, transféré par le routeur, transite alors par le pare-feu IPQoS. Pour utiliser IPQoS, le pare-feu ne doit pas passer outre la pile de transmission IP.

La stratégie de sécurité du pare-feu détermine si le trafic entrant est autorisé à entrer ou à sortir du réseau interne. La stratégie QoS contrôle les niveaux de service applicables au trafic entrant ayant traversé le pare-feu. Selon la stratégie QoS retenue, le trafic sortant peut également être associé à un comportement de transmission particulier.

Planification de la stratégie de qualité de service

Lorsque vous planifiez une stratégie de qualité de service (QoS), vous devez examiner, classer les services que le réseau fournit, puis leur donner un ordre de priorité. Vous devez également évaluer la quantité de bande passante disponible de manière à déterminer le débit de chaque classe de trafic arrivant sur le réseau.

Aides à la planification de la stratégie QoS

Rassemblez les informations pour la planification de la stratégie dans un format prenant en compte les informations nécessaires pour le fichier de configuration IPQoS. Par exemple, servez-vous du modèle suivant pour énumérer les catégories principales d'information à intégrer au fichier de configuration IPQoS.

TABLEAU 33–1 Modèle de planification QoS

Classe	Priorité	Filtre	Sélecteur	Débit	Transfert ?	Comptabilisation ?
Classe 1	1	Filtre1 Filtre 3	Sélecteur 1 Sélecteur 2	Débits de l'indicateur selon le type de mesure	Niveau de priorité du marqueur	Requiert des statistiques de comptabilisation des flux
Classe 1	1	Filtre 2	Sélecteur 1 Sélecteur 2	SO	SO	SO
Classe 2	2	Filtre1	Sélecteur 1 Sélecteur 2	Débits de l'indicateur selon le type de mesure	Niveau de priorité du marqueur	Requiert des statistiques de comptabilisation des flux
Classe 2	2	Filtre 2	Sélecteur 1 Sélecteur 2	SO	SO	SO

Il est possible de diviser chaque catégorie principale pour définir encore plus précisément la stratégie QoS. Les sections suivantes indiquent comment obtenir des informations sur les catégories illustrées dans le modèle.

Planification de la stratégie QoS (liste des tâches)

Cette liste de tâches répertorie les principales tâches de planification d'une stratégie QoS et renvoie vers les procédures permettant d'effectuer chaque tâche.

Tâche	Description	Voir
1. Établissez la topologie du réseau pour qu'il prenne en charge IPQoS.	Identifiez les hôtes et les routeurs du réseau de manière à fournir des services différenciés.	"Préparation d'un réseau pour IPQoS" à la page 827
2. Définissez les classes dans lesquelles les services du réseau doivent être répartis.	Examinez les types de service et les niveaux de service offerts par votre site et déterminez à quelles classes de trafic discret les services appartiennent.	"Définition des classes pour votre stratégie QoS" à la page 828
3. Définissez les filtres pour les classes.	Déterminez les méthodes les plus adaptées pour isoler le trafic d'une classe particulière par rapport au flux du trafic réseau.	"Définition de filtres dans la stratégie QoS" à la page 831

Tâche	Description	Voir
4. Définissez les débits de contrôle de flux visant à mesurer le trafic lorsque les paquets quittent le système IPQoS.	Déterminez les débits acceptables pour chaque classe de trafic.	"Planification du contrôle de flux" à la page 832
5. Définissez les valeurs DSCP ou les valeurs dont la priorité est définie par l'utilisateur à appliquer à la stratégie QoS.	Mettez en place un plan et déterminez le comportement de transmission assigné à un flux de trafic si le flux est géré par le routeur ou le commutateur.	"Planification du comportement de transmission" à la page 835
6. Le cas échéant, définissez un plan de contrôle statistique concernant les flux de trafic sur le réseau.	Analysez les classes de trafic pour identifier les flux à contrôler à des fins comptables ou statistiques.	"Planification de la comptabilisation des flux" à la page 838

Remarque – La suite de la section décrit la planification de la stratégie QoS d'un système IPQoS. Pour planifier la stratégie QoS d'un routeur Diffserv, consultez la documentation du routeur ainsi que le site Web du fabricant.

▼ Préparation d'un réseau pour IPQoS

La procédure suivante dresse la liste des tâches générales de planification à effectuer avant de créer la stratégie QoS.

1 **Examinez la topologie du réseau. Élaborez ensuite une stratégie associant les systèmes IPQoS et les routeurs Diffserv.**

Pour consulter des exemples de topologie, reportez-vous à la section "Planification de la topologie de réseau Diffserv" à la page 822.

2 **Identifiez les hôtes de la topologie qui nécessitent IPQoS ou qui sont susceptibles d'être intéressés par le service IPQoS.**

3 **Définissez parmi les systèmes compatibles IPQoS ceux qui peuvent recourir à la même stratégie QoS.**

Si, par exemple, vous envisagez d'activer IPQoS sur tous les hôtes du réseau, identifiez ceux qui peuvent utiliser une même stratégie QoS. Chaque système IPQoS doit posséder une stratégie QoS locale. Celle-ci est implémentée dans le fichier de configuration IPQoS associé. Cependant, il est possible de créer un fichier de configuration IPQoS exploitable par une large gamme de systèmes. Il suffit alors de copier le fichier de configuration dans chaque système partageant les mêmes exigences en matière de stratégie QoS.

4 **Évaluez et effectuez toutes les tâches de planification requises par le routeur Diffserv sur votre réseau.**

Reportez-vous à la documentation du routeur et au site Web du fabricant pour plus de détails.

▼ Définition des classes pour votre stratégie QoS

La première étape de la définition de la stratégie QoS consiste à organiser les flux de trafic en plusieurs classes. Vous n'avez pas besoin de créer des classes pour chaque type de trafic sur un réseau Diffserv. De plus, selon la topologie du réseau, vous pouvez être amené à créer une stratégie QoS différente pour chaque système compatible IPQoS.

Remarque – Pour des informations générales sur les classes, reportez-vous à la section "Classes IPQoS" à la page 812.

La procédure suivante suppose que vous ayez établi les systèmes de votre réseau qui sont compatibles IPQoS comme indiqué dans la section "Préparation d'un réseau pour IPQoS" à la page 827.

1 **Créez un tableau de planification QoS pour organiser les informations de la stratégie QoS.**

Pour obtenir des suggestions, reportez-vous au Tableau 33–1.

2 **Effectuez les étapes restantes pour chaque stratégie QoS figurant sur le réseau.**

3 **Définissez les classes à utiliser dans la stratégie QoS.**

Les questions suivantes contribuent à analyser le trafic réseau en vue de la définition de classes.

- **L'entreprise offre-t-elle des accords de niveau de service à ses clients ?**

  Si oui, évaluez les niveaux de priorité relatifs définis pour les accords de niveau de service qu'offre l'entreprise. Les clients peuvent se voir proposer une même application assortie de niveaux de priorité différents.

  Par exemple, l'entreprise peut offrir un hébergement de site Web à chacun de ses clients ce qui signifie qu'il est nécessaire de définir une classe pour chaque site Web client. Un accord de niveau de service peut fournir un site Web Premium au titre d'un niveau de service. Un autre accord de niveau de service peut consister en un site Web personnel utilisable « au mieux » à l'usage de clients bénéficiant de remises. Ce facteur signale non seulement différentes classes de sites Web, mais également des comportements (PHB) potentiellement différents, assignés aux classes de sites Web.

- **Le système IPQoS offre-t-il des applications courantes nécessitant éventuellement un contrôle des flux ?**

Vous pouvez améliorer les performances réseau en activant IPQoS sur les serveurs proposant des applications courantes qui génèrent un trafic important. Les exemples les plus courants sont les applications de messagerie électronique, de discussion réseau et FTP. Envisagez de créer des classes indépendantes pour le trafic entrant et sortant de chaque type de service, si besoin est. Par exemple, il est possible de créer une classe `courrier entrant` et une classe `courrier sortant` pour la stratégie QoS d'un serveur de messagerie.

- **Le réseau exécute-t-il des applications qui impliquent une transmission en haute priorité ?**

  Toute application critique nécessitant une transmission en priorité haute doit être prioritaire dans la file d'attente du routeur. C'est le cas, par exemple, des flux de données vidéo et audio.

  Définissez les classes entrantes et sortantes pour ces applications à haute priorité. Ensuite, insérez les classes dans les stratégies QoS du routeur Diffserv et du système IPQoS fournissant les applications.

- **Le réseau fait-il l'objet de flux de trafic à contrôler en raison de la consommation importante de bande passante ?**

  Exécutez `netstat` , `snoop` et d'autres utilitaires de contrôle réseau pour détecter les types de trafic à l'origine des problèmes survenant sur le réseau. Étudiez les classes que vous avez créées jusqu'ici, puis générez de nouvelles classes pour les catégories de problèmes de trafic non définis. Si vous avez déjà défini des classes pour une catégorie de problèmes, définissez les débits du compteur chargé de contrôler le trafic problématique.

  Créez des classes pour le trafic posant problème dans chaque système IPQoS situé sur le réseau. Chaque système IPQoS peut alors gérer un trafic problématique en réduisant le débit du flux arrivant sur le réseau. Assurez-vous également de spécifier ces classes dans la stratégie QoS sur le routeur Diffserv. Le routeur peut ainsi mettre en attente et planifier les flux problématiques conformément à la configuration de la stratégie QoS.

- **Avez-vous besoin de connaître les statistiques sur certains types de trafic ?**

  L'examen rapide d'un accord de niveau de service peut révéler les types des trafics client devant être comptabilisés. Si votre site offre des accords de niveau de service, vous avez sans doute déjà créé des classes relatives au trafic impliquant des données de comptabilisation. Vous pouvez également être amené à définir des classes en vue de la collecte de statistiques concernant les flux de trafic que vous contrôlez. Il est possible de définir des classes pour le trafic soumis à des restrictions d'accès pour des raisons de sécurité.

4 Dressez la liste des classes que vous avez définies dans le tableau de planification QoS élaboré à l'étape 1.

5 Attribuez un niveau de priorité à chacune des classes.

Par exemple, le niveau de priorité 1 représente la classe dotée de la priorité la plus élevée. Définissez les priorités suivantes en ordre décroissant pour les autres classes. Le niveau de priorité assigné est utilisé à des fins organisationnelles uniquement. Les niveaux de priorité

définis dans le modèle de stratégie QoS ne sont pas réellement utilisés par IPQoS. Par ailleurs, vous pouvez attribuer une même priorité à plusieurs classes si cela convient à la stratégie QoS.

6 **Lorsque vous avez terminé la définition des classes, vous pouvez passer à la définition des filtres pour chaque classe, comme expliqué à la section "Définition de filtres dans la stratégie QoS" à la page 831.**

Informations supplémentaires

Définition de la priorité des classes

Au fur et à mesure que vous créez des classes, vous vous rendrez compte des classes devant bénéficier de la priorité la plus élevée, d'une priorité moyenne ou d'une priorité « au mieux ». Un plan de hiérarchisation des classes s'avère particulièrement important lorsque vous assignez des comportements par pas au trafic sortant comme indiqué à la section "Planification du comportement de transmission" à la page 835.

Outre l'attribution d'un tel comportement à une classe, il est également possible de définir, pour la classe, un sélecteur de priorité dans un filtre. Le sélecteur de priorité est actif sur l'hôte IPQoS seulement. Considérons plusieurs classes avec des débits et des valeurs DSCP (Differentiated Services Code Point) identiques qui se font concurrence au niveau de la bande passante lorsqu'ils sortent du système IPQoS. Le sélecteur de priorité de chaque classe permet de classer le niveau de service attribué aux classes dont les valeurs sont identiques.

Définition des filtres

Les filtres créés permettent d'identifier les flux de paquets appartenant à une classe particulière. Chaque filtre contient des sélecteurs définissant les critères qui contribuent à l'évaluation d'un flux de paquet. Le système IPQoS utilise ensuite les critères des sélecteurs pour extraire les paquets à partir d'un flux de trafic. Le système IPQoS associe ensuite les paquets à une classe. Pour obtenir une présentation des filtres, reportez-vous à la section "Filtres IPQoS" à la page 812.

Le tableau suivant répertorie les sélecteurs les plus répandus. Les cinq premiers sélecteurs représentent l'uplet IPQoS dont le système IPQoS se sert pour identifier les paquets sous forme de membres d'un flux. Pour obtenir la liste complète des sélecteurs, reportez-vous au Tableau 37–1.

TABLEAU 33–2 Sélecteurs IPQoS communs

Nom	Définition
`saddr`	Adresse source.
`daddr`	Adresse de destination.
`sport`	Numéro de port source. Vous pouvez utiliser un numéro de port connu comme indiqué dans `/etc/services` ou un numéro de port défini par l'utilisateur.

TABLEAU 33–2 Sélecteurs IPQoS communs *(Suite)*

Nom	Définition
`dport`	Numéro de port de destination.
`protocol`	Numéro de protocole IP ou nom du protocol attribué au type de flux de trafic dans le fichier `/etc/protocols`.
`ip_version`	Style d'adresse à utiliser. Vous avez le choix entre IPv4 et IPv6. IPv4 est le style par défaut.
`dsfield`	Contenu du champ DS, c'est-à-dire la valeur DSCP. Servez-vous de ce sélecteur pour extraire les paquets entrants déjà signalés par une valeur DSCP.
`priority`	Niveau de priorité attribué à la classe. Pour plus d'informations, reportez-vous à la section "Définition des classes pour votre stratégie QoS" à la page 828.
`user`	Identifiant utilisateur UNIX ou nom de l'utilisateur à l'exécution de l'application de niveau supérieur.
`projid`	ID de projet utilisé à l'exécution de l'application de niveau supérieur.
`direction`	Direction du flux de trafic. La valeurs est `LOCAL_IN`, `LOCAL_OUT`, `FWD_IN` ou `FWD_OUT`.

Remarque – Choisissez les sélecteurs avec discernement. Veillez à ne pas utiliser plus de sélecteurs que nécessaire pour extraire les paquets d'une classe. En effet plus le nombre de sélecteurs est important, plus cela aura d'impact sur les performances IPQoS.

▼ Définition de filtres dans la stratégie QoS

Avant de commencer

Avant d'effectuer les étapes suivantes, vous devez avoir suivi la procédure "Définition des classes pour votre stratégie QoS" à la page 828.

1. **Créez au moins un filtre pour chaque classe dans la planification QoS que vous avez mise sur pied à la section "Définition des classes pour votre stratégie QoS" à la page 828.**

   Envisagez de créer des filtres indépendants pour le trafic entrant et le trafic sortant de chaque classe, si besoin est. Par exemple, intégrez un filtre `ftp-in` et un filtre `ftp-out` à la stratégie QoS d'un serveur FTP compatible IPQoS. Vous pouvez ensuite définir le sélecteur `direction` qui convient en plus des sélecteurs de base.

2. **Définissez au moins un sélecteur pour chaque filtre au sein d'une classe.**

   Utilisez le tableau de planification QoS, illustré par le Tableau 33–1, pour remplir les filtres des classes définies.

Exemple 33–1 Définition des filtres pour le trafic FTP

Le tableau suivant explique comment définir un filtre pour le trafic FTP sortant.

Classe	Priorité	Filtres	Sélecteurs
`ftp-traffic`	4	`ftp-out`	`saddr 10.190.17.44`
			`daddr 10.100.10.53`
			`sport 21`
			`direction LOCAL_OUT`

Voir aussi

- Pour définir un plan de contrôle des flux, reportez-vous à la section "Planification du contrôle de flux" à la page 832.
- Pour spécifier les comportements de transmission associés aux flux lorsqu'ils reviennent sur le réseau, reportez-vous à la section "Planification du comportement de transmission" à la page 835.
- Pour planifier la comptabilisation des flux pour certains types de trafic, reportez-vous à la section "Planification de la comptabilisation des flux" à la page 838.
- Pour ajouter plusieurs classes à la stratégie QoS, reportez-vous à la section "Définition des classes pour votre stratégie QoS" à la page 828.
- Pour ajouter plusieurs filtres à la stratégie QoS, reportez-vous à la section "Définition de filtres dans la stratégie QoS" à la page 831.

▼ Planification du contrôle de flux

Le contrôle de flux implique de mesurer les flux de trafic pour une classe, puis de libérer les paquets sur le réseau à un débit défini. Lorsque vous planifiez le contrôle de flux, vous définissez les paramètres à appliquer aux modules de mesure IPQoS. Les compteurs déterminent le débit auquel le trafic est diffusé sur le réseau. Pour une présentation des modules de mesure, reportez-vous à la section "Présentation des compteurs (`tokenmt` et `tswtclmt`)" à la page 812.

La procédure suivante suppose que vous ayez défini les filtres et les sélecteurs comme décrit dans la section "Définition de filtres dans la stratégie QoS" à la page 831.

1. **Déterminez la bande passante maximum pour votre réseau.**

2. **Vérifiez tous les accords de niveau de service gérés par le réseau. Identifiez les clients et le type de service assuré.**

   Pour garantir un niveau de service donné, il peut être indispensable de contrôler certaines classes de trafic générées par le client.

3 **Vérifiez la liste des classes créées à la section "Définition des classes pour votre stratégie QoS" à la page 828.**

Déterminez si d'autres classes, outre celles qui sont associées aux accords de niveau de service, doivent faire l'objet de mesures.

Supposons que le système IPQoS exécute une application générant un niveau de trafic élevé. Après avoir établi une classification du trafic de l'application, évaluez les flux de manière à vérifier le débit auquel les paquets du flux arrivent sur le réseau.

Remarque – Il n'est pas utile de quantifier toutes les classes. Gardez à l'esprit cette consigne lorsque vous examinez la liste des classes.

---

4 **Dans chaque classe, déterminez les filtres en rapport avec un trafic devant faire l'objet d'un contrôle de flux. Affinez ensuite la liste des classes nécessitant des opérations de mesure.**

Lorsque les classes sont dotées de plusieurs filtres, il se peut que seul un filtre exige d'être contrôlé. Supposons que vous définissiez des filtres pour le trafic entrant et le trafic sortant d'une classe donnée. Vous pouvez établir que seul trafic d'une direction exige un contrôle de flux.

5 **Choisissez un module de mesure pour chaque classe à traiter.**

Ajoutez le nom du module à la colonne de mesure dans le tableau de planification QoS.

6 **Ajoutez les débits des classes à mesurer dans la table organisationnelle.**

Si vous utilisez le module `tokenmt`, définissez les débits en bits par seconde suivants :

- Débit garanti
- Débit de pointe

Si ces débits suffisent à mesurer une classe donnée, contentez-vous de spécifier le débit garanti et la taille de rafale garantie pour le module `tokenmt`.

Si nécessaire, vous pouvez également définir les débits suivants :

- Taille de rafale garantie
- Taille de rafale de pointe

Pour la définition complète des débits `tokenmt`, reportez-vous à la section "Configuration du `tokenmt` en tant que compteur à débit double" à la page 889. Vous trouverez également des informations plus détaillées dans la page de manuel `tokenmt` (7ipp).

Si vous recourez au module `tswtclmt`, il est nécessaire de définir les débits (en bits par seconde) suivants.

- Débit garanti
- Débit de pointe

Vous pouvez aussi paramétrer la taille de la fenêtre en millisecondes. Ces débits sont indiqués à la section "Module de mesure `tswtclmt`" à la page 890 et à la page de manuel `twstclmt`(7ipp).

7 Ajoutez les résultats de conformité du trafic mesuré.

Les résultats des deux modules de mesure s'affichent en vert, en rouge et en orange. Ajoutez à votre tableau organisationnel QoS, les résultats de la conformité du trafic concernant les débits que vous définissez. Les résultats des opérations de mesure sont expliqués en détail dans la section "Module de mesure" à la page 888.

Vous devez préciser l'action à entreprendre lorsque le trafic se conforme ou ne se conforme pas au débit garanti. La plupart du temps, cette action consiste à marquer l'en-tête du paquet par un comportement appelé PHB (per-hop behavior). Lorsque le trafic est vert, l'action autorisée peut être de continuer le traitement des flux de trafic tant que ces derniers ne dépassent pas le contrat de trafic. Une autre action possible peut être de rejeter les paquets de la classe si les flux sont supérieurs au débit de pointe.

Exemple 33–2 Définition des compteurs

Le tableau suivant affiche les entrées d'une classe de trafic de messagerie électronique. Le réseau sur lequel se trouve le système IPQoS dispose d'une bande passante totale de 100 Mbits/sec, soit 10 millions de bits par seconde. La stratégie QoS assigne une priorité basse à la classe du courrier électronique. Cette classe obtient également le traitement « au mieux ».

Classe	Priorité	Filtre	Sélecteur	Débit
`email`	8	`mail_in`	`daddr10.50.50.5`	
			`dport imap`	
			`direction LOCAL_IN`	
`email`	8	`mail_out`	`saddr10.50.50.5`	mesure=`tokenmt`
			`sport imap`	débit garanti=5000000
			`direction LOCAL_OUT`	taille de rafale garantie =5000000
				débit de pointe =10000000
				taille de rafale de pointe=1000000
				niveau de priorité vert=poursuivre le traitement
				niveau de priorité orange=signaliser par un PHB orange
				niveau de priorité rouge=rejeter

Voir aussi

- Pour spécifier les comportements de transmission associés aux flux lorsque les paquets arrivent dans le réseau, reportez-vous à la section "Planification du comportement de transmission" à la page 835.
- Pour planifier la comptabilisation des flux pour certains types de trafic, reportez-vous à la section "Planification de la comptabilisation des flux" à la page 838.
- Pour ajouter plusieurs classes à la stratégie QoS, reportez-vous à la section "Définition des classes pour votre stratégie QoS" à la page 828.
- Pour ajouter plusieurs filtres à la stratégie QoS, reportez-vous à la section "Définition de filtres dans la stratégie QoS" à la page 831.
- Pour définir un autre plan de contrôle des flux, reportez-vous à la section "Planification du contrôle de flux" à la page 832.
- Pour créer un fichier de configuration IPQoS, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.

Planification du comportement de transmission

Le comportement de transmission détermine la priorité ainsi que le niveau de priorité des flux de trafic qui vont être transférés au réseau. Vous avez le choix entre deux comportements principaux : hiérarchiser les flux d'une classe par rapport à d'autres classes de trafic ou rejeter l'intégralité des flux.

Le modèle Diffserv utilise un marqueur pour assigner le comportement de transmission choisi aux flux de trafic. IPQoS comporte les deux modules de marquage suivants.

- `dscpmk` – Permet de marquer le champ DS d'un paquet IP à l'aide d'un DSCP (Differentiated Service Code Point, point de code de services différenciés)
- `dlcosmk` – Sert à marquer l'étiquette VLAN d'un datagramme par une valeur de classe de service (CoS)

Remarque – Les suggestions de cette section concernent les paquets IP uniquement. Si votre système IPQoS comprend un dispositif VLAN, vous pouvez utiliser le marqueur `dlcosmk` pour identifier certains comportements de transmission associés aux datagrammes. Pour plus d'informations, reportez-vous à la section "Utilisation du marqueur `dlcosmk` avec les périphériques VLAN" à la page 893.

Pour définir la priorité d'un trafic IP, vous devez attribuer un DSCP à chaque paquet. Le marqueur `dscpmk` code le champ DS du paquet à l'aide d'un DSCP. Vous choisissez le DSCP pour une classe dans un groupe de points de codes connus associés au type de comportement. Ces points de codes correspondent à 46 (101110) pour le PHB de classe EF et une plage de points de codes pour le PHB de classe AF. Pour des informations générales sur le DSCP et la transmission, reportez-vous à la section "Trafic sur un réseau compatible IPQoS" à la page 816.

Avant de commencer Les étapes suivantes supposent que vous ayez défini les classes et les filtres de la stratégie QoS. Même si vous combinez généralement les opérations de mesure et de marquage du trafic à contrôler, le marquage seul permet de définir un comportement de transmission.

1. **Vérifiez les classes créées jusqu'à présent, ainsi que les priorités assignées à chacune d'entre elles.**

   Il n'est pas utile de marquer toutes les classes de trafic.

2. **Attribuez le PHB EF (expedited forwarding, traitement accéléré) à la classe avec la priorité la plus élevée.**

   Le PHB EF garantit que les paquets marqués EF DSCP 46 (101110) sont diffusés sur le réseau avant les paquets de classe AF. Réservez le PHB EF pour le trafic prioritaire. Pour plus d'informations sur EF, reportez-vous à la section "PHB Expedited Forwarding (EF) (ou traitement accéléré)" à la page 892.

3. **Attribuez des comportements de routeurs aux classes dont le trafic doit être mesuré.**

4. **Définissez des points de codes DS pour les autres classes conformément aux priorités associées aux classes.**

Exemple 33–3 Stratégie QoS pour une application de jeu

Le trafic est généralement mesuré pour les raisons suivantes :

- Un accord de niveau de service garantit aux paquets de cette classe un service supérieur ou inférieur lorsque le réseau est fortement sollicité.
- Une classe dotée d'une priorité moindre aura tendance à submerger le réseau.

Les fonctions de marquage et de mesure permettent de fournir à ces classes des services différenciés et une gestion de la bande passante. Le tableau suivant présente, à titre d'exemple, une partie d'une stratégie QoS. Cette stratégie définit une classe pour un jeu populaire générant un niveau important de trafic.

Classe	Priorité	Filtre	Sélecteur	Débit	Transfert ?
`games_app`	9	`games_in`	`sport 6080`	SO	SO

Classe	Priorité	Filtre	Sélecteur	Débit	Transfert ?
`games_app`	9	`games_out`	`dport 6081`	mesure=`tokenmt`	vert =AF31
				débit garanti=5000000	orange=AF42
				taille de rafale garantie =5000000	rouge=rejeter
				débit de pointe =10000000	
				taille de rafale de pointe=15 000 000	
				niveau de priorité vert=poursuivre le traitement	
				niveau de priorité orange=signaliser par un PHB orange	
				niveau de priorité rouge=rejeter	

Les comportements assignent des DSCP de priorité basse au trafic `games_app` conforme au débit garanti ou inférieur au débit de pointe. Si le trafic `games_app` dépasse le débit de pointe, la stratégie QoS indique que les paquets issus du trafic `games_app` doivent être ignorés. Le Tableau 37–2 dresse la liste de tous les points de codes AF.

Voir aussi

- Pour planifier la comptabilisation des flux pour certains types de trafic, reportez-vous à la section “Planification de la comptabilisation des flux” à la page 838.
- Pour ajouter plusieurs classes à la stratégie QoS, reportez-vous à la section “Définition des classes pour votre stratégie QoS” à la page 828.
- Pour ajouter plusieurs filtres à la stratégie QoS, reportez-vous à la section “Définition de filtres dans la stratégie QoS” à la page 831.
- Pour définir un plan de contrôle des flux, reportez-vous à la section “Planification du contrôle de flux” à la page 832.
- Pour spécifier d'autres comportements de transmission associés aux flux lorsque les paquets arrivent dans le réseau, reportez-vous à la section “Planification du comportement de transmission” à la page 835.
- Pour créer un fichier de configuration IPQoS, reportez-vous à la section “Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 848.

▼ Planification de la comptabilisation des flux

Faites appel au module `flowacct` IPQoS pour effectuer le suivi des flux de trafic à des fins de facturation et de gestion du réseau. Appliquez la procédure pour déterminer si votre stratégie QoS doit inclure une comptabilisation des flux.

1 Votre entreprise offre-t-elle des accords de niveaux de services à ses clients ?

Dans l'affirmative, recourez à la comptabilisation des flux. Examinez les accords de niveaux de services pour déterminer les types de trafic réseau que l'entreprise veut facturer à ces clients. Passez ensuite en revue votre stratégie QoS pour identifier les classes de trafic à facturer.

2 Existe-t-il des applications devant faire l'objet d'un contrôle ou d'un test pour pallier des éventuels problèmes liés au réseau ?

Dans l'affirmative, envisagez de faire appel à la comptabilisation des flux de manière à observer le comportement de ces applications. Examinez la stratégie QoS pour identifier les classes assignées au trafic et qui nécessitent un contrôle.

3 Signalez par la lettre O, dans la colonne de comptabilisation des flux, chaque classe nécessitant une comptabilisation dans la table de planification QoS.

Voir aussi

- Pour ajouter plusieurs classes à la stratégie QoS, reportez-vous à la section "Définition des classes pour votre stratégie QoS" à la page 828.
- Pour ajouter plusieurs filtres à la stratégie QoS, reportez-vous à la section "Définition de filtres dans la stratégie QoS" à la page 831.
- Pour définir un plan de contrôle des flux, reportez-vous à la section "Planification du contrôle de flux" à la page 832.
- Pour spécifier les comportements de transmission associés aux flux lorsque les paquets arrivent dans le réseau, reportez-vous à la section "Planification du comportement de transmission" à la page 835.
- Pour planifier d'autres comptabilisations des flux pour certains types de trafic, reportez-vous à la section "Planification de la comptabilisation des flux" à la page 838.
- Pour créer le fichier de configuration IPQoS, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.

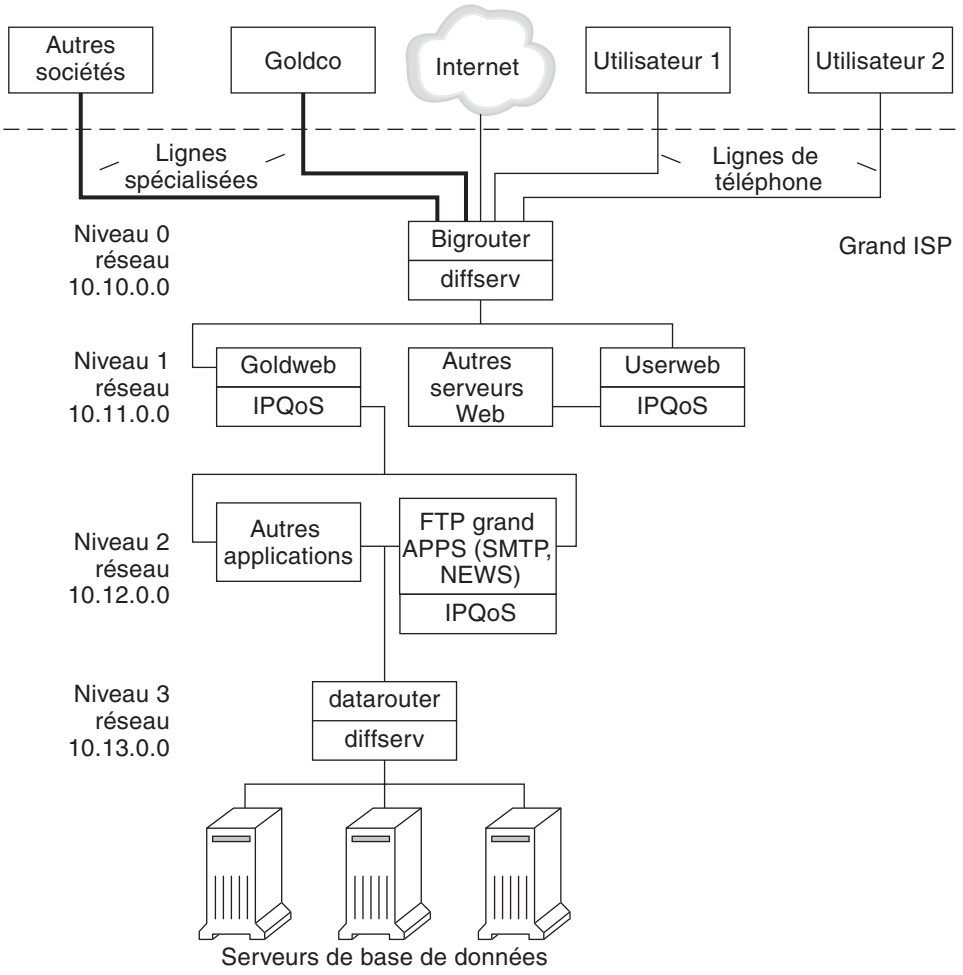
Présentation d'un exemple de configuration IPQoS

Les tâches des autres chapitres de ce guide reprennent l'exemple de configuration IPQoS présenté dans cette section. L'exemple fait état d'une solution de services différenciés mise en place pour l'intranet public de BigISP, fournisseur de services fictif. BigISP offre des services à des grandes entreprises qui ont accès à BigISP par le biais de lignes spécialisées. Les utilisateurs qui se connectent via des modems peuvent également acheter des services auprès de BigISP.

Topologie IPQoS

La figure suivante illustre la topologie du réseau exploitée par l'intranet public de BigISP.

FIGURE 33–4 Exemple de topologie IPQoS



BigISP a mis en place les quatre niveaux suivants dans son intranet public :

- **Niveau 0** – Le réseau `10.10.0.0` inclut un routeur Diffserv étendu appelé `Bigrouter` possédant des interfaces externes et internes. Plusieurs sociétés, notamment une grande organisation dénommée Goldco, a loué des services à lignes spécialisées aboutissant au `Bigrouter`. Le niveau 0 gère également des particuliers qui communiquent via les lignes téléphoniques ou le réseau RNIS.
- **Niveau 1** – Le réseau `10.11.0.0` fournit des services Web. Le serveur `Goldweb` héberge le site Web de Goldco que ce dernier a acquis auprès de BigISP dans le cadre du service premium. Le serveur `Userweb` héberge des sites Web de taille réduite achetés par des particuliers. Les sites `Goldweb` et `Userweb` sont compatibles IPQoS.

- **Niveau 2** – Le réseau `10.12.0.0` met des applications à la disposition de l'ensemble de ses clients. Le serveur d'applications `BigAPPS` est compatible IPQoS. `BigAPPS` fournit des services de type SMTP, actualités et FTP.
- **Niveau 1** – Le réseau `10.13.0.0` héberge des serveurs de bases de données de grande taille. L'accès au niveau 3 est contrôlé par `datarouter` (routeur Diffserv).

◆ ◆ ◆ CHAPITRE 34

Création du fichier de configuration IPQoS (tâches)

Ce chapitre décrit la procédure de création de fichiers de configuration IPQoS. Ce chapitre aborde les points suivants :

Ce chapitre suppose que vous ayez préalablement défini une stratégie QoS complète et que vous soyez prêt à l'appliquer comme base du fichier de configuration IPQoS. Pour obtenir des instructions sur la planification de la stratégie QoS, reportez-vous à la section "Planification de la stratégie de qualité de service" à la page 825.

Définition d'une stratégie QoS dans le fichier de configuration IPQoS (liste des tâches)

Cette liste répertorie les tâches IPQoS d'ordre général nécessaires à la création d'un fichier de configuration et les liens vers les sections décrivant les étapes à suivre pour effectuer ces tâches.

Tâche	Description	Voir
1. Planifiez la configuration de votre réseau IPQoS.	Déterminez les systèmes sur le réseau local qui doivent être activés pour IPQoS.	"Préparation d'un réseau pour IPQoS" à la page 827

Tâche	Description	Voir
2. Planifiez la stratégie QoS pour les systèmes IPQoS sur votre réseau.	Déterminez les différentes classes de service pour les flux de trafic. Déterminez ensuite les flux nécessitant une gestion du trafic.	"Planification de la stratégie de qualité de service" à la page 825
3. Créez le fichier de configuration IPQoS et définissez son action initiale.	Créez le fichier IPQoS, appelez le classificateur IP et définissez une classe de traitement.	"Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848
4. Créez les filtres d'une classe.	Ajoutez les filtres qui définissent le trafic sélectionné et organisé en une classe.	"Définition des filtres dans le fichier de configuration IPQoS" à la page 850
5. Ajoutez plusieurs classes et des filtres au fichier de configuration IPQoS.	Créez des classes et des filtres supplémentaires pour le traitement par le classificateur IP.	"Création d'un fichier de configuration IPQoS pour un serveur Web au mieux" à la page 856
6. Ajoutez une instruction `action` avec des paramètres visant à configurer les modules de mesure.	Si la stratégie QoS fait appel au contrôle de flux, spécifiez les débits de contrôle de flux ainsi que les niveaux de conformité par rapport au compteur.	"Configuration du contrôle de flux dans le fichier de configuration IPQoS " à la page 866
7. Ajoutez une instruction d'`action` avec des paramètres visant à configurer le marqueur.	Si la stratégie QoS fait intervenir des comportements différenciés, définissez le mode de transmission des différentes classes de service.	"Définition de la transmission du trafic dans le fichier de configuration IPQoS" à la page 852
8. Ajoutez une instruction `action` aux paramètres visant à configurer les modules de mesure.	Si la stratégie QoS implique la collecte de statistiques relatives aux flux de trafic, définissez la manière dont les données sont rassemblées.	"Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS" à la page 855
9. Appliquez le fichier de configuration IPQoS.	Ajoutez le contenu d'un fichier de configuration IPQoS spécifié dans le module du noyau qui convient.	"Application d'une nouvelle configuration aux modules de noyau IPQoS" à la page 872
10. Configurez les comportements dans les fichiers du routeur.	Si les fichiers de configuration IPQoS du réseau définissent les comportements de transmission, ajoutez les DSCP obtenus dans les fichiers d'ordonnancement appropriés sur le routeur.	"Configuration d'un routeur dans un réseau compatible IPQoS " à la page 869

Outils de création d'une stratégie QoS

La stratégie QoS de votre réseau se trouve dans le fichier de configuration IPQoS. Vous créez ce fichier de configuration dans un éditeur de texte. Définissez ensuite ce fichier comme argument de l'utilitaire de configuration IPQoS, `ipqosconf`. Lorsque vous donnez pour instruction à `ipqosconf` d'appliquer la stratégie définie dans le fichier de configuration, la stratégie est consignée dans le noyau du système IPQoS. Pour des informations détaillées sur la commande `ipqosconf`, reportez-vous à la page de manuel `ipqosconf`(1M). Pour obtenir des instructions sur l'utilisation d'`ipqosconf` , reportez-vous à la section "Application d'une nouvelle configuration aux modules de noyau IPQoS" à la page 872.

Fichier de configuration IPQoS standard

Un fichier de configuration IPQoS consiste en l'arborescence d'une instruction d'`action` chargée d'implémenter la stratégie QoS, définie à la section "Planification de la stratégie de qualité de service" à la page 825. Le fichier de configuration IPQoS permet de configurer les modules IPQoS. Chaque instruction d'action contient un jeu de *classes*, de *filtres* ou de *paramètres* à traiter par le module appelé dans l'instruction d'action.

Pour connaître la syntaxe complète du fichier de configuration IPQoS, reportez-vous à l'Exemple 37–3 et à la page de manuel `ipqosconf`(1M).

Configuration de la topologie d'un exemple IPQoS

Les tâches décrites dans ce chapitre indiquent comment créer un fichier de configuration IPQoS pour trois systèmes compatibles IPQoS. Ces systèmes font partie de la topologie du réseau de l'entreprise BigISP, présentée sur la Figure 33–4.

- `Goldweb` – Serveur Web hébergeant les sites Web de clients ayant acquis des accords de niveau de service de type premium
- `Userweb` – Serveur Web moins puissant hébergeant des sites web personnels pour des usagers domestiques qui ont souscrit à des accords de niveau de service « au mieux »
- `BigAPPS` – Serveur d'application délivrant des messages électroniques, des actualités sur le réseau et un service FTP aux clients des services Premium et au mieux

Ces trois fichiers de configuration illustrent les configurations IPQoS les plus courantes. Il est possible d'utiliser les fichiers d'exemple présentés à la section suivante comme modèle de votre propre implémentation IPQoS.

Création de fichiers de configuration IPQoS pour les serveurs Web

Cette section présente le fichier de configuration IPQoS et la procédure destinée à créer un fichier de configuration pour un serveur Web de type premium. Cette section explique comment configurer un niveau de service complètement différent dans un autre fichier de configuration pour un serveur hébergeant des sites Web personnels. Les deux serveurs appartiennent au réseau illustré à la Figure 33–4.

Le fichier de configuration suivant définit les activités IPQoS du serveur `Goldweb`. Ce serveur héberge le site Web de Goldco, l'entreprise qui a acquis un accord de niveau de service de niveau premium.

EXEMPLE 34–1 Fichier de configuration IPQoS pour un serveur Web premium

```
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
    }
```

EXEMPLE 34–1 Fichier de configuration IPQoS pour un serveur Web premium *(Suite)*

```
}
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
    }
}
```

Le fichier de configuration suivant définit les activités IPQoS sur `Userweb`. Ce serveur héberge des sites Web pour les accords de niveau de service à bas prix ou *au mieux*. Ce niveau de service garantit le meilleur service susceptible d'être fourni après la gestion, par le système IPQoS, du trafic correspondant aux clients bénéficiant d'accords de niveau de service plus onéreux.

EXEMPLE 34–2 Exemple de configuration pour un serveur Web « au mieux »

```
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
```

EXEMPLE 34–2 Exemple de configuration pour un serveur Web « au mieux » *(Suite)*

```
        dscp_map{0-63:12}
        next_action continue
    }
}
```

Création du fichier de configuration IPQoS et définition des classes de trafic

Vous créez le fichier de configuration IPQoS initial dans le répertoire que vous jugez le plus facile à gérer. Les tâches ce chapitre font appel au répertoire `/var/ipqos` pour enregistrer les fichiers de configuration IPQoS. La procédure suivante génère le segment initial du fichier de configuration IPQoS présenté dans l'Exemple 34–1.

Remarque – Lors de la création du fichier de configuration IPQoS, veillez à commencer et à terminer chaque instruction `action` et chaque clause par des accolades ({ }). Pour plus de détails sur l'utilisation des accolades, reportez-vous à l'Exemple 34–1.

---

1 **Connectez-vous au serveur Web premium et générez un nouveau fichier de configuration IPQoS suivi de l'extension `.qos`.**

La première ligne non commentée de chaque fichier de configuration IPQoS doit commencer par le numéro de version `fmt_version 1.0`.

2 **Faites suivre le paramètre d'ouverture par l'instruction `action` initiale chargée de configurer le classificateur d'IP générique `ipgpc`.**

L'action initiale marque le début de l'arborescence des instructions `action` composant le fichier de configuration IPQoS. Par exemple, le fichier `/var/ipqos/Goldweb.qos` commence par l'instruction initiale `action` destinée à appeler le classificateur `ipgpc`.

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
```

`fmt_version 1.0`	Marque le début du fichier de configuration IPQoS.
`action {`	Marque le début de l'instruction d'action.
`module ipgpc`	Configure le classificateur `ipgpc` en tant qu'action initiale du fichier de configuration.
`name ipgpc.classify`	Définit le nom de l'instruction `action` du classificateur qui doit toujours correspondre à `ipgpc.classify`.

Pour plus d'informations sur les détails de la syntaxe des instructions `action`, reportez-vous à la section "Instruction `action`" à la page 899 et à la page de manuel `ipqosconf`(1M).

3 Ajoute une clause `params` au paramètre de statistiques `global_stats`.

```
params {
          global_stats TRUE
   }
```

Le paramètre `global_stats TRUE` dans l'instruction `ipgpc.classify` permet de collecter les statistiques liées à cette action. `global_stats TRUE` permet de recueillir des statistiques par classe dès qu'une définition de clause de classe a la valeur `enable_stats TRUE`.

L'activation des statistiques a un effet sur les performances. Il est possible de recueillir des statistiques sur un nouveau fichier de configuration IPQoS pour vérifier qu'IPQoS fonctionne correctement. Par la suite, vous pouvez désactiver la collecte de statistiques en attribuant à l'argument `global_stats` la valeur `FALSE`.

Les statistiques générales ne représentent qu'un seul type de paramètre que vous pouez définir dans une clause `params`. Pour plus d'informations sur la syntaxe et sur d'autres détails relatifs aux clauses `params`, reportez-vous à la section "Clause `params`" à la page 902 et à la page de manuel `ipqosconf(1M)`.

4 Définissez une classe destinée à identifier le trafic lié au serveur premium.

```
class {
        name goldweb
        next_action markAF11
        enable_stats FALSE
    }
```

Cette instruction appelée une *clause de classe*. Le contenu de la clause `class` est le suivant.

name goldweb	Crée la classe `goldweb` pour identifier le trafic rattaché au serveur `Goldweb`.
next_action markAF11	Donne l'instruction au module `ipgpc` de transmettre les paquets de la classe `goldweb` à l'instruction d'action `markAF1.` Cette instruction `markAF11` appelle le marqueur `dscpmk`.
enable_stats FALSE	Active le recueil de statistiques pour la classe `goldweb.` Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques de cette classe ne sont pas recueillies.

Pour des informations détaillées sur la syntaxe de la clause `class`, reportez-vous à la section "Clause `class`" à la page 901 et à la page de manuel `ipqosconf`(1M).

5 Définissez une classe identifiant une application devant bénéficier de la priorité de transmission la plus haute.

```
class {
        name video
```

```
        next_action markEF
        enable_stats FALSE
    }
```

`name video`	Crée la classe `vidéo` destinée à identifier le trafic du flux vidéo sortant du serveur `Goldweb`.
`next_action markEF`	Donne l'instruction au module `ipgpc` de transmettre les paquets de la classe `video` à l'instruction `markEF` après traitement par `ipgpc`. L'instruction `markEF` appelle le marqueur `dscpmk`.
`enable_stats FALSE`	Active le recueil de statistiques pour la classe `video`. Néanmoins, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, la collecte de statistiques n'est pas activée pour la classe.

Voir aussi

- Pour définir les filtres de la classe que vous venez de créer, reportez-vous à la section "Définition des filtres dans le fichier de configuration IPQoS" à la page 850.
- Pour créer une clause de classe supplémentaire pour le fichier de configuration, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.

▼ Définition des filtres dans le fichier de configuration IPQoS

La procédure suivante précise comment définir les filtres d'une classe dans le fichier de configuration IPQoS.

Avant de commencer

La procédure suppose que vous ayez déjà lancé la création du fichier et défini des classes. Les étapes poursuivent la génération du fichier `/var/ipqos/Goldweb.qos` créé à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.

Remarque – Lors de la création du fichier de configuration IPQoS, veillez à commencer et à terminer chaque clause `class` et chaque clause `filter` par des accolades ({ }). Pour plus de détails sur l'utilisation des accolades, reportez-vous à l'Exemple 34–1.

---

1 Ouvrez le fichier de configuration IPQoS et recherchez la fin de la dernière classe définie.

Par exemple, sur le serveur IPQoS `Goldweb`, vous devez débuter après la clause `class` suivante dans le fichier `/var/ipqos/Goldweb.qos` :

```
class {
        name video
        next_action markEF
```

```
    enable_stats FALSE
}
```

2 Définissez une clause `filter` afin de sélectionner le trafic sortant du système IPQoS.

```
filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class goldweb
}
```

`name webout`	Attribue le nom `webout` au filtre.
`sport 80`	Sélectionne le trafic par le port source 80, port réservé au trafic (Web) HTTP.
`direction LOCAL_OUT`	Affine la sélection du trafic sortant provenant du système local.
`class goldweb`	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `goldweb`.

Pour des informations sur la syntaxe et d'autres détails sur la clause `filter` figurant dans le fichier de configuration IPQoS, reportez-vous à la section "Clause `filter`" à la page 901.

3 Définissez une clause `filter` pour sélectionner le trafic de flux vidéo dans le système IPQoS.

```
filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
}
```

name videoout	Attribue le nom `videoout` au filtre.
`sport videosrv`	Sélectionne le trafic par le port source `videosrv`, port précédemment défini pour les applications de flux vidéo du système.
`direction LOCAL_OUT`	Affine la sélection du trafic sortant provenant du système local.
`class video`	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `video`.

Voir aussi

- Pour définir les comportements au niveau des modules de marquage, reportez-vous à la section "Définition de la transmission du trafic dans le fichier de configuration IPQoS" à la page 852.
- Pour définir les paramètres de contrôle des flux au niveau des modules de mesure, reportez-vous à la section "Configuration du contrôle de flux dans le fichier de configuration IPQoS " à la page 866.
- Pour activer le fichier de configuration IPQoS, reportez-vous à la section "Application d'une nouvelle configuration aux modules de noyau IPQoS" à la page 872.

- Pour définir des filtres supplémentaires, reportez-vous à la section "Définition des filtres dans le fichier de configuration IPQoS" à la page 850.
- Pour créer des classes pour les flux de trafic provenant d'applications, reportez-vous à la section "Configuration d'un fichier de configuration IPQoS pour un serveur d'application" à la page 861.

▼ Définition de la transmission du trafic dans le fichier de configuration IPQoS

La procédure suivante indique comment définir la transmission du trafic en ajoutant des comportements par pas à une classe dans le fichier de configuration IPQoS.

Avant de commencer

Cette procédure suppose que vous disposiez d'un fichier de configuration IPSQoS assorti de classes et de filtres déjà définis. Les étapes poursuivent la génération du fichier `/var/ipqos/Goldweb.qos` de l'Exemple 34–1.

Remarque – La procédure montre comment configurer la transmission du trafic à l'aide du module de marquage `dscpmk`. Pour plus d'informations sur la transmission du trafic sur des systèmes VLAN à l'aide du marqueur `dlclosmk`, reportez-vous à la section "Utilisation du marqueur `dlcosmk` avec les périphériques VLAN" à la page 893.

---

1 Ouvrez le fichier de configuration IPQoS et recherchez la fin du dernier filtre défini.

Par exemple, sur le serveur IPQoS `Goldweb`, vous devez débuter après la clause `filtre` suivante dans le fichier `/var/ipqos/Goldweb.qos` :

```
filter {
        name videoout
        sport videosrv
        direction LOCAL_OUT
        class video
    }
}
```

La clause `filter` se trouve à la fin de l'instruction `action` du classificateur `ipgpc`. Par conséquent, vous devez insérer deux accolades : la première signale la fin du filtre et la deuxième la fin de l'instruction `action`.

2 Appelez le marqueur à l'aide de l'instruction `action` suivante.

```
action {
    module dscpmk
    name markAF11
```

module dscpmk Sollicite le module de marquage `dscpmk`.

name markAF11 Attribut le nom `markAF11` à l'instruction `action`.

La classe précédemment définie `goldweb` inclut une instruction `next_action` `markAF11`. Cette instruction envoie les flux de trafic vers l'instruction d'action `markAF11` à l'issue du traitement par le classificateur.

3 Définit les actions que le marqueur doit appliquer au flux de trafic.

```
    params {
        global_stats FALSE
        dscp_map{0-63:10}
        next_action continue
    }
}
```

global_stats FALSE Active la collecte de statistiques pour l'instruction `action` `markAF11` du marqueur. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques ne sont pas recueillies.

dscp_map{0–63:10} Attribue un DSCP égal à `10` aux en-têtes de paquets de la classe de trafic `goldweb` actuellement traitée par le marqueur.

next_action continue Indique qu'aucun traitement supplémentaire n'est requis sur les paquets de la classe de trafic `goldweb` et que ces paquets peuvent revenir dans le flux réseau.

Un DSCP `10` donne pour instruction au marqueur d'attribuer la valeur décimale 10 (binaire 001010) à toutes les entrées de la structure `dscp`. Ce point de code signale que les paquets de la classe de trafic `goldweb` sont soumis au comportement AF11. AF11 garantit à tous les paquets de DSCP `10` un service haute priorité avec un taux de perte faible. Ainsi, le trafic sortant des client premium sur `Goldweb` bénéficie de la priorité la plus haute disponible pour le PHB Assured Forwarding (AF). Pour consulter le tableau des DSCP possibles pour AF, reportez-vous au Tableau 37–2.

4 Lancez une autre instruction `action` du marqueur.

```
action {
    module dscpmk
    name markEF
```

module dscpmk Sollicite le module de marquage `dscpmk`.

`name markEF` Attribue le nom `markEF` à l'instruction `action`.

5 Définissez les actions que le marqueur doit appliquer au flux de trafic.

```
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

`global_stats TRUE`	Active la collecte des statistiques sur une classe `video`, chargée de sélectionner les paquets de flux vidéo.
`dscp_map{0–63:46}`	Attribue un DSCP égal à `46` aux en-têtes de paquets de la classe de trafic `video` actuellement traitée par le marqueur.
`next_action acct`	Donne l'instruction au module `dscpmk` de transmettre les paquets de la classe `video` à l'instruction `action acct` après traitement par `dscpmk`. L'instruction `acct action` appelle le module `flowacct`.

Le DSCP `46` demande au module `dscpmk` d'attribuer la valeur décimale 46 (binaire 101110) à toutes les entrées de structure `dscp`, dans le champ DS. Ce point de code signale que les paquets de la classe de trafic `video` sont soumis au comportement EF.

Remarque – Le point de code recommandé est 46 (binaire 101110). D'autres DSCP assignent des PHB AF à un paquet.

Le PHB EF garantit aux paquets de DSCP `46` un traitement prioritaire par les systèmes compatibles IPQoS et Diffserv. Définir des flux pour les applications nécessite un service de priorité élevée conduisant logiquement à l'attribution de PHB de type EF dans la stratégie QoS. Pour plus de détails sur le PHB EF, reportez-vous à la section "PHB Expedited Forwarding (EF) (ou traitement accéléré)" à la page 892.

6 Ajoutez les DSCP que vous venez de créer dans les fichiers appropriés sur le routeur Diffserv.

Pour plus d'informations, reportez-vous à la section "Configuration d'un routeur dans un réseau compatible IPQoS " à la page 869.

Voir aussi

- Pour lancer la collecte de statistiques de comptabilisation des flux de trafic, reportez-vous à la section "Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS" à la page 855.
- Pour définir les comportements au niveau des modules de marquage, reportez-vous à la section "Définition de la transmission du trafic dans le fichier de configuration IPQoS" à la page 852.
- Pour définir les paramètres de contrôle des flux au niveau des modules de mesure, reportez-vous à la section "Configuration du contrôle de flux dans le fichier de configuration IPQoS " à la page 866.
- Pour activer le fichier de configuration IPQoS, reportez-vous à la section "Application d'une nouvelle configuration aux modules de noyau IPQoS" à la page 872.
- Pour définir des filtres supplémentaires, reportez-vous à la section "Définition des filtres dans le fichier de configuration IPQoS" à la page 850.

- Pour créer des classes pour les flux de trafic provenant d'applications, reportez-vous à la section "Configuration d'un fichier de configuration IPQoS pour un serveur d'application" à la page 861.

Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS

La procédure suivante indique la manière d'activer la comptabilisation pour une classe de trafic dans le fichier de configuration IPQoS. La procédure précise comment définir la comptabilisation des flux pour la classe `video`, présentée à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848. Cette classe sélectionne le trafic vidéo qui doit être facturé au client premium au titre de l'accord de niveau de service contracté.

Avant de commencer La procédure suppose que vous possédiez un fichier de configuration IPQoS comportant des classes, des filtres, des actions de mesure, le cas échéant, et d'éventuelles actions de marquage. Les étapes poursuivent la génération du fichier `/var/ipqos/Goldweb.qos` de l'Exemple 34–1.

1 Ouvrez le fichier de configuration IPQoS et recherchez la fin de la dernière instruction `action` définie.

Par exemple, sur le serveur IPQoS `Goldweb`, vous devez débuter après l'instruction `action markEF` suivante dans le fichier `/var/ipqos/Goldweb.qos`.

```
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

2 Spécifiez une instruction `action` qui déclenche la comptabilisation des flux.

```
action {
    module flowacct
    name acct
```

`module flowacct` Invoque le module de comptabilisation des flux `flowacct`.

`name acct` Attribue le nom `acct` à l'instruction `action`.

3 Définissez une clause `params` pour contrôler la comptabilisation de la classe de trafic.

```
params {
        global_stats TRUE
        timer 10000
```

```
        timeout 10000
        max_limit 2048
        next_action continue
    }
}
```

`global_stats TRUE`	Active la collecte des statistiques sur la classe `video`, chargée de sélectionner les paquets de flux vidéo.
`timer 10000`	Spécifie la durée de l'intervalle, exprimé en millisecondes, lors de l'analyse de la table de flux afin de vérifier les flux dont le délai d'attente a expiré. Pour ce paramètre, l'intervalle correspond à 10 000 millisecondes.
`timeout 10000`	Spécifie la valeur minimale de l'intervalle du délai d'expiration. Un flux arrive à expiration lorsque les paquets du flux n'apparaissent pas à l'issue de l'intervalle défini. Pour ce paramètre, les paquets parviennent à expiration au bout de 10 000 millisecondes.
`max_limit 2048`	Définit le nombre maximum d'enregistrements de flux actifs dans la table de flux pour cette instance d'action.
`next_action continue`	Indique qu'aucun traitement supplémentaire n'est requis sur les paquets de la classe de trafic `video` et que ces paquets peuvent revenir dans le flux réseau.

Le module `flowacct` collecte les informations statistiques sur les flux de paquet d'une classe particulière tant que la valeur `timeout` spécifiée n'est pas atteinte.

Voir aussi

- Pour configurer les comportements par pas sur un routeur, reportez-vous à la section “Configuration d'un routeur dans un réseau compatible IPQoS ” à la page 869.
- Pour activer le fichier de configuration IPQoS, reportez-vous à la section “Application d'une nouvelle configuration aux modules de noyau IPQoS” à la page 872.
- Pour créer des classes pour les flux de trafic provenant d'applications, reportez-vous à la section “Configuration d'un fichier de configuration IPQoS pour un serveur d'application” à la page 861.

▼ Création d'un fichier de configuration IPQoS pour un serveur Web au mieux

Le fichier de configuration IPQoS d'un serveur Web au mieux diffère légèrement du fichier de configuration IPQoS utilisé par un serveur Web de niveau premium. La procédure utilise le fichier de configuration illustré à l'Exemple 34–2.

1 Connectez-vous au serveur Web au mieux.

2 Produisez un nouveau fichier de configuration IPQoS suivi de l'extension `.qos`.

```
fmt_vesion 1.0
action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
   }
```

Le fichier `/var/ipqos/userweb.qos` doit commencer par l'instruction partielle `action` visant à appeler le classificateur `ipgpc`. En outre, l'instruction `action` possède une clause params en mesure d'activer le recueil de statistiques. Pour obtenir une explication de l'instruction `action`, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.

3 Définissez une classe identifiant le trafic lié au serveur Web au mieux.

```
class {
        name userweb
        next_action markAF12
        enable_stats FALSE
    }
```

`name userweb`	Crée une classe appelée `userweb` pour la transmission du trafic Web émanant des utilisateurs.
`next_action markAF1`	Demande au module `ipgpc` de transmettre les paquets de la classe `userweb` à l'instruction `action` `markAF12` après traitement par `ipgpc`. L'instruction `action` `markAF12` appelle le module `dscpmk`.
`enable_stats FALSE`	Active le recueil de statistiques pour la classe `userweb`. Néanmoins, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, la collecte de statistiques ne se produit pas.

Pour obtenir une explication de la tâche de la clause `class`, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.

4 Définissez une clause `filter` pour sélectionner les flux de trafic pour la classe `userweb`.

```
   filter {
       name webout
       sport 80
       direction LOCAL_OUT
       class userweb
   }
}
```

`name webout`	Attribue le nom `webout` au filtre.
`sport 80`	Sélectionne le trafic par le port source 80, port réservé au trafic (Web) HTTP.
`direction LOCAL_OUT`	Affine la sélection du trafic sortant provenant du système local.

class userweb — Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `userweb`.

Pour obtenir une explication de la tâche liée à la clause `filter`, reportez-vous à la section "Définition des filtres dans le fichier de configuration IPQoS" à la page 850.

5 Commencez l'instruction `action` en appelant le marqueur `dscpmk`.

```
action {
    module dscpmk
    name markAF12
```

`module dscpmk` — Sollicite le module de marquage `dscpmk`.

`name markAF12` — Attribue le nom `markAF12` à l'instruction `action`.

La classe précédemment définie `userweb` inclut une instruction `next_action` `markAF12.` Cette instruction envoie les flux de trafic vers l'instruction `action` `markAF12` à l'issue du traitement par le classificateur.

6 Définissez les paramètres pour le marqueur à utiliser pour traitement du flux de trafic.

```
    params {
        global_stats FALSE
        dscp_map{0-63:12}
        next_action continue
    }
}
```

`global_stats FALSE` — Active la collecte de statistiques pour l'instruction `action` `markAF12` du marqueur. Néanmoins, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, la collecte de statistiques n'a pas lieu.

`dscp_map{0–63:12}` — Attribue un DSCP égal à `12` aux en-têtes de paquets de la classe de trafic `userweb` actuellement traitée par le marqueur.

next_action continue — Indique qu'aucun traitement supplémentaire n'est requis pour les paquets de la classe de trafic `userweb` et que ces paquets peuvent revenir dans le flux réseau.

Un DSCP `12` donne pour instruction au marqueur d'attribuer la valeur décimale 12 (binaire 001100) à toutes les entrées de la structure `dscp`. Ce point de code signale que les paquets de la classe de trafic `userweb` sont soumis au comportement AF12. AF12 garantit à tous les paquets de DSCP `12` un service haute priorité avec un taux de perte moyen.

7 Lorsque vous terminez le fichier de configuration IPQoS, appliquez la configuration.

Voir aussi

- Pour ajouter des classes et d'autres configurations aux flux de trafic provenant d'applications, reportez-vous à la section "Configuration d'un fichier de configuration IPQoS pour un serveur d'application" à la page 861.

- Pour configurer les comportements par pas sur un routeur, reportez-vous à la section “Configuration d'un routeur dans un réseau compatible IPQoS ” à la page 869.
- Pour activer le fichier de configuration IPQoS, reportez-vous à la section “Application d'une nouvelle configuration aux modules de noyau IPQoS” à la page 872.

Création d'un fichier de configuration pour un serveur d'application

Cette section décrit comment créer un fichier de configuration pour un serveur d'application délivrant des applications importantes aux clients. La procédure recourt au serveur `BigAPPS` illustré à la Figure 33–4.

Le fichier de configuration suivant définit les activités IPQoS du serveur `BigAPPS`. Ce serveur héberge, à l'usage des clients, des données FTP, des messages électroniques (SMTP) ainsi que des informations sur le réseau (NNTP).

EXEMPLE 34–3 Exemple de fichier de configuration pour un serveur d'application

```
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 {
```

EXEMPLE 34–3 Exemple de fichier de configuration pour un serveur d'application *(Suite)*

```
        name ftpout
        sport ftp
        class ftp
    }
   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
```

EXEMPLE 34–3 Exemple de fichier de configuration pour un serveur d'application *(Suite)*

```
    }
}
```

Configuration d'un fichier de configuration IPQoS pour un serveur d'application

1 Connectez-vous au serveur IPQoS et générez un nouveau fichier de configuration IPQoS suivi de l'extension `.qos`.

Par exemple, créez le fichier `/var/ipqos/BigAPPS.qos` pour le serveur d'application. Commencez par les phrases suivantes pour lancer l'instruction `action` visant à appeler le classificateur `ipgpc` :

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
```

Pour obtenir une explication de l'instruction `action` d'ouverture, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.

2 Créez des classes pour sélectionner le trafic de trois applications situées sur le serveur BigAPPS.

Ajoutez les définitions de classe après l'instruction `action` de départ.

```
    class {
        name smtp
        enable_stats FALSE
        next_action markAF13
    }
    class {
        name news
        next_action markAF21
    }
    class {
        name ftp
        enable_stats TRUE
        next_action meterftp
    }
```

`name smtp` Crée une classe appelée `smtp` qui intègre les flux de trafic de messagerie électronique à gérer par l'application SMTP.

`enable_stats FALSE`	Active le recueil de statistiques pour la classe `smtp`. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques de cette classe ne sont pas recueillies.
`next_action markAF13`	Demande au module `ipgpc` de transmettre les paquets de la classe `smtp` à l'instruction `action` `markAF13` après traitement par `ipgpc`.
`name news`	Crée une classe appelée `news` qui intègre les flux d'informations sur le réseau à gérer par l'application NNTP.
`next_action markAF21`	Donne l'instruction au module `ipgpc` de transmettre les paquets de la classe `news` à l'instruction `markAF21` après traitement par `ipgpc`.
`name ftp`	Crée une classe appelée `ftp` qui traite le trafic sortant géré par l'application FTP.
`enable_stats TRUE`	Active le recueil de statistiques pour la classe `ftp`.
`next_action meterftp`	Demande au module `ipgpc` de transmettre les paquets de la classe `ftp` à l'instruction `action` `meterftp` après traitement par `ipgpc`.

Pour plus d'informations sur la définition des classes, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.

3 Définissez des clauses `filter` afin de sélectionner le trafic des classes définies à l'étape 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
    }
}
```

`name smtpout`	Attribue le nom `smtpout` au filtre.
`sport smtp`	Sélectionne le trafic transitant par le port source 25 représentant le port consacré à l'application `sendmail` (SMTP).

`class smtp`	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `smtp`.
`name newsout`	Attribue le nom `newsout` au filtre.
`sport nntp`	Sélectionne le trafic transitant par le port source `nntp`, couramment utilisé pour l'application d'informations réseau (NNTP).
`class news`	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `news`.
`name ftpout`	Attribue le nom `ftpout` au filtre.
`sport ftp`	Sélectionne les données de contrôle passant par le port source 21, port réservé au trafic FTP.
`name ftpdata`	Attribue le nom `ftpdata` au filtre.
`sport ftp-data`	Sélectionne les données de contrôle passant par le port source 21, port réservé aux données de trafic FTP.
`class ftp`	Identifie la classe à laquelle les filtres `ftpout` et `ftpdata` appartiennent. Dans cet exemple, il s'agit de `ftp`.

Voir aussi

- Pour définir des filtres, reportez-vous à la section "Définition des filtres dans le fichier de configuration IPQoS" à la page 850.
- Pour définir les comportements pour le trafic de l'application, reportez-vous à la section "Configuration de la transmission du trafic d'une application dans le fichier de Configuration IPQoS" à la page 863.
- Pour configurer le contrôle des flux à l'aide des modules de mesure, reportez-vous à la section "Configuration du contrôle de flux dans le fichier de configuration IPQoS " à la page 866.
- Pour configurer la comptabilisation des flux, reportez-vous à la section "Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS" à la page 855.

▼ Configuration de la transmission du trafic d'une application dans le fichier de Configuration IPQoS

La procédure suivante indique comment configurer le transfert du trafic d'une application. Dans la procédure, vous définissez les comportements par pas pour les classes de trafic de l'application qui sont susceptibles d'avoir des niveaux de priorité inférieurs à ceux d'autres flux de trafic sur un réseau. Les étapes poursuivent la génération du fichier `/var/ipqos/BigAPPS.qos` de l'Exemple 34–3.

Avant de commencer Cette procédure suppose que vous disposiez d'un fichier de configuration IPSQoS assorti de classes et de filtres déjà définis pour les applications à marquer.

1 Ouvrez le fichier de configuration IPQoS créé pour le serveur d'application et localisez la fin de la dernière clause `filter`.

Dans le fichier `/var/ipqos/BigAPPS.qos`, le filtre final est le suivant :

```
 filter {
        name ftpdata
        sport ftp-data
        class ftp
    }
}
```

2 Appelez le marqueur de la manière suivante :

```
action {
    module dscpmk
    name markAF13
```

`module dscpmk` Sollicite le module de marquage `dscpmk`.

`name markAF13` Attribue le nom `markAF13` à l'instruction `action`.

3 Définissez le comportement par pas à signaler au niveau des flux de trafic de courriers électroniques.

```
    params {
        global_stats FALSE
        dscp_map{0-63:14}
        next_action continue
    }
}
```

`global_stats FALSE` Active la collecte de statistiques pour l'instruction `action` `markAF13` du marqueur. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques ne sont pas recueillies.

`dscp_map{0–63:14}` Attribue un DSCP égal à `14` aux en-têtes de paquets de la classe de trafic `smtp` actuellement traitée par le marqueur.

`next_action continue` Indique qu'aucun traitement supplémentaire n'est requis pour les paquets de la classe de trafic `smtp`. Ces paquets peuvent alors revenir dans le flux du réseau.

Un DSCP `14` donne pour instruction au marqueur d'attribuer la valeur décimale 14 (binaire 001110) à toutes les entrées de la structure `dscp`. Le DSCP `14` définit le comportement AF13. Le marqueur signale les paquets de la classe de trafic `smtp` par le DSCP `14` dans le champ DS.

AF13 assigne à l'ensemble des paquets marqués d'un DSCP `14` un niveau de priorité élevé. Cependant, étant donné que AF13 garantit une priorité de classe 1, le routeur garantit une

priorité élevée au trafic sortant des courriers électroniques dans la file d'attente. Pour consulter le tableau de l'ensemble des points de code AF, reportez-vous au Tableau 37–2.

4 Ajoutez une instruction `action` de marqueur pour définir un comportement pour le trafic des informations réseau :

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

`name markAF21` Attribut le nom `markAF21` à l'instruction `action`.

`dscp_map{0–63:18}` Attribue un DSCP égal à `18` aux en-têtes de paquets de la classe de trafic `nntp` actuellement traitée par le marqueur.

Le DSCP `18` donne pour instruction au marqueur d'attribuer la valeur décimale 18 (binaire 010010) à toutes les entrées de la structure `dscp`. Le DSCP `18` définit le comportement AF21. Le marqueur signale les paquets de la classe de trafic `news` par le DSCP `18` dans le champ DS.

AF21 garantit que tous les paquets avec un DSCP égal à `18` se voient attribuer un niveau de perte fable assorti d'une priorité de classe 2. Ainsi, les probabilités de perdre les données de trafic d'informations sur le réseau sont faibles.

Voir aussi

- Pour ajouter des informations de configuration pour les serveurs Web, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.
- Pour configurer le contrôle des flux à l'aide des modules de mesure, reportez-vous à la section "Configuration du contrôle de flux dans le fichier de configuration IPQoS " à la page 866.
- Pour configurer la comptabilisation des flux, reportez-vous à la section "Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS" à la page 855.
- Pour configurer les comportements sur un routeur, reportez-vous à la section "Configuration d'un routeur dans un réseau compatible IPQoS " à la page 869.
- Pour activer le fichier de configuration IPQoS, reportez-vous à la section "Application d'une nouvelle configuration aux modules de noyau IPQoS" à la page 872.

Configuration du contrôle de flux dans le fichier de configuration IPQoS

Pour contrôler le débit selon lequel un flux de trafic est libéré sur le réseau, vous devez définir des paramètres de mesure. Vous pouvez utiliser un des deux modules de mesure, `tokenmt` ou `tswtclmt`, dans le fichier de configuration IPQoS.

La procédure suivante poursuit l'élaboration du fichier de configuration IPQoS pour le serveur d'application de l'Exemple 34–3. Dans la procédure, vous pouvez configurer les actions de mesure, mais aussi les actions de deux modules de marquage appelées par l'instruction `action` du module de mesure.

Avant de commencer Les étapes supposent que vous ayez déjà défini une classe et un filtre pour l'application dont vous voulez contrôler le flux.

1 Ouvrez le fichier de configuration IPQoS créé pour le serveur d'applications.

Dans le fichier `/var/ipqos/BigAPPS.qos`, vous commencez après l'action du marqueur suivante :

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

2 Créez une instruction `action` pour le module de mesure afin de contrôler le trafic d'une classe `ftp`.

```
action {
    module tokenmt
    name meterftp
```

`module tokenmt` Sollicite le module de mesure `tokenmt`.

`name meterftp` Attribut le nom `meterftp` à l'instruction `action`.

3 Ajoutez les paramètres à configurer le débit du module de mesure.

```
params {
       committed_rate 50000000
       committed_burst 50000000
```

`committed_rate 50000000` Assigne une vitesse de transmission de 50 000 000 bps au trafic de la classe `ftp`.

`committed_burst 50000000` Valide une taille de rafale de 50 000 000 bits pour le trafic de la classe `ftp`.

Pour une explication des paramètres `tokenmt`, reportez-vous à la section "Configuration du `tokenmt` en tant que compteur à débit double" à la page 889.

4 Ajoutez des paramètres pour configurer les niveaux de priorité de conformité de trafic :

```
    red_action markAF31
    green_action_name markAF22
    global_stats TRUE
    }
}
```

`red_action_name markAF31` Indique que le flux de trafic de la classe `ftp` dépasse le débit garanti, les paquets sont envoyés vers l'instruction de marquage `action` `markAF31`.

`green_action_name markAF22` Indique que le flux de trafic de la classe `ftp` est conforme au débit garanti, les paquets sont envoyés à l'instruction de l'action `markAF22`.

`global_stats TRUE` Active le recueil de statistiques pour la classe `ftp`.

Pour plus d'informations sur la conformité du trafic, reportez-vous à la section "Module de mesure" à la page 888.

5 Ajoutez une instruction `action` du marqueur pour assigner un comportement par pas aux flux de trafic non conformes d'une classe `ftp`.

```
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
```

`module dscpmk` Sollicite le module de marquage `dscpmk`.

`name markAF31` Attribue le nom `markAF31` à l'instruction `action`.

`global_stats TRUE` Active le recueil de statistiques pour la classe `ftp`.

`dscp_map{0–63:26}` Assigne un DSCP 26 aux en-têtes de paquets de la classe de trafic `ftp` lorsque ce trafic dépasse le taux garanti.

`next_action continue` Indique qu'aucun traitement supplémentaire n'est requis pour les paquets de la classe de trafic `ftp`. Ces paquets peuvent alors revenir dans le flux du réseau.

Un DSCP 26 donne pour instruction au marqueur d'attribuer la valeur décimale 26 (binaire 011010) à toutes les entrées de la structure `dscp`. Le DSCP 26 définit le comportement AF31. Le marqueur signale les paquets de la classe de trafic `ftp` par le DSCP 26 dans le champ DS.

AF31 garantit que tous les paquets avec un DSCP égal à 26 se voient attribuer un niveau de perte faible assorti d'une priorité de classe 3. En d'autres termes, la probabilité de rejeter un trafic FTP non conforme est faible. Pour consulter le tableau de l'ensemble des points de code AF, reportez-vous au Tableau 37–2.

6 Ajoutez une instruction `action` du module de marquage pour assigner un PHB aux flux de trafic `ftp` qui se conforment au débit contractuel.

```
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
```

`name markAF22` Attribut le nom `markAF22` à l'instruction `action`.

`dscp_map{0–63:20}` Assigne un DSCP `20` aux en-têtes de paquets de la classe de trafic `ftp` lorsque le trafic `ftp` dépasse le débit configuré.

Un DSCP égal à 20 donne pour instruction au marqueur d'attribuer la valeur décimale 20 (binaire 010100) à toutes les entrées de la structure `dscp`. Le DSCP `20` définit le comportement AF22. Le marqueur signale les paquets de la classe de trafic `ftp` par le DSCP `20` dans le champ DS.

AF22 garantit que tous les paquets avec un DSCP égal à `20` se voient attribuer un niveau de perte moyen assorti d'une priorité de classe 2. En conséquence, le trafic FTP respectant ces conditions peut compter sur un niveau de priorité moyen parmi les flux libérés simultanément par le système IPQoS. Toutefois, le routeur assigne une plus grande priorité aux classes de trafic dotées d'un niveau de priorité identique de classe 1 ou supérieur. Pour consulter le tableau de l'ensemble des points de code AF, reportez-vous au Tableau 37–2.

7 Insère les DSCP créés pour le serveur d'application dans les fichiers correspondants sur le routeur Diffserv.

Voir aussi

- Pour activer le fichier de configuration IPQoS, reportez-vous à la section "Application d'une nouvelle configuration aux modules de noyau IPQoS" à la page 872.
- Pour ajouter des informations de configuration pour les serveurs Web, reportez-vous à la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.

- Pour configurer la comptabilisation des flux, reportez-vous à la section "Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS" à la page 855.
- Pour configurer les comportements sur un routeur, reportez-vous à la section "Configuration d'un routeur dans un réseau compatible IPQoS " à la page 869.

Fourniture de services différenciés sur un routeur

Pour fournir des services réellement différenciés, vous devez inclure un routeur Diffserv dans la topologie de votre réseau comme décrit dans la section "Stratégies matérielles pour le réseau Diffserv" à la page 822. Les étapes véritables de la configuration Diffserv sur un routeur ainsi que la mise à jour des fichiers du routeur dépassent le cadre de ce guide.

Cette section donne des indications générales sur la procédure de coordination des informations de transmission entre les différents systèmes IPQoS sur le réseau et le routeur Diffserv.

▼ Configuration d'un routeur dans un réseau compatible IPQoS

La procédure suivante prend pour exemple la topologie illustrée à la Figure 33–4.

Avant de commencer Elle suppose que vous ayez déjà configuré les systèmes IPQoS sur votre réseau en effectuant les tâches précédemment décrites dans ce chapitre.

1 Examinez les fichiers de configuration pour tous les systèmes IPQoS de votre réseau.

2 Identifiez chaque point de code utilisé dans les stratégies QoS.

Dressez la liste des points de code ainsi que celle des systèmes et des classes auxquels font référence les points de code. Le tableau suivant indique les zones pour lesquelles vous pouvez avoir fait appel à un même point de code. Cette pratique est autorisée. Cependant, veillez à fournir d'autres critères dans le fichier de configuration IPQoS (un sélecteur de `priorité`, par exemple) pour déterminer la priorité de deux classes marquées de manière identique.

Par exemple, dans le cadre du réseau illustré dans les procédures de ce chapitre, il est possible d'élaborer le tableau de points de codes suivants.

Système	Classe	PHB	Point de code DS
`Goldweb`	`video`	EF	46 (101110)

Système	Classe	PHB	Point de code DS
`Goldweb`	`goldweb`	AF11	10 (001010)
`Userweb`	`webout`	AF12	12 (001100)
`BigAPPS`	`smtp`	AF13	14 (001110)
`BigAPPS`	`news`	AF18	18 (010010)
`BigAPPS`	Trafic `ftp` conforme	AF22	20 (010100)
`BigAPPS`	Trafic `ftp` non conforme	AF31	26 (011010)

3 Ajoutez les points de code provenant des fichiers de configuration IPQoS de votre réseau au fichiers qui conviennent sur le routeur Diffserv.

Les points de code fournis contribuent à configurer le mécanisme d'ordonnancement Diffserv du routeur. Reportez-vous à la documentation du fabricant du routeur ainsi qu'à son site Web pour obtenir des instructions.

◆ ◆ ◆ CHAPITRE 35

Démarrage et maintenance d'IPQoS (tâches)

Ce chapitre inclut les tâches destinées à activer un fichier de configuration IPQoS et à consigner les événements en rapport avec IPQoS. Il aborde les sujets suivants :

Administration d'IPQoS (liste des tâches)

Cette section répertorie l'ensemble des tâches visant à démarrer et à gérer IPQoS sur un système Oracle Solaris. Avant d'utiliser ces tâches, vous devez disposer d'un fichier de configuration IPQoS complet comme décrit dans la section "Définition d'une stratégie QoS dans le fichier de configuration IPQoS (liste des tâches)" à la page 843.

Le tableau suivant répertorie et décrit ces tâches et contient des liens vers les sections expliquant en détails comment effectuer ces tâches.

Tâche	Description	Voir
1. Configurez IPQoS sur un système.	Exécutez la commande `ipqosconf` pour activer le fichier de configuration IPQoS sur un système.	"Application d'une nouvelle configuration aux modules de noyau IPQoS" à la page 872
2. Assurez-vous que les scripts de démarrage Oracle Solaris sont appliqués au fichier de configuration IPQoS débogué après chaque initialisation du système.	Veillez à ce que le fichier de configuration IPQoS soit appliqué chaque fois que le système redémarre.	"Vérification de l'application de la configuration IPQoS après chaque redémarrage" à la page 873.

Tâche	Description	Voir
3. Activez la journalisation de `syslog` pour IPQoS.	Ajoutez une entrée pour activer la journalisation par `syslog` des messages IPQoS.	"Activation de la journalisation des messages IPQoS lors de l'initialisation" à la page 874.
4. Résolvez tout problème éventuel lié à IPQoS.	Vérifiez les messages d'erreur pour dépanner IPQoS.	Reportez-vous aux messages d'erreur figurant dans le Tableau 35–1.

Application d'une configuration IPQoS

Vous activez ou effectuez toute autre opération pour le fichier de configuration IPQoS à l'aide de la commande `ipqosconf`.

▼ Application d'une nouvelle configuration aux modules de noyau IPQoS

Vous exécutez la commande `ipqosconf` pour lire le fichier de configuration IPQoS et pour configurer les modules IPQoS dans le noyau UNIX. La procédure suivante présente le fichier `/var/ipqos/Goldweb.qos`, en guise d'exemple, créé dans la section "Création de fichiers de configuration IPQoS pour les serveurs Web" à la page 846. Pour obtenir des informations détaillées, reportez-vous à la page de manuel `ipqosconf`(1M).

1 Prenez le rôle d'administrateur principal ou connectez-vous en tant que superutilisateur dans le système IPQoS.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Appliquez la nouvelle configuration.

```
# /usr/sbin/ipqosconf -a/var/ipqos/Goldweb.qos
```

La commande `ipqosconf` consigne les informations du fichier de configuration IPQoS spécifié dans les modules IPQoS du noyau Oracle Solaris. Dans cet exemple, les informations du fichier `/var/ipqos/Goldweb.qos` sont appliquées au noyau Oracle Solaris actuel.

Remarque – Lorsque vous appliquez un fichier de configuration IPQoS avec l'option `-a`, les actions dans le fichier sont actives seulement pour la session en cours.

---

3. **Testez et déboguez la nouvelle configuration IPQoS.**

   Les utilitaires UNIX permettent d'effectuer le suivi du comportement d'IPQoS et de recueillir des statistiques sur votre mise en œuvre IPQoS. Ces informations vous aident à déterminer si la configuration fonctionne comme prévu.

Voir aussi

- Pour étudier les statistiques concernant le fonctionnement des modules IPQoS, reportez-vous à la section "Collecte des informations statistiques" à la page 882.
- Pour consigner les messages `ipqosconf`, reportez-vous à la section "Activation de la journalisation des messages IPQoS `syslog` " à la page 874.
- Pour vous assurer que la configuration IPQoS est appliquée après chaque initialisation, reportez-vous à la section "Vérification de l'application de la configuration IPQoS après chaque redémarrage" à la page 873.

▼ Vérification de l'application de la configuration IPQoS après chaque redémarrage

Vous devez rendre explicite la persistance de la configuration IPQoS d'un redémarrage à l'autre. Sinon, la configuration actuelle n'a d'effet que jusqu'au redémarrage système suivant. Lorsque IPQoS fonctionne convenablement sur un système, procédez comme suit pour définir la configuration de manière permanente.

1. **Prenez le rôle d'administrateur principal ou connectez-vous en tant que superutilisateur dans le système IPQoS.**

   Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2. **Testez l'existence d'une configuration IPQoS dans des modules de noyau.**

   ```
   # ipqosconf -l
   ```

   Si une configuration existe déjà, `ipqosconf` affiche la configuration à l'écran. En l'absence de sortie, appliquez la configuration comme indiqué à la section "Application d'une nouvelle configuration aux modules de noyau IPQoS" à la page 872.

3. **Assurez-vous que la configuration IPQoS existante est appliquée chaque fois que le système IPQoS redémarre.**

   ```
   # /usr/sbin/ipqosconf -c
   ```

   L'option `-c` permet d'ajouter la configuration IPQoS actuelle dans le fichier de configuration `/etc/inet/ipqosinit.conf` lors de l'initialisation.

Activation de la journalisation des messages IPQoS syslog

Pour enregistrer des messages IPQoS lors de l'initialisation, vous devez modifier le fichier /etc/syslog.conf comme indiqué dans la procédure suivante.

▼ Activation de la journalisation des messages IPQoS lors de l'initialisation

1 **Prenez le rôle d'administrateur principal ou connectez-vous en tant que superutilisateur dans le système IPQoS.**

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 **Ouvrez le fichier /etc/syslog.conf.**

3 **Ajoutez le texte suivant comme ultime entrée du fichier.**

```
user.info                       /var/adm/messages
```

Insérez des tabulations plutôt que des espaces entre les colonnes.

L'entrée permet de journaliser tous les messages générés par IPQoS dans le fichier /var/adm/messages, lors de l'initialisation.

4 **Réinitialisez le système pour appliquer les messages.**

Exemple 35–1 Sortie d'IPQoS du fichier /var/adm/messages

Lorsque vous affichez /var/adm/messages après le redémarrage système, la sortie peut contenir des messages de journalisation IPQoS similaires aux suivants.

```
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.
```

Des messages d'erreur IPQoS, identiques aux suivants, peuvent éventuellement apparaître dans le fichier /var/adm/messages du système 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.
```

Pour obtenir la description de ces messages d'erreur, reportez-vous au Tableau 35–1.

Dépannage à l'aide des messages d'erreur IPQoS

Cette section contient le tableau des messages d'erreur qui sont générés par IPQoS ainsi que leurs solutions possibles.

TABLEAU 35–1 Messages d'erreur IPQoS

Message d'erreur	Description	Solution
`Undefined action in parameter` *nom du paramètre* `action` *nom de l'action*	Dans le fichier de configuration IPQoS, le nom de l'action spécifiée pour *parameter-name* n'existe pas dans le fichier de configuration.	Créez l'action. Ou faites appel à une action différente existante dans le paramètre.
`action` *nom de l'action* `involved in cycle`	Dans le fichier de configuration IPQoS, *nom de l'action* fait partie du cycle d'actions, ce qui n'est pas autorisé par IPQoS.	Déterminez le cycle d'actions. Supprimez ensuite une des références cycliques du fichier de configuration IPQoS.
`action` *nom de l'action* `isn't referenced by any other actions`	Une définition d'action non `ipgpc` n'est pas référencée par d'autres actions définies dans le fichier de configuration IPQoS, ce qui n'est pas autorisé par IPQoS.	Supprimez l'action non référencée. Vous pouvez aussi faire en sorte qu'une action fasse référence à l'action actuellement sans référence.
`Missing/Invalid config file fmt_version`	Le format du fichier du configuration n'est pas spécifié en tant que première entrée du fichier, ce qui est requis par IPQoS.	Ajoutez la version du format comme indiqué dans la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.
`Unsupported config file format version`	La version de format spécifiée dans le fichier de configuration n'est pas prise en charge par IPQoS.	Remplacez la version du format par `fmt_version 1.0`, nécessaire pour exécuter Solaris 9 9/02 et les versions ultérieures d'IPQoS.
`No ipgpc action defined.`	Vous n'avez pas défini une action pour la classification `ipgpc` dans le fichier de configuration alors que cela est une exigence d'IPQoS.	Définissez une action pour `ipgpc` comme indiqué dans la section "Création du fichier de configuration IPQoS et définition des classes de trafic" à la page 848.
`Can't commit a null configuration`	Lorsque vous avez exécuté `ipqosconf -c` pour valider une configuration, cette configuration était vide. Or, ce n'est pas autorisé par IPQoS.	Assurez-vous d'avoir appliqué un fichier de configuration avant de valider une configuration. Pour obtenir plus d'instructions, reportez-vous à la section "Application d'une nouvelle configuration aux modules de noyau IPQoS" à la page 872.
`Invalid CIDR mask on line` *numéro de la ligne*	Dans le fichier de configuration, vous avez utilisé un masque CIDR en tant que partie de l'adresse IP qui se trouve hors de la plage des adresses IP valides.	Changez la valeur du masque pour qu'elle soit comprise dans la page 1–32 pour IPv4 et 1–128 pour IPv6.

TABLEAU 35–1 Messages d'erreur IPQoS *(Suite)*

Message d'erreur	Description	Solution
`Address masks aren't allowed for host names line` *numéro de la ligne*	Dans le fichier de configuration, vous avez défini un masque CIDR en guise de nom d'hôte ce qui n'est pas autorisé dans IPQoS.	Supprimez le masque ou remplacez le nom d'hôte par une adresse IP.
`Invalid module name line` *numéro de la ligne*	Le nom du module spécifié dans une instruction d'action au sein du fichier de configuration est incorrect.	Vérifiez l'orthographe du nom de module. Pour obtenir la liste des modules IPQoS, reportez-vous au Tableau 37–5.
`ipgpc action has incorrect name line` *numéro de la ligne*	Le nom assigné à l'action `ipgpc` dans le fichier de configuration ne correspond pas à l'action `ipgpc.classify` demandée.	Renommez l'action `ipgpc.classify`.
`Second parameter clause not supported line` *numéro de la ligne*	Dans le fichier de configuration, vous avez spécifié deux clauses de paramètres pour une seule action ce que IPQoS n'autorise pas.	Combinez tous les paramètres faisant référence à l'action en une seule clause de paramètres.
`Duplicate named action`	Dans le fichier de configuration, vous avez attribué le même nom à deux actions.	Renommez ou supprimez une des actions.
`Duplicate named filter/class in action` *nom de l'action*	Vous avez donné le même nom à deux filtres ou à deux classes de la même action, ce qui n'est pas autorisé dans le fichier de configuration IPQoS.	Renommez ou supprimez une des classes.
`Undefined class in filter` *nom du filtre* `in action` *nom de l'action*	Dans le fichier de configuration, le filtre fait référence à une classe qui n'est pas définie dans l'action.	Créez la classe ou remplacez la référence de filtre par une classe déjà existante.
`Undefined action in class` *nom de la classe* `action` *nom de l'action*	Le classe fait référence à une action non définie dans le fichier de configuration.	Créez l'action ou remplacez la référence par une action déjà existante.
`Invalid parameters for action` *nom de l'action*	Dans le fichier de configuration, un des paramètres est incorrect.	Pour le module appelé par l'action nommée, reportez-vous à l'entrée du module figurant dans la section "Architecture IPQoS et modèle Diffserv" à la page 885. Vous avez également la possibilité de consulter la page du manuel `ipqosconf`(1M).
`Mandatory parameter missing for action` *nom de l'action*	Vous n'avez pas défini un paramètre requis pour une action dans le fichier de configuration.	Pour le module appelé par l'action nommée, reportez-vous à l'entrée du module figurant dans la section "Architecture IPQoS et modèle Diffserv" à la page 885. Vous avez également la possibilité de consulter la page du manuel `ipqosconf`(1M).

TABLEAU 35–1 Messages d'erreur IPQoS *(Suite)*

Message d'erreur	Description	Solution
`Max number of classes reached in ipgpc`	Vous avez spécifié plus de classes qu'il n'est permis de le faire dans l'action `ipgpc` du fichier de configuration IPQoS. Le nombre maximum est 10007.	Vérifiez le fichier de configuration et supprimez les classes inutiles. Une autre solution consiste à atteindre le nombre maximum de classes en ajoutant l'entrée `ipgpc_max_classes` *nom de la classe* au fichier `/etc/system`.
`Max number of filters reached in action ipgpc`	Vous avez spécifié plus de filtres qu'il n'est permis de le faire dans l'action `ipgpc` du fichier de configuration IPQoS. Le nombre maximum est 10007.	Vérifiez le fichier de configuration et supprimez les filtres inutiles. Vous pouvez aussi élever le nombre maximum de filtres en ajoutant l'entrée `ipgpc_max_filters` *nombre de filtres* au fichier `/etc/system`.
`Invalid/missing parameters for filter` *nom du filtre* `in action ipgpc`	Dans le fichier de configuration, le filtre *nom du filtre* comporte un paramètre non valide ou un paramètre est manquant.	Reportez-vous à la page de manuel `ipqosconf`(1M) pour obtenir la liste des paramètres corrects.
`Name not allowed to start with '!', line` *numéro de la ligne*	Un nom d'action, de filtre ou de classe doit commencer par un point d'exclamation mark (!), ce qui n'est pas autorisé dans le fichier IPQoS.	Supprimez le point d'exclamation ou changez le nom de l'action, de la classe ou du filtre.
`Name exceeds the maximum name length line` *numéro de la ligne*	Vous avez donné un nom à une action, une classe ou un filtre dans le fichier de configuration qui dépasse la longueur maximum de 23 caractères.	Choisisse un nom d'action, de classe ou de filtre plus court.
`Array declaration line` *numéro de la ligne* `is invalid`	Dans le fichier de configuration, la déclaration de tableau pour le paramètre sur la ligne *numéro de la ligne* n'est pas valide.	Pour définir correctement la syntaxe de déclaration de tableau appelée par l'instruction `action` avec le tableau non valide, reportez-vous à la section "Architecture IPQoS et modèle Diffserv" à la page 885. Vous pouvez aussi consulter la page du manuel `ipqosconf`(1M).
`Quoted string exceeds line,` *numéro de la ligne*	La chaîne n'inclut pas les guillemets de fermeture sur la même ligne, ce qui est obligatoire dans le fichier de configuration.	Assurez-vous que la chaîne comprise entre les guillemets commence et finit sur la même ligne dans le fichier de configuration.
`Invalid value, line` *numéro de la ligne*	La valeur attribuée à la ligne *numéro de la ligne* du fichier de configuration n'est pas prise en charge par le paramètre.	Pour connaître les valeurs autorisées pour le module appelé par l'instruction `action`, reportez-vous à la description du module dans la section "Architecture IPQoS et modèle Diffserv" à la page 885. Vous avez également la possibilité de consulter la page du manuel `ipqosconf`(1M).

TABLEAU 35–1 Messages d'erreur IPQoS *(Suite)*

Message d'erreur	Description	Solution
`Unrecognized value, line` *numéro de la ligne*	La valeur du *numéro de la ligne* du fichier de configuration n'est pas une valeur d'énumération prise en charge par le paramètre.	Vérifiez la validité de la valeur d'énumération choisie pour le paramètre. Pour obtenir une description du module appelé par l'instruction `action` avec le numéro de ligne non reconnu, reportez-vous à la section "Architecture IPQoS et modèle Diffserv" à la page 885. Vous avez également la possibilité de consulter la page du manuel `ipqosconf`(1M).
`Malformed value list line` *numéro de la ligne*	L'énumération spécifiée à la ligne *numéro de la ligne* du fichier de configuration n'est pas conforme à la syntaxe de spécification.	Pour en savoir plus sur la syntaxe correcte du module appelé par l'instruction `action` avec la liste de valeurs non conforme, reportez-vous à la description du module figurant à la section "Architecture IPQoS et modèle Diffserv" à la page 885. Vous avez également la possibilité de consulter la page du manuel `ipqosconf`(1M).
`Duplicate parameter line` *numéro de la ligne*	Un paramètre en double a été spécifié à la ligne *numéro de la ligne* qui n'est pas autorisé dans le fichier de configuration.	Supprimez les paramètres en double.
`Invalid action name line` *numéro de la ligne*	Vous avez attribué à l'action, ligne *numéro de la ligne* du fichier de configuration un nom correspondant à un des noms prédéfinis ("continue" ou "drop").	Renommez l'action de sorte que son nom diffère des noms prédéfinis.
`Failed to resolve src/dst host name for filter at line` *numéro de la ligne*`, ignoring filter`	`ipqosconf` n'a pas pu résoudre l'adresse d'origine ou de destination définie pour le filtre concerné dans le fichier de configuration. En conséquence, le filtre n'est pas pris en compte.	Si le filtre est important, réessayez d'appliquer la configuration plus tard.
`Incompatible address version line` *numéro de la ligne*	La version IP de l'adresse à la ligne *numéro de la ligne* est incompatible avec la version d'une adresse IP ou d'un paramètre `version_ip` déjà spécifié.	Modifiez les deux entrées en conflit de manière à ce qu'elles soient compatibles.
`Action at line` *numéro de la ligne* `has the same name as currently installed action, but is for a different module`	Vous avez essayé de modifier le module d'une action qui existe déjà dans la configuration IPQoS du système, mais ce n'est pas autorisé.	Videz la configuration actuelle avant d'appliquer la nouvelle configuration.

◆ ◆ ◆ CHAPITRE 36

Utilisation de la comptabilisation des flux et de la collecte statistique (tâches)

Ce chapitre décrit comment obtenir des informations comptables et statistiques sur le trafic géré par un système IPQoS. Il aborde les sujets suivants :

Configuration de la comptabilisation des flux (liste des tâches)

La liste de tâches suivante répertorie les tâches générales dont le but est d'obtenir des informations sur les flux de trafic à l'aide du module `flowacct`. La liste renvoie également aux procédures permettant d'effectuer ces tâches.

Tâche	Description	Voir
1. Créez un fichier destiné à contenir les informations comptables sur les flux de trafic.	Exécutez la commande `acctadm` pour produire un fichier répertoriant les résultats issus du traitement de `flowacct`.	"Création d'un fichier contenant les données de comptabilisation des flux" à la page 880
2. Définissez les paramètres de `flowacct` dans le fichier de configuration IPQoS.	Définissez les valeurs des paramètres `timer`, `timeout` et `max_limit`.	"Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS" à la page 855

Enregistrement des informations sur les flux de trafic

Collectez les informations sur les flux à l'aide du module `flowacct` IPQoS. Il est possible, par exemple, de recueillir les adresses source et de destination, le nombre de paquets d'un flux et d'autres données similaires. Le processus consistant à accumuler et à enregistrer des informations relatifs aux flux s'appelle la *comptabilisation de flux*.

Les résultats de la comptabilisation de flux sur le trafic d'une classe donnée sont enregistrés dans la table des *enregistrements de flux*. Chaque enregistrement de flux se décompose en une série d'attributs. Ces attributs contiennent des données sur les flux de trafic de la classe en question sur une période de temps. Pour connaître la liste des attributs de `flowacct`, reportez-vous au Tableau 37–4.

La comptabilisation des flux est un outil pratique pour la facturation des clients telle qu'elle est définie dans leur accord de niveau de service. Vous pouvez également faire appel à la comptabilisation des flux pour obtenir des statistiques sur les flux en rapport avec des applications critiques. Cette section récapitule les tâches au cours desquelles le module `flowacct` est associé à l'utilitaire de comptabilité étendue Oracle Solaris afin d'obtenir les données des flux de trafic.

Les informations suivantes se trouvent dans des ressources hors de ce chapitre :

- Pour connaître la procédure permettant de créer une instruction `flowacct` dans le fichier de configuration IPQoS, reportez-vous à la section “Configuration du contrôle de flux dans le fichier de configuration IPQoS ” à la page 866.
- Pour en savoir plus sur le fonctionnement de `flowacct`, reportez-vous à la section “Module de classification” à la page 885.
- Pour obtenir des informations techniques, reportez-vous à la page de manuel `flowacct`(7ipp).

▼ Création d'un fichier contenant les données de comptabilisation des flux

Avant d'ajouter une action `flowacct` dans le fichier de configuration IPQoS, vous devez créer un fichier pour les enregistrements de flux provenant du module `flowacct`. À cet effet, exécutez la commande `acctadm`. La commande `acctadm` enregistre les attributs de base ou les attributs étendus dans le fichier. Tous les attributs `flowacct` sont répertoriés dans le Tableau 37–4. Pour plus d'informations sur `acctadm`, reportez-vous à la page de manuel `acctadm`(1M).

1 Prenez le rôle d'administrateur principal ou connectez-vous en tant que superutilisateur dans le système IPQoS.

Le rôle d'administrateur principal inclut le profil d'administrateur principal. Pour plus d'informations sur la création d'un rôle et son assignation à un utilisateur, reportez-vous au Chapitre 2, "Utilisation de la console de gestion Solaris (tâches) " du *Guide d'administration système : administration de base*.

2 Créez un fichier standard de comptabilisation de flux.

Voici comment créer un fichier standard de comptabilisation de flux pour le serveur Web Premium tel qu'il est configuré dans l'Exemple 34–1.

```
# /usr/sbin/acctadm -e basic -f /var/ipqos/goldweb/account.info flow
```

`acctadm -e`	Appelle la commande `acctadm` assortie de l'option `-e`. L'option `-e` active les arguments qui suivent.
`basic`	Déclare que seules les données des huit attributs `flowacct` standard doivent être enregistrées dans le fichier.
`/var/ipqos/goldweb/account.info`	Spécifie le nom du chemin complet du fichier contenant les enregistrements de flux émanant de `flowacct`.
`flow`	Demande à `acctadm` d'activer la comptabilisation des flux.

3 Examinez les information sur la comptabilisation des flux concernant le système IPQoS en tapant `acctadm` sans arguments.

`acctadm` génère la sortie suivante :

```
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
```

Toutes les entrées hormis les quatre dernières sont destinées à la fonction du gestionnaire de ressources de Solaris. Le tableau suivant décrit les entrées spécifiques à IPQoS.

Entrée	Description
`Flow accounting: active`	Indique que la comptabilisation est activée.

Entrée	Description
`Flow accounting file: /var/ipqos/goldweb/account.info`	Indique le nom du fichier de comptabilisation des flux actuel.
`Tracked flow resources: basic`	Spécifie que seuls les attributs de flux standard sont suivis.
`Untracked flow resources: dsfield,ctime,lseen,projid,uid`	Dresse la liste des attributs de `flowacct` pour lequel aucun suivi n'est effectué dans le fichier.

4 (Facultatif) Ajoute les attributs étendus au fichier de comptabilisation.

```
# acctadm -e extended -f /var/ipqos/goldweb/account.info flow
```

5 (Facultatif) Renvoie à l'enregistrement les attributs standard dans la fichier de comptabilisation.

```
# acctadm -d extended -e basic -f /var/ipqos/goldweb/account.info
```

L'option `-d` désactive la comptabilité étendue.

6 Voir le contenu du fichier de comptabilisation des flux.

Pour savoir comment afficher le contenu d'un fichier de comptabilisation de flux, reportez-vous à la section "Interface Perl pour libexacct" du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

Voir aussi

- Pour plus d'informations sur la fonction de comptabilisation étendue, reportez-vous au Chapitre 4, "Comptabilisation étendue (présentation)" du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.
- Pour définir les paramètres de `flowacct` dans le fichier de configuration IPQoS, reportez-vous à la section "Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS" à la page 855.
- Pour imprimer les données du fichier créé à l'aide de la commande `acctadm`, reportez-vous à la section "Interface Perl pour libexacct" du *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*.

Collecte des informations statistiques

Vous pouvez utiliser la commande `kstat` pour produire des informations statistiques grâce aux modules IPQoS. Utilisez la syntaxe suivante :

`/bin/kstat -m` *ipqos-module-name*

Spécifiez un nom de module IPQoS valide comme illustré dans le Tableau 37–5. Ainsi, pour afficher les statistiques générées par le marqueur `dscpmk`, utilisez le format suivant de la commande `kstat` :

```
/bin/kstat -m dscpmk
```

Pour obtenir des informations techniques, reportez-vous à la page de manuel `kstat`(1M).

EXEMPLE 36–1 Statistiques `kstat` pour IPQoS

Voici les résultats qu'il est possible d'obtenir suite à l'exécution de la commande `kstat` afin d'obtenir des statistiques sur le module `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` Désigne la classe par le nom de la classe à laquelle les flux de trafic appartiennent. Dans l'exemple illustré, il s'agit de `flacct`.

`bytes_in_tbl` Nombre total d'octets dans la table des flux. Le nombre total d'octets constitue la somme, exprimée en octets, de tous les enregistrements de flux actuellement consignés dans la table de flux. Le nombre total d'octets de cette table de flux est 84. Si aucun flux ne se trouve dans la table, la valeur de `bytes_in_tbl` est 0.

`crtime` Heure à laquelle la sortie `kstat` a été générée.

`epackets` Nombre de paquets ayant entraîné une erreur au cours du traitement. Dans l'exemple, cette valeur est nulle.

`flows_in_tbl` Nombre d'enregistrements de flux dans la table de flux qui, dans cet exemple, est 1. Si aucun enregistrement ne se trouve dans la table, la valeur de `flows_in_tbl` est 0.

`nbytes` Nombre total d'octets visibles par cette instance d'action `flowacct`. Il est de 84 dans l'exemple. La valeur inclut les octets qui se trouvent actuellement dans la table des flux. La valeur inclut également des octets dont le délai est dépassé et qui ne figurent plus dans la table des flux.

`npackets` Nombre total de paquets visibles par cette instance d'action `flowacct`. Il est de 1 dans l'exemple. `npackets` inclut les paquets qui se trouvent actuellement dans la table de flux. `npackets` inclut les paquets dont le délai est dépassé et ne figurant plus dans la table des flux.

`usedmem` Mémoire, exprimée en nombre d'octets, utilisée par la table de flux qui est gérée par cette instance de `flowacct`. La valeur `usedmem` est de 256 dans l'exemple. La valeur de `usedmem` est de 0 si la table des flux n'affiche aucun

EXEMPLE 36–1 Statistiques `kstat` pour IPQoS *(Suite)*

enregistrement de flux.

◆ ◆ ◆ CHAPITRE 37

IPQoS en détails (référence)

Ce chapitre contient du matériel de référence fournissant des informations approfondies sur les sujets IPQoS suivants :

Pour obtenir une présentation générale, reportez-vous au Chapitre 32, "Présentation d'IPQoS (généralités)". Pour obtenir des informations sur la planification, reportez-vous au Chapitre 33, "Planification d'un réseau IPQoS (tâches)". Pour consulter les procédures de configuration d'IPQoS, reportez-vous au Chapitre 34, "Création du fichier de configuration IPQoS (tâches)".

Architecture IPQoS et modèle Diffserv

Cette section décrit l'architecture IPQoS et la manière dont IPQoS implémente le modèle de services différenciés (Diffserv) défini par le document RFC 2475, An Architecture for Differentiated Services (`http://www.ietf.org/rfc/rfc2475.txt?number=2475`) (en anglais). Les éléments suivants du modèle Diffserv sont inclus dans IPQoS :

- classificateur ;
- compteur ;
- marqueur.

Par ailleurs, IPQoS inclut le module de comptabilisation des flux et le marqueur `dlcosmk` utilisé avec les périphériques VLAN (réseau local virtuel).

Module de classification

Dans le modèle Diffserv, le *classifieur* est chargé d'organiser les flux de trafic sélectionnés en groupes auxquels s'appliquent différents niveaux de service. Les classificateurs définis dans le document RFC 2475 ont été initialement conçus pour les routeurs de bordure. En revanche, le

classificateur IPQoS `ipgpc` est destiné à traiter les flux de trafic pour les hôtes internes au réseau local. En conséquence, un réseau doté de systèmes IPQoS et d'un routeur Diffserv peut fournir un niveau supérieur de services différenciés. Pour obtenir une description technique du classificateur `ipgpc`, reportez-vous à la page de manuel `ipgpc` (7ipp).

Le classificateur `ipgpc` effectue les opérations suivantes :

1. Sélection des flux de trafic répondant aux critères spécifiés dans le fichier de configuration IPQoS sur le système IPQoS

   La stratégie QoS définit les différents critères obligatoirement présents dans les en-têtes de paquets. Ces critères sont appelés *sélecteurs*. Le classificateur `ipgpc` compare ces sélecteurs aux en-têtes de paquets reçus par le système IPQoS. `ipgpc` sélectionne ensuite tous les paquets correspondants.
2. Séparation des flux de paquets en *classes* : trafic réseau dont les caractéristiques sont identiques comme indiqué dans le fichier de configuration IPQoS
3. Examen de la valeur du champ de services différenciés (DS) du paquet grâce à la présence d'un point de code de services différenciés ou DSCP

   La présence du DSCP indique si l'expéditeur a prévu un comportement de transmission pour le trafic entrant.
4. Définition de l'action supplémentaire spécifiée dans le fichier de configuration IPQoS pour les paquets d'une classe particulière
5. Transmission des paquets au module IPQoS suivant indiqué dans le fichier de configuration IPQoS ou renvoi des paquets dans le trafic réseau

Pour obtenir des informations générales sur le classificateur, reportez-vous à la section "Présentation du classificateur (`ipgpc`)" à la page 811. Pour plus d'informations sur l'appel du classificateur dans le fichier de configuration IPQoS, reportez-vous à la section "Fichier de configuration IPQoS" à la page 898.

Sélecteurs IPQoS

Le classificateur `ipgpc` prend en charge un grand nombre de sélecteurs que vous pouvez utiliser dans la clause `filter` du fichier de configuration IPQoS. Lorsque vous définissez un filtre, veillez à n'utiliser que le minimum de sélecteurs nécessaire à la récupération du trafic d'une classe particulière. Le nombre de filtres défini peut avoir des conséquences sur les performances du protocole IPQoS.

Le tableau suivant dresse la liste des sélecteurs disponibles pour `ipgpc`.

TABLEAU 37–1 Sélecteurs de filtre pour le classificateur IPQoS

Sélecteur	Argument	Informations sélectionnées
`saddr`	Numéro d'adresse IP.	Adresse source.

TABLEAU 37–1 Sélecteurs de filtre pour le classificateur IPQoS *(Suite)*

Sélecteur	Argument	Informations sélectionnées
`daddr`	Numéro d'adresse IP.	Adresse de destination.
`sport`	Numéro du port ou nom du service comme indiqué dans le fichier `/etc/services`.	Port source à partir duquel provient une classe de trafic.
`dport`	Numéro du port ou nom du service comme indiqué dans le fichier `/etc/services`.	Port de destination auquel une classe de trafic est liée.
`protocol`	Numéro ou nom de protocole comme indiqué dans le fichier `/etc/services`.	Protocole à utiliser par cette classe de trafic.
`dsfield`	Point de code DS (DSCP) d'une valeur comprise dans l'intervalle 0–63.	DSCP définissant un comportement de transmission à appliquer au paquet. Si ce paramètre est spécifié, le paramètre `dsfield_mask` doit également être spécifié.
`dsfield_mask`	Masque de bits d'une valeur comprise entre 0 et 255.	Utilisé conjointement avec le sélecteur `dsfield`. `dsfield_mask` est appliqué au sélecteur `dsfield` pour déterminer les bits qu'il faut faire correspondre.
`if_name`	Nom de l'interface.	Interface à utiliser pour le trafic entrant et le trafic sortant d'une classe particulière.
`user`	Numéro de l'identifiant utilisateur UNIX ou nom d'utilisateur à sélectionner. Si aucun identifiant utilisateur ou nom d'utilisateur ne se trouve dans le paquet, le paramètre par défaut –1 est appliqué.	ID utilisateur fourni à une application.
`projid`	Numéro de l'ID du projet à sélectionner.	ID du projet fourni à une application.
`priority`	Numéro de la priorité. La priorité la plus basse est de 0.	Priorité attribuée aux paquets de cette classe. La priorité sert à classer les filtres selon leur importance dans une même classe.
`direction`	Cet argument correspond à l'un des éléments suivants :	Direction du flux du paquet de la machine IPQoS.
	`LOCAL_IN`	Trafic local d'entrée au système IPQoS.
	`LOCAL_OUT`	Trafic local de sortie au système IPQoS.
	`FWD_IN`	Trafic d'entrée à transférer.
	`FWD_OUT`	Trafic de sortie à transférer.
`precedence`	Valeur du niveau de priorité. Le niveau de priorité le plus élevé est de 0.	Le niveau de priorité sert à classer les filtres de même priorité.

TABLEAU 37–1 Sélecteurs de filtre pour le classificateur IPQoS *(Suite)*

Sélecteur	Argument	Informations sélectionnées
`ip_version`	`V4` ou `V6`	Schéma d'adressage utilisé par les paquets. Il s'agit de IPv4 ou de IPv6.

Module de mesure

Le *compteur* permet de suivre le taux de transmission des flux exprimé en nombre de paquets. Le compteur détermine si le paquet est conforme aux paramètres configurés. Le module de mesure détermine l'action suivante à entreprendre pour un paquet provenant d'un jeu d'actions en fonction de la taille du paquet, des paramètres configurés et du débit du flux.

Le compteur comprend deux modules de mesure, `tokenmt` et `tswtclmt`, que vous définissez dans le fichier de configuration IPQoS. Vous pouvez configurer l'un des deux modules ou les deux modules pour une classe donnée.

Lorsque vous configurez un module de mesure, vous pouvez définir deux paramètres pour une même vitesse de tranfert :

- `committed-rate` – définit le taux de transmission acceptable en bits par seconde pour les paquets d'une classe particulière.
- `peak-rate` – définit le taux de transmission maximal en bits par seconde autorisé pour les paquets d'une classe particulière.

Une action de mesure d'un paquet peut aboutir à l'un des trois résultats suivants :

- `green` – Le paquet contraint le flux à rester dans les limites du débit garanti.
- `yellow` – Le paquet contraint le flux à dépasser le débit garanti, mais pas le débit de pointe.
- `red` – Le paquet contraint le flux à dépasser le débit de pointe.

Vous pouvez associer chaque résultat à différentes actions dans le fichier de configuration IPQoS. Le débit garanti et le débit de pointe sont traités à la section suivante.

Module de mesure `tokenmt`

Le module `tokenmt` utilise des *seaux de jetons* pour mesurer le taux de transmission d'un flux. Vous pouvez configurer `tokenmt` pour fonctionner comme un compteur à débit simple ou à débit double. Une instance d'action `tokenmt` gère deux seaux de jetons qui déterminent si le flux de trafic est conforme aux paramètres configurés.

La page de manuel `tokenmt(7ipp)` explique comment IPQoS implémente le paradigme du contrôle de jetons. Pour obtenir des informations générales sur les seaux de jetons, reportez-vous à la documentation *Services différenciés pour Internet* de Kalevi Kilkki et à différents sites Web.

Les paramètres de configuration pour `tokenmt` sont les suivants :

- `committed_rate` – spécifie le taux garanti du flux en bits par seconde.
- `committed_burst` – spécifie la taille maximale de rafale garantie en bits. Le paramètre `committed_burst` définit le nombre de paquets sortants d'une classe spécifique pouvant arriver sur le réseau à un débit garanti.
- `peak_rate` – spécifie le débit de pointe en bits par seconde.
- `peak_burst` – spécifie la taille maximale de rafale ou de pointe en bits. Le paramètre `peak_burst` accorde à une classe de trafic une taille peak-burst qui dépasse le débit garanti.
- `color_aware` – active le mode de compatibilité pour `tokenmt`.
- `color_map` – définit un tableau d'entiers faisant correspondre les valeurs DSCP au vert, à l'orange et au rouge.

Configuration du tokenmt en tant que compteur à débit simple

Pour configurer `tokenmt` en tant que compteur à débit simple, ne spécifiez pas le paramètre `peak_rate` pour `tokenmt` dans le fichier de configuration IPQoS. Pour configurer une instance `tokenmt` à débit simple afin d'obtenir un résultat rouge, vert ou orange, vous devez spécifier le paramètre `peak_burst` . Si vous n'utilisez pas le paramètre `peak_burst`, vous pouvez configurer `tokenmt` de sorte qu'il aboutisse seulement à un résultat rouge ou vert. Pour consulter un exemple de `tokenmt` à débit simple donnant lieu à deux résultats, reportez-vous à l'Exemple 34–3.

Lorsque `tokenmt` fonctionne comme un compteur à débit simple, le paramètre `peak_burst` définit, en fait, la taille de rafale excessive. Les paramètres `committed_rate` et `committed_burst` ou `peak_burst` doivent désigner des entiers positifs non nuls.

Configuration du tokenmt en tant que compteur à débit double

Pour configurer `tokenmt` en tant que compteur à débit double, spécifiez le paramètre `peak_rate` pour l'action `tokenmt` dans le fichier de configuration IPQoS. Un module `tokenmt` à débit double a toujours trois résultats : vert, rouge et orange. Les paramètres `committed_rate` , `committed_burst` et `peak_burst` doivent désigner des entiers positifs non nuls.

Configuration du module tokenmt en mode de reconnaissance des couleurs

Pour configurer un module `tokenmt` à débit double en mode de reconnaissance des couleurs, vous devez prévoir des paramètres supplémentaires pour ajouter la fonction d'interprétation des couleurs." L'instruction suivante montre comment configurer le mode de reconnaissance des couleurs pour `tokenmt`.

EXEMPLE 37–1 Action `tokenmt` de prise en compte des couleurs dans le fichier de configuration IPQoS

```
action {
    module tokenmt
    name meter1
```

EXEMPLE 37–1 Action `tokenmt` de prise en compte des couleurs dans le fichier de configuration IPQoS *(Suite)*

```
    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}
    }
}
```

Vous pouvez activer la fonction de reconnaissance des couleurs en définissant le paramètre `color_aware` sur `true`. En tant que module d'interprétation des couleurs, `tokenmt` suppose que le paquet est déjà marqué en rouge, orange ou vert par une action `tokenmt` précédente. Le module d'interprétation des couleurs `tokenmt` évalue un paquet à l'aide du DSCP figurant dans l'en-tête du paquet en plus des paramètres de compteur à débit double.

Le paramètre `color_map` contient un tableau auquel le DSCP de l'en-tête du paquet est lié. Considérez le tableau `color_map` suivant :

```
color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
```

Les paquets avec un DSCP compris entre 0 et 20 ou équivalent à 22 correspondent au vert. Les paquets avec un DSCP équivalent à 21 ou compris entre 23 et 42 correspondent au rouge. Les paquets avec un DSCP compris entre 43 et 63 sont associés à l'orange. Par défaut, `tokenmt` conserve une table de correspondance de couleurs. Cependant, il est possible de modifier au besoin les valeurs par défaut à l'aide des paramètres `color_map`.

Pour les paramètres *couleur*`_action_name`, vous pouvez spécifier `continue` de manière à terminer le traitement du paquet. Vous pouvez aussi ajouter un argument pour soumettre le paquet à une action de marquage, par exemple, `yellow_action_name mark22`.

Module de mesure `tswtclmt`

Le module `tswtclmt` évalue la bande passante moyenne pour une classe de trafic en procédant à l'*estimation du débit* en fonction du temps. `tswtclmt` fonctionne toujours comme un contrôle à trois résultats. La fonction d'estimation du débit fournit une indication du taux d'arrivée du flux. Ce taux doit correspondre à la bande passante moyenne applicable à un flux de trafic sur une période de temps donnée appelée *fenêtre*. L'algorithme d'estimation du débit provient de la spécification RFC 2859 *A Time Sliding Window Three Colour Marker*.

Servez-vous des paramètres suivants pour configurer `tswtclmt` :

- `committed_rate` – spécifie le taux garanti en bits par seconde.

- `peak_rate` – spécifie le débit de pointe en bits par seconde.
- `window` – définit la fenêtre de temps, exprimée en millisecondes pendant laquelle la bande passante moyenne est maintenue.

Pour des détails techniques sur `tswtclmt`, reportez-vous à la page de manuel `tswtclmt(7ipp)` Pour obtenir des informations générales sur les lisseurs de débits semblables à `tswtclmt`, reportez-vous au document RFC 2963, A Rate Adaptive Shaper for Differentiated Services (`http://www.ietf.org/rfc/rfc2963.txt?number=2963`) (en anglais).

Module de marquage

IPQoS inclut deux modules de marquage, `dscpmk` et `dlcosmk`. Cette section contient des informations sur l'utilisation des deux marqueurs. En théorie, vous devez utiliser `dscpmk`, car `dlcosmk` n'est disponible que pour les systèmes IPQoS et les périphériques VLAN.

Pour obtenir des informations techniques sur `dscpmk`, reportez-vous à la page de manuel `dscpmk`(7ipp). Pour obtenir des informations techniques sur `dlcosmk`, reportez-vous à la page de manuel `dlcosmk`(7ipp).

Utilisation du marqueur `dscpmk` pour la transmission des paquets

Le marqueur reçoit les flux de trafic après traitements successifs par les modules de classification ou de mesure. Le marqueur associe un comportement de transmission au trafic. Ce comportement indique l'action à appliquer aux flux lorsque ces flux quittent le système IPQoS. Le comportement de transmission d'une classe de trafic est défini par le *comportement par pas ou PHB*. Le PHB affecte une priorité à une classe de trafic précisant les flux prioritaires de cette classe par rapport aux autres classes de trafic. Les PHB régissent uniquement les comportements de transmission sur le réseau contigu du système IPQoS. Pour plus d'informations sur les PHB, reportez-vous à la section “PHB (Per-Hop Behaviors)” à la page 816.

La *transmission de paquet* est le processus consistant à envoyer le trafic d'une classe particulière vers sa prochaine destination sur un réseau. Pour un hôte tel qu'un système IPQoS, un paquet est transmis de l'hôte vers le flux de réseau local. Lorsqu'il s'agit d'un routeur Diffserv, un paquet est transmis du réseau local vers le pas suivant du routeur.

Le marqueur signale dans le champ DS de l'en-tête du paquet un comportement défini dans le fichier de configuration IPQoS. Par la suite, le système IPQoS et les systèmes Diffserv suivants transmettent le trafic comme indiqué dans le champ DS jusqu'à ce que le marquage change. Pour attribuer un PHB, le système IPQoS inscrit une valeur dans le champ DS de l'en-tête du paquet. Cette valeur est appelée le point de code de services différenciés (DSCP). L'architecture Diffserv définit deux types de comportement de transmission, EF et AF, utilisant des DSCP différents. Pour plus d'informations sur les DSCP, reportez-vous à la section “Point de code DS” à la page 816.

Le système IPQoS lit le DSCP et évalue le niveau de priorité par rapport à d'autres flux de trafic sortants. Le système IPQoS établit la priorité des flux de trafic simultanés et libère chaque flux sur le réseau en fonction de sa priorité.

Le routeur Diffserv reçoit les flux de trafic sortants et lit le champ DS dans les en-têtes de paquets. Le DSCP permet au routeur de classifier et d'ordonnancer les flux de trafic simultanés. Le routeur transmet chaque flux en fonction de la priorité indiquée par le PHB. Notez que le PHB ne peut pas être appliqué au-delà de la limite du routeur du réseau à moins que les systèmes Diffserv des pas suivants reconnaissent le même PHB.

PHB Expedited Forwarding (EF) (ou traitement accéléré)

Expedited forwarding (EF) garantit que les paquets dotés du point de code recommandé 46 EF (101110) bénéficient du meilleur traitement disponible sur le réseau. Le service Expedited forwarding est souvent comparé à une ligne spécialisée. Les routeurs Diffserv garantissent un traitement préférentiel aux paquets accompagnés du point de code 46 (101110) pour l'acheminement vers leur destination. Pour obtenir des informations techniques sur le service EF, reportez-vous au document RFC 2598, *An Expedited Forwarding PHB*.

PHB Assured Forwarding (AF) (traitement assuré)

Assured forwarding (AF) offre quatre classes de comportements de transmission applicables au marqueur. Le tableau suivant présente les classes, les trois « drop precedences » (niveaux de priorité) de chaque classe et les DSCP recommandés associés à chaque priorité. Chaque DSCP est représenté par sa valeur AF, sa valeur en notation décimale et en notation binaire.

TABLEAU 37–2 Points de code Assured Forwarding

	Classe 1	Classe 2	Classe 3	Classe 4
Faible niveau de priorité	AF11 = 10 (001010)	AF21 = 18 (010010)	AF31 = 26 (011010)	AF41 = 34 (100010)
Niveau de priorité intermédiaire	AF12 = 12 (001100)	AF22 = 20 (010100)	AF32 = 28 (011100)	AF42 = 36 (100100)
Niveau de priorité élevé	AF13 = 14 (001110)	AF23 = 22 (010110)	AF33 = 30 (011110)	AF43 = 38 (100110)

Tout système Diffserv peut faire appel au point de code AF afin de l'utiliser en tant que guide lors de la fourniture de services différenciés à différentes classes de trafic.

Lorsque ces paquets atteignent un routeur Diffserv, le routeur évalue les points de code des paquets ainsi que les DSCP d'autres flux de trafic placés dans la file d'attente. Le routeur transmet ou rejette les paquets, selon la bande passante disponible et les priorités définies par les

DSCP des paquets. Notez que l'accès à la bande passante est garanti en priorité aux paquets marqués par un PHB EF par rapport aux paquets marqués par un PHB AF (quelle que soit leur classe).

Coordonnez le marquage des paquets entre les différents systèmes IPQoS de votre réseau et le routeur Diffserv pour veiller à ce que les paquets soient transférés comme prévu. Par exemple, supposons que les systèmes IPQoS de votre réseau marquent les paquets à l'aide des points de code AF21 (010010), AF13 (001110), AF43 (100110) et EF (101110). Vous devez ensuite ajouter les DSCP AF21, AF13, AF43 et EF au fichier approprié sur le routeur Diffserv.

Vous trouverez des informations techniques sur le tableau de points de code AF dans le document RFC 2597. Vous trouverez des informations détaillées concernant la configuration du PHB AF sur le site Web des fabricants de routeurs Cisco Systems et Juniper Networks. Servez-vous de ces informations pour définir les PHB AF des systèmes IPQoS ainsi que les routeurs. Par ailleurs, la documentation des fabricants de routeurs contient des instructions pour la définition des points de code DS sur leur matériel.

Fourniture d'un DSCP au marqueur

Le DSCP occupe 6 bits. Le champ DS a une longueur d'1 octet. Lorsque vous définissez un DSCP, le marquer marque les 6 premiers bits significatifs de l'en-tête du paquet avec le code de point DS. Les deux bits restants (les moins significatifs) ne sont pas utilisés.

Pour définir un DSCP, servez-vous du paramètre suivant au sein d'une instruction d'action du marqueur :

```
dscp_map{0-63:DS_codepoint}
```

Le paramètre `dscp_map` est un tableau à 64 éléments que vous remplissez à l'aide de la valeur (DSCP). Le paramètre `dscp_map` sert à faire correspondre les DSCP entrants aux DSCP sortants appliqués par le marqueur `dscpmk`.

Vous devez spécifier la valeur DSCP pour le paramètre `dscp_map` en notation décimale. Par exemple, vous devez traduire le point de code EF de 101110 en valeur décimale 46 ce qui équivaut à `dscp_map{0-63:46}`. Pour les points de code AF, vous devez exprimer les différents points de code présentés dans le Tableau 37–2 en notation décimale spécialement pour le paramètre `dscp_map`.

Utilisation du marqueur `dlcosmk` avec les périphériques VLAN

Le module de marquage `dlcosmk` spécifie le comportement dans l'en-tête MAC d'un datagramme. Vous ne pouvez utiliser le paramètre `dlcosmk` que dans un système IPQoS avec une interface VLAN.

`dlcosmk` ajoute quatre octets, désignés sous l'appellation d'*étiquette VLAN*, à l'en-tête MAC. L'étiquette VLAN inclut une valeur de priorité utilisateur de 3 bits, définie par la norme IEEE

801.D. Les commutateurs Diffserv en mesure de reconnaître VLAN peuvent lire le champ de priorité utilisateur dans un datagramme. Les valeurs de priorité utilisateur 801.D implémentent les marques de classe de service (CoS), connues et comprises par les commutateurs du marché.

Vous pouvez utiliser les valeurs de priorité utilisateur dans l'action du marqueur `dlcosmk` en définissant les indices de classes de service répertoriés dans le tableau suivant.

TABLEAU 37–3 Valeurs de priorité utilisateur 801.D

Classe de service	Définition
0	Au mieux (Best effort)
1	Arrière-plan (Background)
2	Secours (Spare)
3	Effort excellent (Excellent effort)
4	Charge contrôlée (Controlled load)
5	Vidéo inférieure à une latence de 100ms (Video less than 100ms latency)
6	Vidéo inférieure à une latence de 10ms (Video less than 10ms latency)
7	Contrôle du réseau (Network control)

Pour plus d'informations sur `dlcosmk`, reportez-vous à la page de manuel `dlcosmk(7ipp)`.

Configuration IPQoS pour les systèmes comportant des périphériques VLAN

Cette section illustre un scénario de réseau simple montrant comment implémenter IPQoS sur les systèmes avec des périphériques VLAN. Le scénario prend en compte deux systèmes IPQoS, `ordinateur1` et `ordinateur2`, reliés par un commutateur. Le périphérique VLAN sur `ordinateur1` a l'adresse IP `10.10.8.1`. Le périphérique VLAN sur l'`ordinateur2` a l'adresse IP `10.10.8.3`.

Le fichier de configuration IPQoS suivant de l'`ordinateur1` décrit une solution simple pour marquer le trafic allant du commutateur à l'`ordinateur2`.

EXEMPLE 37–2 Fichier de configuration IPQoS pour un système avec un périphérique VLAN

```
fmt_version 1.0
action {
        module ipgpc
          name ipgpc.classify

        filter {
                name myfilter2
```

EXEMPLE 37–2 Fichier de configuration IPQoS pour un système avec un périphérique VLAN *(Suite)*

```
                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
        }
}
```

Dans cette configuration, tout le trafic de l'`ordinateur1` destiné au périphérique VLAN sur l'`ordinateur2` est transféré sur le marqueur `dlcosmk`. L'action de marqueur `marque4` indique à `dlcosmk` d'ajouter une marque VLAN aux datagrammes de la classe `maclasse` possédant une classe de service de 4. La valeur de priorité utilisateur 4 indique que le commutateur reliant les deux machines doit donner le transfert de charge contrôlé aux flux de trafic `maclasse` de `machine1`.

Module `flowacct`

Le module `flowacct` d'IPQoS enregistre les informations sur les flux de trafic, un processus connu sous le nom de *comptabilisation des flux*. La comptabilisation des flux produit des données qui peuvent servir à la facturation des clients ou à l'évaluation du trafic d'une classe particulière.

La comptabilisation des flux est facultative. Le module `flowacct` est généralement le dernier module par lequel passent les flux de trafic mesurés ou marqués avant d'être libérés sur le réseau. Pour voir la position de `flowacct` dans le modèle Diffserv, reportez-vous à la Figure 32–1. Pour obtenir des informations techniques sur `flowacct`, reportez-vous à la page de manuel `flowacct`(7ipp).

Pour activer la comptabilisation de flux, vous devez utiliser la fonction de comptabilisation `exacct` d'Oracle Solaris avec les commandes `acctadm` et `flowacct`. Pour connaître les étapes générales de la configuration de la comptabilisation, reportez-vous à la section “Configuration de la comptabilisation des flux (liste des tâches)” à la page 879.

Paramètres `flowacct`

Le module `flowacct` rassemble les informations sur les flux dans une *table de flux* composée d'*enregistrements de flux*. Chaque entrée de la table contient un enregistrement de flux. Vous ne pouvez pas afficher une table de flux.

Dans le fichier de configuration IPQoS, vous définissez les paramètres `flowacct` suivants pour mesurer les enregistrements de flux et consigner les enregistrements dans la table :

- `timer` – définit un intervalle, en millisecondes, lorsque les flux dont le délai a expiré sont supprimés de la table de flux et consignés dans le fichier créé par `acctadm`.
- `timeout` – définit un intervalle, en millisecondes, spécifiant la durée d'inactivité d'un flux de paquet avant que ce dernier ne soit considéré comme ayant expiré.

Remarque – Vous pouvez configurer `timer` et `timeout` de sorte qu'ils aient des valeurs différentes.

- `max_limit` – définit la limite supérieure du nombre d'enregistrements de flux pouvant être stockés dans la table de flux.

Pour obtenir un exemple d'utilisation des paramètres `flowacct` dans le fichier de configuration IPQoS, reportez-vous à la section "Configuration du contrôle de flux dans le fichier de configuration IPQoS " à la page 866.

Table de flux

Le module `flowacct` gère une table visant à enregistrer tous les flux de paquets rencontrés par une instance de `flowacct`. Un flux est identifié par les paramètres suivants qui incluent l'uplet à 8 attributs de `flowacct` :

- adresse source ;
- adresse de destination ;
- port source ;
- port de destination ;
- DSCP ;
- ID d'utilisateur ;
- ID du projet ;
- numéro du protocole.

Si tous les paramètres de l'uplet à 8 attributs concernant un même flux sont identiques, la table de flux ne contient qu'une seule entrée. Le paramètre `max_limit` détermine le nombre d'entrées que peut inclure une table de flux.

La table de flux est numérisée à l'intervalle spécifié dans le fichier de configuration IPQoS grâce au paramètre `timer`. Le paramètre par défaut est de 15 secondes. Un flux « arrive à expiration » lorsque ses paquets ne sont pas visibles par le système IPQoS à la fin du `délai d'attente` (au

moins) indiqué dans le fichier de configuration IPQoS. Le délai d'attente par défaut est de 60 secondes. Les entrées dont le délai d'attente a été dépassé sont ensuite enregistrées dans le fichier de comptabilisation créé par la commande `acctadm`.

Enregistrements `flowacct`

Un enregistrement `flowacct` inclut les attributs décrits dans le tableau suivant.

TABLEAU 37–4 Attributs d'un enregistrement `flowacct`

Nom d'attribut	Contenu des attributs	Type
`src-addr-`*type-adresse*	Adresse source de l'expéditeur. *type-adresse* équivaut à `v4` pour IPv4 ou `v6` pour IPv6, comme indiqué dans le fichier de configuration IPQoS.	De base
`dest-addr-`*type-adresse*	Adresse de destination des paquets. *type-adresse* équivaut à `v4` pour IPv4 ou `v6` pour IPv6, comme indiqué dans le fichier de configuration IPQoS.	De base
`src-port`	Port source d'où provient le flux.	De base
`dest-port`	Numéro du port de destination vers lequel le flux est dirigé.	De base
`protocol`	Numéro du protocole du flux.	De base
`total-packets`	Nombre de paquets dans le flux.	De base
`total-bytes`	Nombre d'octets dans le flux.	De base
nom-action	Nom de l'action `flowacct` ayant enregistré le flux.	De base
`creation-time`	Première fois qu'un paquet est vu par `flowacct`.	Étendu uniquement
`last-seen`	Dernière fois qu'un paquet du flux a été vu.	Étendu uniquement
`diffserv-field`	DSCP dans les en-têtes de paquets sortants du flux.	Étendu uniquement
`user`	ID utilisateur ou nom d'utilisateur UNIX obtenu par l'application.	Étendu uniquement
`projid`	ID du projet obtenu par l'application.	Étendu uniquement

Utilisation d'`acctadm` avec le module `flowacct`

Vous utilisez la commande `acctadm` pour créer un fichier réservé aux enregistrements de flux générés par `flowacct`. `acctadm` s'utilise en parallèle avec la fonction de comptabilisation étendue. Pour plus d'informations techniques sur `acctadm`, reportez-vous à la page de manuel `acctadm(1M)`.

Le module `flowacct` observe les flux et inscrit les enregistrements de flux dans la table de flux. `flowacct` évalue ensuite ses paramètres et attributs dans l'intervalle spécifié par `timer`. Un paquet expire s'il n'est pas visible pendant la durée équivalent aux valeurs `last_seen` et `timeout`. Toutes les entrées ayant dépassé le délai d'expiration sont supprimées de la table de flux. Elles sont alors consignées dans le fichier de comptabilisation à l'issue de l'intervalle spécifié par le paramètre `timer`.

Pour appliquer `acctadm` au module `flowacct`, respectez la syntaxe suivante :

`acctadm -e` *file-type* `-f` *filename* `flow`

`acctadm -e`	Appelle la commande `acctadm` assortie de l'option `-e`. La valeur -e indique la présence d'une liste de ressources.
type-fichier	Spécifie les attributs à collecter. *type-fichier* doit être remplacé par la valeur `basic` ou `extended`. Pour connaître la liste des attributs de chaque type de fichier, reportez-vous au Tableau 37–4.
`-f`*nom-fichier*	Crée le fichier *nom-fichier* dans lequel sont consignés les enregistrements de flux.
`flow`	Implique l'exécution de la commande `acctadm` avec IPQoS.

Fichier de configuration IPQoS

Cette section décrit en détail les différentes parties du fichier de configuration IPQoS. La stratégie activée au démarrage d'IPQoS est stockée dans le fichier `/etc/inet/ipqosinit.conf`. Bien qu'il soit possible de modifier ce fichier, dans le cas d'un nouveau système IPQoS, il est préférable de créer un fichier de configuration sous un autre nom. Les tâches à réaliser pour appliquer et déboguer une configuration IPQoS sont présentées dans le Chapitre 34, “Création du fichier de configuration IPQoS (tâches)”.

La syntaxe du fichier de configuration IPQoS est présentée dans l'Exemple 37–3. Cet exemple utilise les conventions suivantes :

- `caractères machine` – Informations d'ordre syntaxique décrivant les différentes parties du fichier de configuration. Comme ce style correspond à des explications, vous n'avez pas à saisir de texte.
- **`caractères gras`** – Texte littéral qu'il est nécessaire de saisir dans le fichier de configuration IPQoS. Vous devez toujours commencer, par exemple, le fichier de configuration IPQoS par l'instruction **`fmt_version`**.
- *caractères en italique* – Variable que vous devez remplacer par des données descriptives de votre configuration. Vous devez toujours remplacer, par exemple, la variable *nom-action* ou *nom-module* par les informations relatives à votre configuration.

EXEMPLE 37–3 Syntaxe du fichier de configuration IPQoS

```
file_format_version ::= fmt_version version

action_clause ::= action {
      name action-name
      module module-name
      params-clause |  ""
      cf-clauses
}
action_name ::= string
module_name ::= ipgpc | dlcosmk | dscpmk | tswtclmt | tokenmt | flowacct

params_clause ::= params {
      parameters
      params-stats |   ""
      }
parameters ::=     prm-name-value parameters |  ""
prm_name_value ::= param-name param-value

params_stats ::= global-stats boolean

cf_clauses ::= class-clause cf-clauses |
               filter-clause cf-clauses | ""

class_clause ::= class {
      name class-name
      next_action next-action-name
      class-stats | ""
                  }
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
```

Le texte restant décrit chacune des principales parties du fichier de configuration IPQoS.

Instruction `action`

Les instructions `action` servent à appeler les différentsmodules IPQoS décrits à la section “Architecture IPQoS et modèle Diffserv” à la page 885.

Lorsque vous créez le fichier de configuration IPQoS, vous devez toujours commencer par indiquer le numéro de version. Vous devez ensuite ajouter l'instruction `action` suivante pour appeler le classificateur :

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
}
```

Faites suivre l'instruction `action` du classificateur par une clause `params` ou une clause `class`.

Respectez la syntaxe suivante pour toutes les autres instructions `action` :

```
action {
name action-name
module module-name
params-clause | ""
cf-clauses
}
```

`name` *nom-action*	Attribue un nom à l'action.
`module` *nom-module*	Identifie le module IPQoS à appeler (il doit s'agir de l'un des modules présentés dans le Tableau 37–5).
clause-params	Il peut s'agir des paramètres à traiter par le classificateur (statistiques globales ou prochaine action à effectuer, par exemple).
clauses-cf	Ensemble constitué d'aucune ou de plusieurs clauses `class` ou `filter`

Définitions des modules

La définition du module désigne le module chargé de traiter les paramètres dans l'instruction `action`. Le fichier de configuration IPQoS peut inclure les modules suivants.

TABLEAU 37–5 Modules IPQoS

Nom du module	Définition
`ipgpc`	Classifieur IP
`dscpmk`	Marqueur servant à créer des DSCP dans des paquets IP
`dlcosmk`	Marqueur à utiliser avec les périphériques VLAN
`tokenmt`	Compteur de seau à jetons
`tswtclmt`	Compteur de fenêtre de temps

TABLEAU 37–5 Modules IPQoS *(Suite)*

Nom du module	Définition
`flowacct`	module de comptabilisation des flux ;

Clause `class`

Vous définissez une clause `class` pour chaque classe de trafic.

Respectez la syntaxe suivante pour définir les classes restantes dans la configuration IPQoS :

```
class {

      name class-name
      next_action next-action-name
}
```

Pour collecter des statistiques au sujet d'une classe particulière, vous devez d'abord activer les statistiques globales dans l'instruction `ipgpc.classify action.` Pour plus d'informations, reportez-vous à la section "Instruction `action`" à la page 899.

Utilisez l'instruction `enable_stats TRUE` chaque fois que vous souhaitez établir des statistiques pour une classe. Si vous n'avez pas besoin de connaître les statistiques d'une classe, il suffit de spécifier `enable_stats FALSE` ou de supprimer l'instruction `enable_stats`.

Le trafic sur un réseau IPQoS non défini de façon explicite est relégué vers la *classe par défaut*.

Clause `filter`

Les *filtres* sont constitués de sélecteurs qui regroupent les flux de trafic en classes. Ces sélecteurs définissent plus précisément les critères à appliquer au trafic de la classe créée dans la clause class. Si un paquet répond à tous les critères des sélecteurs du filtre de priorité supérieur, il est considéré comme un membre de la classe du filtre. Pour obtenir la liste complète des sélecteurs applicables au classificateur `ipgpc`, reportez-vous au Tableau 37–1.

Vous définissez les filtres dans le fichier de configuration IPQoS à l'aide d'une *clause filter* correspondant à la syntaxe suivante :

```
filter {
       name filter-name
       class class-name
       parameters (selectors)
       }
```

Clause params

La clause params contient les instructions de traitement pour le module défini dans l'instruction action. Respectez la syntaxe suivante pour la clause params :

```
params {
            parameters
            params-stats | ""
       }
```

Dans la clause params, vous utilisez les paramètres qui se rapportent au module.

La valeur *stats-paramètres* définie dans la clause params est soit global_stats TRUE, soit global_stats FALSE. L'instruction global_stats TRUE a pour effet d'activer les statistiques de type UNIX pour l'instruction action à partir de laquelle les statistiques globales sont demandées. Pour afficher les statistiques, exécutez la commande kstat. Vous devez activer les statistiques de l'instruction action avant d'activer les statistiques par classe.

Utilitaire de configuration ipqosconf

L'utilitaire ipqosconf sert à lire le fichier de configuration IPQoS et à configurer les modules IPQoS dans le noyau UNIX. ipqosconf effectue les actions suivantes :

- Il applique le fichier de configuration aux modules du noyau IPQoS (ipqosconf -a *nom-fichier*).
- Il affiche le fichier de configuration IPQoS résidant actuellement dans le noyau (ipqosconf -l).
- Il s'assure que la configuration IPQoS en cours est lue et appliquée à chaque redémarrage de la machine (ipqosconf -c).
- Il vide les modules du noyau IPQoS actuels (ipqosconf -f).

Pour des détails techniques, reportez-vous à la page de manuel ipqosconf(1M).

Glossaire

3DES Voir Triple-DES.

AC Voir autorité de certification (AC).

adresse à usage local Adresse unicast dont la portée du routage est exclusivement locale (au sein du masque de sous-réseau ou d'un réseau d'abonnés). Cette adresse peut également avoir un caractère local ou global.

adresse anycast Adresse IPv6 attribuée à un groupe d'interfaces (appartenant généralement à des nœuds différents). Un paquet envoyé à une adresse anycast est acheminé vers l'interface *la plus proche* possédant cette adresse. La route suivie par le paquet est conforme à la mesure de distance du protocole de routage.

adresse CIDR Classless Inter-Domain Routing, routage interdomaine sans classe. Format d'adresse IPv4 non basé sur les classes de réseau (classe A, B et C). Les adresses CIDR ont une longueur de 32 bits. Elles utilisent le format de notation décimal avec points IPv4 standard en plus d'un préfixe réseau. Ce préfixe définit le numéro de réseau et le masque de réseau.

adresse d'hébergement Adresse temporaire d'un nœud mobile utilisée comme point de sortie du tunnel lorsque le nœud mobile est connecté à un réseau étranger.

adresse de diffusion Adresses réseau IPv4 avec la partie hôte de l'adresse ne comportant que des zéros (10.50.0.0) ou des valeurs à un bit (10.50.255.255). Un paquet envoyé à une adresse de diffusion à partir d'un ordinateur situé sur le réseau local est transmis à tous les ordinateurs reliés au réseau.

adresse de données Adresse IP pouvant servir d'adresse source ou cible de données. Une adresse de données permet l'envoi et la réception de données sur toutes les interfaces du groupe IPMP auquel elle appartient. En outre, le jeu d'adresses de données dans un groupe IPMP peut être utilisé de manière continue à condition qu'une interface du groupe soit en cours de fonctionnement.

adresse de multidiffusion Adresse IPv6 identifiant un groupe d'interfaces d'une manière particulière. Un paquet envoyé à une adresse de multidiffusion est diffusé à toutes les interfaces du groupe. La fonctionnalité de l'adresse de multidiffusion IPv6 est similaire à celle de l'adresse de diffusion IPv4.

adresse de site local (site-local-use) Désignation utilisée pour l'adressage sur un site unique.

adresse de test Adresse IP dans un groupe IPMP à utiliser comme adresse source ou cible de test et non comme adresse source ou cible du trafic des données.

adresse DÉSAPPROUVÉE Adresse IP ne pouvant pas servir d'adresse source pour les données d'un groupe IPMP. En règle générale, les adresses de test IPMP sont DÉSAPPROUVÉES . Toutefois, toute adresse peut être indiquée comme adresse DÉSAPPROUVÉE en vue d'empêcher son utilisation en tant qu'adresse source.

adresse domicile Adresse IP allouée pendant une longue période à un nœud mobile. L'adresse reste identique lorsque le nœud est rattaché à un autre point d'Internet ou du réseau de l'organisation.

adresse lien-local Dans IPv6, désignation utilisée en guise d'adresse d'une liaison simple lors d'une configuration d'adresse automatique, par exemple. Par défaut, l'adresse lien-local est créée à partir de l'adresse MAC du système.

adresse privée Adresse IP impossible à acheminer via le réseau Internet. Les adresses privées peuvent être utilisées par des réseaux internes sur des hôtes n'ayant pas besoin d'établir une connexion Internet. Ces adresses sont définies dans Allocation d'adresses aux Internets privés (`http://www.ietf.org/rfc/rfc1918.txt?number=1918`) et souvent appelées adresses "1918".

adresse unicast Adresse IPv6 identifiant une interface unique sur un nœud IPv6. Le préfixe de site, l'ID du sous-réseau et l'ID de l'interface sont les trois composantes de l'adresse unicast.

AES Standard de chiffrement avancé (Advanced Encryption Standard). Technique de chiffrement de données symétrique par blocs de 128 bits. Le gouvernement des Etats-Unis a adopté la variante Rijndael de l'algorithme comme norme de chiffrement en octobre 2000. AES remplace le chiffrement DES comme norme administrative.

agent de mobilité Agent local ou étranger.

agent étranger Routeur ou serveur du réseau étranger visité par le nœud mobile.

agent local Routeur ou serveur du réseau local d'un nœud mobile.

association de sécurité SA, Security Association. Association définissant les propriétés en matière de sécurité entre un premier hôte et un deuxième hôte.

association de sécurité de la mobilité Ensemble des mesures de sécurité (un algorithme d'authentification, par exemple) comprises entre deux nœuds et appliquées à des messages du protocole IP mobile échangés entre les deux nœuds.

attaque par réflexion Attaque consistant à envoyer à distance des paquets ICMP requête d'écho à une adresse de diffusion IP ou à plusieurs adresses de diffusion dans le but de congestionner le réseau ou de provoquer de graves interruptions de service.

attaque par rejeu Dans IPsec, attaque impliquant la capture d'un paquet par un intrus. Le paquet stocké remplace ou réplique l'original par la suite. Pour se protéger contre ce type d'attaque, il suffit que le paquet contienne un champ qui s'incrémente pendant la durée de vie de la clé secrète assurant la sécurité du paquet.

autorité de certification (AC) Organisation ou société « tiers de confiance » publiant des certificats numériques utilisés pour créer des signatures numériques et des biclés. L'AC garantit l'identité d'une personne ayant reçu un certificat unique.

basculement Processus de rétablissement de l'accès réseau à partir d'une interface défaillante vers une interface physique correcte. L'accès réseau inclut le trafic IPv4 monodiffusion, multidiffusion et diffusion, ainsi que le trafic IPv6 monodiffusion et multidiffusion.

base de données des stratégies de sécurité SPD, Security Policy Database. Base de données définissant le niveau de protection à appliquer à un paquet. La base de données SPD filtre le trafic IP afin de déterminer s'il est nécessaire de rejeter un paquet, de le transmettre en clair ou de le protéger avec IPsec.

Blowfish Algorithme de chiffrement par bloc symétrique de longueur de clé variable (entre 32 et 448 bits). Son créateur, Bruce Schneier, affirme que Blowfish est optimisé pour les applications pour lesquelles la clé n'a pas besoin d'être régulièrement modifiée.

charge utile Données transportées dans un paquet. La charge utile n'inclut pas les informations d'en-tête nécessaires pour amener le paquet à destination.

classe Dans IPQoS, groupe de flux de réseau dotés de caractéristiques identiques. Vous définissez les classes dans le fichier de configuration IPQoS.

comptabilisation des flux Dans IPQoS, processus visant à collecter et à enregistrer les informations sur les flux de trafic. Pour ce faire, il convient de définir les paramètres du module `flowacct` dans le fichier de configuration IPQoS.

compteur Module de l'architecture Diffserv mesurant le débit du trafic d'une classe particulière. L'implémentation IPQoS inclut deux compteurs, `tokenmt` et `tswtclmt`.

configuration automatique Processus selon lequel un hôte configure automatiquement son adresse IPv6 à partir du préfixe de site et des adresses MAX locales.

configuration automatique sans état Processus par lequel un hôte génère ses propres adresses IPv6 en combinant son adresse MAC et un préfixe IPv6 publié par un routeur IPv6 local.

couche liaison Couche située immédiatement sous IPv4/IPv6.

cryptographie par clé asymétrique Système de chiffrement dans lequel l'expéditeur et le destinataire du message utilisent différentes clés pour chiffrer et déchiffrer le message. Les clés asymétriques servent à établir un canal sécurisé pour le chiffrement par clé symétrique. Le protocole Diffie-Hellman est un exemple de protocole de clé asymétrique. Voir aussi cryptographie par clé symétrique.

cryptographie par clé publique Système cryptographique utilisant deux clés différentes : une clé publique connue de tous et une clé privée présentée exclusivement au destinataire du message. IKE fournit des clés publiques à IPsec.

cryptographie par clé symétrique Système de cryptage dans lequel l'expéditeur et le destinataire d'un message partagent une clé unique commune. Cette clé commune sert au chiffrement et au déchiffrement du message. Les clés symétriques permettent de chiffrer l'ensemble de la transmission de données dans IPsec. DES est un exemple de système de cryptographie par clé symétrique.

datagramme Voir datagramme IP.

datagramme IP Paquet d'informations transporté par IP. Un datagramme IP contient un en-tête et des données. L'en-tête inclut les adresses de la source et de la destination du datagramme. Les autres champs de l'en-tête permettent d'identifier et de recombiner les données avec les datagrammes associés lorsqu'ils arrivent à destination.

DES Standard de chiffrement de données (Data Encryption Standard). Méthode de chiffrement à clé symétrique mise au point en 1975 et normalisée par l'ANSI en 1981 car ANSI X.3.92. DES utilise une clé 56 bits.

détection d'un agent Dans un réseau IP mobile, processus selon lequel un nœud mobile détermine s'il a changé de place et indique sa position actuelle ainsi que son adresse d'hébergement sur un réseau étranger.

détection de défaillance Processus de détection intervenant lorsqu'une interface ou le chemin d'une interface vers un périphérique de couche Internet ne fonctionne plus. Le multiacheminement sur réseau IP (IPMP, IP Network Multipathing) inclut deux types de détection de défaillance : l'une utilise les liaisons (par défaut), l'autre les sondes (facultatif).

détection de réparation Processus permettant de déterminer à quel moment une NIC ou le chemin de la carte vers un périphérique de couche 3 est de nouveau fonctionnel après un échec.

détection de routeur Processus selon lequel les hôtes localisent des routeurs résidant sur une liaison directe.

détection des voisins Mécanisme IP permettant à des hôtes de localiser d'autres hôtes résidant sur une liaison directe.

DOI Un DOI (Domain of Interpretation, domaine d'interprétation) définit les formats de données, les types d'échange du trafic réseau ainsi que les conventions d'appellation des informations liées à la sécurité. Les stratégies de sécurité, les algorithmes et les modes cryptographiques sont toutes des informations ayant trait à la sécurité.

double pile Protocole TCP/IP intégrant IPv4 et IPv6 au niveau de la couche réseau, le reste de la pile étant identique. Lorsque vous activez le protocole IPv6 lors de l'installation d'Oracle Solaris, l'hôte reçoit la version double pile du protocole TCP/IP.

DSA Algorithme de signature numérique (Digital Signature Algorithm) Algorithme de clé publique dont la longueur de clé varie de 512 à 4 096 bits. La norme du gouvernement américain, DSS, atteint 1 024 bits. L'algorithme DSA repose sur l'algorithme SHA-1 en entrée.

DSCP DS Codepoint, point de code DS. Valeur de 6 bits qui, si elle figure dans le champ DS d'un en-tête IP, indique le mode de transfert d'un paquet.

en-tête Voir en-tête IP.

en-tête d'authentification En-tête d'extension assurant l'authentification et l'intégrité des datagrammes IP, mais pas leur confidentialité.

en-tête de paquet Voir en-tête IP.

en-tête IP Vingt octets de données identifiant de manière unique un paquet Internet. L'en-tête inclut l'adresse source et l'adresse de destination du paquet. Une partie facultative de l'en-tête permet d'insérer des octets supplémentaires.

encapsulation Processus selon lequel un en-tête et une charge utile sont placés dans le premier paquet, puis insérés dans la charge utile du deuxième paquet.

encapsulation IP-in-IP Mécanisme de mise en tunnel des paquets IP au sein de paquets IP.

encapsulation minimal Forme facultative IPv4 de la mise en tunnel IPv4 prise en charge par les agents locaux, les agents étrangers et les nœuds mobiles. L'encapsulation permet d'économiser 8 ou 12 octets de surcharge par rapport à l'encapsulation IP-in-IP.

enregistrement Processus permettant à un nœud mobile d'enregistrer son adresse d'hébergement auprès de son agent local et de son agent étranger lorsque le nœud en question est hors du système local.

filtrage de paquets Fonction de pare-feu pouvant être configurée pour autoriser ou interdire le transit de paquets particuliers via un pare-feu.

filtre Ensemble de règles définissant les caractéristiques d'une classe dans le fichier de configuration IPQoS. Le système IPQoS sélectionne les flux de trafic conformes aux filtres du fichier de configuration IPQoS en vue de leur traitement. Voir filtrage de paquets.

filtre de paquets dynamique Voir filtre de paquets sans état.

filtre de paquets sans état filtrage de paquets permettant de contrôler l'état des connexions actives et d'identifier, à l'aide des informations obtenues, les paquets du réseau autorisés à franchir le pare-feu. En assurant le suivi et la coordination des requêtes et des réponses, un filtre de paquets sans état a la possibilité d'écarter une réponse non satisfaisante.

gestion des clés La façon dont vous gérez les associations de sécurité.

GRE Generic Routing Encapsulation, encapsulation de routage générique. Forme facultative de mise en tunnel prise en charge par les agents locaux, les agents étrangers et les nœuds mobiles. GRE permet l'encapsulation d'un paquet de protocole de couche réseau dans un paquet de livraison de tout protocole (un autre ou le même) de couche réseau.

groupe anycast Groupe d'interfaces dotées de la même adresse anycast IPv6. L'implémentation du protocole IPv6 dans Oracle Solaris n'est pas compatible avec la création de groupes et d'adresses anycast. Cependant, les nœuds IPv6 Oracle Solaris peuvent assurer le transport du trafic vers des groupes anycast.

groupe IPMP Groupe de multiacheminement sur réseau IP composé d'un jeu d'interfaces réseau et d'un jeu d'adresses de données que le système considère interchangeables afin d'améliorer la disponibilité et l'utilisation. Le groupe IPMP, y compris ses adresses de données et ses interfaces IP sous-jacentes, est représenté par une interface IPMP.

HMAC Méthode de hachage à clé pour l'authentification de messages. HMAC est un algorithme d'authentification à clé secrète. HMAC est utilisé avec une fonction de repère cryptographique répétitive, telle que MD5 ou SHA-1, combinée avec une clé secrète partagée. La puissance cryptographique de HMAC dépend des propriétés de la fonction de repère sous-jacente.

hôte Système qui n'effectue pas le transfert des paquets. Lors de l'installation d'Oracle Solaris, un système est désigné comme hôte par défaut et ne peut plus transmettre de paquets. Un hôte possède généralement une seule interface physique, mais peut également en avoir plusieurs.

hôte multiréseau Système doté de plusieurs interfaces physiques et qui ne traite pas les paquets. Un hôte multiréseau peut exécuter des protocoles de routage.

ICMP Internet Control Message Protocol, protocole Internet des messages de contrôle. Ce protocole sert à gérer les messages d'erreur ainsi que les messages de contrôle des échanges.

ICMP requête d'écho Paquet transmis à une machine sur Internet en vue de solliciter une réponse. De tels paquets sont communément appelés paquets "ping".

identifiant d'accès réseau NAI, Network Access Identifier. Désignation qui identifie de manière unique le nœud mobile sous la forme utilisateur@domaine.

IKE Internet Key Exchange, échange de clé Internet. IKE automatise la mise en service de matériel d'identification authentifié pour les associations de sécurité IPsec.

index du paramètre de sécurité SPI, Security Parameter Index. Nombre entier indiquant la rangée de la SADB qui permettra au récepteur de décrypter un paquet reçu.

interface de réserve Interface physique prévue pour gérer le trafic des données uniquement en cas de défaillance d'une autre interface physique.

interface physique Mode de raccordement d'un système à une liaison. Ce mode de raccordement est souvent mis en œuvre sous la forme d'un pilote de périphérique et d'une NIC. Certaines cartes d'interface réseau (`igb`, par exemple) peuvent disposer de plusieurs points de connexion.

interface réseau virtuelle (VNIC) Pseudo-interface offrant une connectivité réseau virtuelle qu'elle soit ou non configurée sur une interface réseau physique. Conteneurs tels que des zones IP exclusives ou des domaines xVM configurés sur des VNIC afin de former un réseau virtuel.

IP Internet Protocol, protocole Internet. Méthode ou protocole utilisé pour envoyer les données d'un ordinateur à l'autre via Internet.

IP Voir IP, IPv4, IPv6.

IPQoS Fonction logicielle qui permet l'implémentation du modèle Diffserv standard en plus de la comptabilisation des flux et du marquage 802.1 D des réseaux locaux virtuels. À l'aide d'IPQoS, il est possible de fournir différents niveaux de services réseau aux clients et applications, comme indiqué dans le fichier de configuration IPQoS.

IPsec Sécurité IP. Architecture de sécurité assurant la protection des datagrammes IP.

IPv4 Protocole Internet, version 4. IPv4 est parfois appelé IP. Cette version prend en charge un espace d'adressage à 32 bits.

IPv6 Protocole Internet, version 6. IPv6 prend en charge un espace d'adressage à 128 bits.

liaison de mobilité Association d'une adresse locale et d'une adresse d'hébergement, accompagnée de la durée de vie restante de cette association.

liaison IP Utilitaire ou moyen de communication à l'aide duquel les nœuds peuvent communiquer dans la couche liaison. La couche liaison se trouve immédiatement sous IPv4/IPv6. Les réseaux Ethernet (simple ou reliés par un pont) ou les réseaux ATM sont des exemples de liaisons IP. Une liaison IP est définie par un ou plusieurs numéros ou préfixes de masque de sous-réseau IPv4. Un même numéro ou préfixe de masque de sous-réseau IPv4 ne peut pas être attribué à plusieurs liaisons IP. Dans le système ATM LANE, une liaison IP est un LAN à émulation simple. Lorsque vous utilisez le système ARP, la portée du protocole ARP correspond à une liaison IP simple.

liste de révocation de certificats (LRC) Liste des certificats de clés publiques ayant fait l'objet d'une révocation par une AC. Les LRC sont stockées dans la base de données des LRC, gérée par IKE.

MAC MAC garantit l'intégrité des données et authentifie leur origine. MAC ne protège aucunement contre l'écoute frauduleuse des informations échangées.

marqueur 1. Module de l'architecture diffserv et IPQoS attribuant une valeur au champ DS d'un paquet IP. Cette valeur indique la manière dont est traité le paquet. Dans l'implémentation IPQoS, le module du marqueur est `dscpmk`.

2. Module dans l'implémentation IPQoS qui marque l'indicateur de réseau local virtuel d'un datagramme Ethernet par une valeur de priorité utilisateur. La valeur de priorité utilisateur indique comment les datagrammes sont transmis sur un réseau comportant des périphériques VLAN. Ce module est appelé `dlcosmk`.

MD5 Fonction de hachage cryptographique répétitive utilisée pour authentifier les messages, y compris les signatures numériques. Elle a été développée en 1991 par Rivest.

migration d'adresse Processus consistant à déplacer une adresse d'une interface réseau à l'autre. La migration d'adresse se produit dans le cadre d'un basculement en cas de défaillance d'une interface ou dans le cadre d'un rétablissement lors de la réparation d'une interface.

modèle Diffserv Norme d'architecture du groupe IETF (Internet Engineering Task Force, groupe d'étude d'ingénierie Internet) destinée à l'implémentation de services différenciés sur les réseaux IP. Les modules principaux comprennent la classification, la mesure, le marquage, l'ordonnancement et le rejet. IPQoS implémente les modules de classification, de mesure et de marquage. Le modèle Diffserv est décrit dans le document RFC 2475, *An Architecture for Differentiated Services*.

monter Action d'ouvrir un périphérique associé à un nom d'interface physique. Lorsqu'une interface est montée, les flux sont configurés de manière à ce que le protocole IP puisse utiliser le périphérique. Pour monter une interface au cours d'une session d'un système, il convient d'exécuter la commande `ifconfig`.

MTU Maximum Transmission Unit, unité de transmission maximale. Taille, exprimée en octets, des données pouvant être transmises via une liaison. Ainsi, la MTU d'une liaison Ethernet est de 1 500 octets.

nœud Dans IPv6, tout système IPv6, qu'il s'agisse d'un hôte ou d'un routeur.

nœud mobile Hôte ou routeur pouvant remplacer son point de jonction à un réseau par un autre tout en conservant la totalité des communications existantes à l'aide de son adresse IP domicile.

NAT Voir traduction d'adresses réseau.

NIC Network Interface Card, carte d'interface réseau. Carte réseau jouant le rôle d'interface d'un réseau. Certaines NIC ont plusieurs interfaces physiques. C'est le cas des cartes `igb`.

nom du keystore Nom qu'un administrateur attribue à une zone de stockage, ou keystore, sur une NIC. Le nom du keystore est également appelé jeton ou ID de jeton.

paquet Groupe d'informations transmis sous forme d'une unité sur les lignes de communications. Un paquet contient un en-tête IP et une charge utile.

pare-feu Dispositif ou logiciel prévu pour isoler le réseau privé ou le réseau intranet d'une organisation d'Internet, afin de le protéger contre d'éventuelles intrusions. Un pare-feu peut inclure le filtrage de paquets, des serveurs proxy et les valeurs NAT (Network Address Translation, translation d'adresse réseau).

périphérique VLAN Interface réseau permettant de renvoyer le trafic vers le niveau Ethernet (liaison de données) de la pile de protocole IP.

PFS Perfect Forward Secrecy, secret rigoureux des transmission .Avec la fonction PFS, la clé visant à protéger la transmission des données n'est pas utilisée pour dériver d'autres clés. Il en est de même pour la source de la clé.

PFS s'applique à l'échange de clés authentifiées uniquement. Voir aussi protocole Diffie-Hellman.

PHB Per-Hop Behavior, comportement par saut. Priorité accordée à une classe de trafic. Le comportement par saut indique la priorité des flux de cette classe par rapport aux autres classes de trafic.

pile Voir pile IP.

pile de protocole Voir pile IP.

pile IP TCP/IP est souvent appelé une "pile". Ce terme fait référence aux couches (TCP, IP et parfois d'autres) par lesquelles transitent toutes les données aux extrémités client et serveur d'un échange de données.

PKI Public Key Infrastructure, infrastructure de clé publique. Système de certificats numériques, d'autorités de certification et d'autres autorités d'enregistrement prévu pour vérifier et authentifier la validité de chaque partie impliquée dans une transaction Internet.

pool d'adresses Dans un système IP mobile, ensemble d'adresses désignées par l'administrateur du réseau domestique afin d'être utilisées par les nœuds mobiles qui nécessitent une adresse domicile.

priorité utilisateur Valeur de 3 bits ayant pour effet de mettre en œuvre des marqueurs de classe de services, qui définissent la façon dont les datagrammes Ethernet sont transférés sur un réseau de périphériques VLAN.

protocole de transport de contrôle de flux SCTP, Stream Control Transport Protocol. Protocole de la couche transport assurant des communications orientées connexion sous une forme similaire au protocole TCP. De plus, SCTP gère les multiréseaux (une des extrémités de la connexion peut être associée à plusieurs adresses IP).

protocole Diffie-Hellman Également appelé chiffrement par clé publique. Protocole d'accord de clés cryptographiques asymétriques mis au point par Diffie et Hellman en 1976. Ce protocole permet à deux utilisateurs d'échanger une clé secrète via un moyen non sécurisé sans secrets préalables. Diffie-Hellman est utilisé par le protocole IKE.

protocole ESP Encapsulating Security Payload, association de sécurité. Extension de l'en-tête assurant l'intégrité et la confidentialité des datagrammes. ESP est l'un des cinq composants de l'architecture de sécurité IP (IPsec).

publication d'un agent Dans un réseau IP mobile, message envoyé à intervalles réguliers à des agents locaux et étrangers pour publier leur présence lors d'un lien direct.

publication des voisins Réponse à un message de sollicitation de voisinage ou processus selon lequel un nœud envoie des publications de voisinage non sollicitées pour signaler une modification de l'adresse de couche liaison.

publication du routeur Processus selon lequel les routeurs annoncent leur présence (avec divers paramètres de connexion et paramètres Internet) de façon périodique ou en réponse à un message de sollicitation d'un routeur.

reconfiguration dynamique Fonction permettant de reconfigurer un système en cours d'exécution sans incidence ou presque sur les opérations en cours. La reconfiguration dynamique n'est pas prise en charge par toutes les plates-formes Sun. Certaines plates-formes Sun ne prennent en charge que la reconfiguration dynamique de certains types de matériel comme les NIC.

redirection Dans un routeur, technique permettant de signaler à un hôte le meilleur nœud (prochain saut) en vue d'atteindre une destination particulière.

reniflage Action d'espionner les communications des réseaux informatiques. Cette technique est fréquemment employée avec des programmes automatisés pour extirper hors ligne des informations telles que des mots de passe en clair.

répartition de charge Processus consistant à distribuer le trafic entrant et sortant au sein d'un groupe d'interfaces. La répartition de charge permet d'augmenter le rendement. Elle ne se produit que lorsque le trafic réseau se dirige vers plusieurs destinations utilisant plusieurs connexions. Il existe deux types de répartition de charge : la répartition de charge entrante pour le trafic entrant et la répartition de charge sortante pour le trafic sortant.

réseau étranger Tout réseau autre que le réseau domestique du nœud mobile.

réseau local Réseau qui possède un préfixe réseau correspondant au préfixe réseau de l'adresse domicile d'un nœud mobile.

réseau virtuel Regroupement de ressources et fonctionnalités réseau logicielles et matérielles gérées en tant qu'entité logicielle unique. Un réseau virtuel *interne* regroupe les ressources réseau sur un seul système, parfois appelé "réseau en boîte".

résultat Action à réaliser à l'issue de la mesure du trafic. Les compteurs IPQoS aboutissent à trois résultats signalés par la couleur rouge, jaune et verte. Vous définissez ces codes couleur dans le fichier de configuration IPQoS.

rétablissement Processus de restauration de l'accès réseau pour une interface en cas de détection de sa réparation.

routeur Système généralement composé de plusieurs interfaces ayant pour fonction d'exécuter des protocoles de routage et de transférer des paquets. Vous pouvez configurer un système à une seule interface en guise de routeur à condition que le système se trouve à l'extrémité d'une liaison PPP.

RSA Méthode permettant d'obtenir des signatures numériques et des systèmes de cryptographie par clé publique. Cette méthode qui date de 1978 a été décrite par trois développeurs (Rivest, Shamir et Adleman).

SA Voir association de sécurité.

SADB Security Associations Database, base de données des associations de sécurité. Table définissant les clés cryptographiques et les algorithmes cryptographiques. Les clés et les algorithmes ont pour intérêt de sécuriser la transmission des données.

saut Mesure permettant l'identification du nombre de routeurs séparant deux hôtes. Si trois routeurs séparent une source et une destination, les hôtes se trouvent à quatre sauts l'un de l'autre.

SCTP Voir protocole de transport de contrôle de flux.

sélecteur Élément définissant de façon spécifique les critères à appliquer aux paquets d'une classe particulière en vue de sélectionner ce trafic dans le flux du réseau. Vous définissez les sélecteurs dans la clause de filtrage du fichier de configuration IPQoS.

serveur proxy Serveur faisant l'interface entre une application client (telle qu'un navigateur Web) et un autre serveur. Ce type de serveur permet de filtrer les requêtes afin d'interdire l'accès à certains sites Web, par exemple.

SHA-1 Secure Hashing Algorithm, algorithme de hachage sécurisé. L'algorithme s'applique à toute longueur d'entrée inférieure à 2^{64} afin d'obtenir une synthèse des messages. L'algorithme SHA-1 sert d'entrée à l'algorithme DSA.

signature numérique Code numérique associé à un message électronique qui identifie l'expéditeur de manière unique.

sollicitation des voisins Sollicitation envoyée par un nœud afin de déterminer l'adresse de couche liaison d'un voisin. Une telle sollicitation consiste à vérifier qu'un voisin est toujours accessible par une adresse de couche liaison mise en cache.

sollicitation du routeur Processus selon lequel les hôtes demandent à des routeurs de générer immédiatement des publications du routeur, et non pas lors de la prochaine exécution programmée.

SPD Voir base de données des stratégies de sécurité.

SPI Voir index du paramètre de sécurité.

table de liaison Dans un réseau IP mobile, table d'agents locaux associant une adresse domicile à une adresse d'hébergement et indiquant notamment la durée de vie restante et le temps accordé.

TCP/IP Transmission Control Protocol/Internet Protocol, protocole de contrôle de la transmission/protocole Internet. TCP/IP est le langage de communication ou protocole de base sur Internet. Il peut également servir de protocole de communication sur un réseau privé (intranet ou extranet).

traduction d'adresses réseau NAT, Network Address Translation. Traduction d'une adresse IP utilisée au sein d'un réseau sous une adresse IP différente connue au sein d'un autre réseau. Cette technique sert à limiter le nombre d'adresses IP globales nécessaires.

Triple-DES Triple-Data Encryption, triple chiffrement des données. Méthode de chiffrement par clé symétrique. Elle nécessite une clé de 168 bits. L'abréviation de Triple-DES est 3DES.

tunnel Chemin suivi par un datagramme pendant son encapsulation. Voir encapsulation.

tunnel bidirectionnel Tunnel pouvant transmettre des datagrammes dans les deux directions.

tunnel de transfert Tunnel partant de l'agent local et aboutissant à l'adresse d'hébergement du nœud mobile.

tunnel inverse Tunnel débutant à l'adresse d'hébergement du nœud mobile et se terminant au niveau de l'agent local.

usurpation Action d'accéder par intrusion à un ordinateur en envoyant un message avec une adresse IP provenant prétendument d'un hôte de confiance. Pour ce faire, un pirate doit d'abord utiliser différentes techniques pour identifier l'adresse IP d'un hôte fiable, puis modifier les en-têtes de paquets pour donner l'impression que les paquets proviennent de cet hôte.

valeur de hachage Nombre généré à partir d'une chaîne de texte. Les fonctions de hachage garantissent que les messages transmis n'ont pas été sabotés. MD5 et SHA-1 sont des exemples de fonctions de hachage unidirectionnel.

VPN Virtual Private Network, réseau privé virtuel. Réseau logique sécurisé utilisant des tunnels dans un réseau public tel qu'Internet.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z