Bull

AIX 4.3 Guide de gestion du système Communications et réseaux

REFERENCE
86 F2 31JX 02

Bull

Bull

AIX 4.3 Guide de gestion du système Communications et réseaux

Logiciel

Octobre 1999

BULL ELECTRONICS ANGERS
CEDOC
34 Rue du Nid de Pie – BP 428
49004 ANGERS CEDEX 01
FRANCE

REFERENCE
86 F2 31JX 02

Imprimé en France

Vos suggestions sur la forme et le fond de ce manuel seront les bienvenues. Une feuille destinée à recevoir vos remarques se trouve à la fin de ce document.

Pour commander d'autres exemplaires de ce manuel ou d'autres publications techniques Bull, veuillez utiliser le bon de commande également fourni en fin de manuel.

Marques déposées

Toutes les marques déposées sont la propriété de leurs titulaires respectifs.

AIX® est une marque déposée d'IBM Corp. et est utilisée sous licence.

UNIX est une marque déposée licenciée exclusivement par X/Open Company Ltd.

An 2000

Le produit documenté dans ce manuel est agréé pour l'An 2000.

A propos de ce manuel

Ce manuel s'adresse aux administrateurs système AIX qui gèrent les connexions du système au réseau. Pour aborder ce manuel, il est recommandé de bien connaître le système d'exploitation de base (BOS), ainsi que les points traités dans les manuels *AIX 4.3 Guide d'administration : système d'exploitation et unités* et *AIX 4.3 Guide de l'utilisateur : communications et réseaux*.

A qui s'adresse ce manuel ?

Ce manuel s'adresse aux administrateurs système effectuant les tâches de gestion du système impliquant des communications dans un réseau.

Mode d'emploi du manuel

Chaque chapitre, structuré généralement de façon identique, commence par des informations d'ordre général, puis continue par des informations relatives à l'installation et à la configuration, la maintenance et la détection des incidents, puis conclut par des informations de référence. Les informations concernant les procédures se trouvent près des informations conceptuelles correspondantes pour un accès plus facile.

Conventions typographiques

Les conventions typographiques suivantes sont utilisées dans ce manuel :

Gras	Commandes, mots-clés, fichiers, répertoires et autres éléments dont le nom est prédéfini par le système.
Italique	Paramètres dont le nom ou la valeur est fourni par l'utilisateur.
`Espacement fixe`	Exemples (valeurs spécifiques, texte affiché, code programme), messages système ou données entrées par l'utilisateur.

ISO 9000

Ce produit répond aux normes qualité ISO 9000.

Prise en charge AIX pour X/Open UNIX95 Specification

AIX est conçu pour prendre en charge la X/Open UNIX95 Specification permettant la portabilité de systèmes basés sur UNIX. Plusieurs interfaces nouvelles ont été ajoutées, et d'autres améliorées, pour respecter cette spécification. AIX 4.3 est encore plus ouvert et plus portable au niveau des applications.

Dans le même temps, la compatibilité avec les versions antérieures d'AIX est préservée. Ceci est possible grâce à la création d'une nouvelle variable d'environnement, qui permet de définir l'environnement pour chaque système, utilisateur ou processus.

Pour déterminer comment développer une application portable UNIX95, vous pouvez avoir besoin de vous reporter à la X/Open UNIX95 Specification.

Bibliographie

Les manuels suivants complètent la documentation sur les communications.

AIX - Bibliographie, CEDOC 86 F2 71WE.

AIX 4.3 Guide d'administration : système d'exploitation et unités, CEDOC 86 F2 99HX.

AIX 4.3 Guide de l'utilisateur : communications et réseaux, CEDOC 86 F2 98HX.

AIX General Programming Concepts : Writing and Debugging Programs, CEDOC 86 A2 34JX.

AIX Commands Reference, CEDOC 86 A2 38JX à 86 A2 43JX.

AIX 4.3 Guide d'installation, CEDOC 86 F2 43GX.

La section TTY Subsystem Overview du manuel *AIX General Programming Concepts : Writing and Debugging Programs* donne des informations d'ordre général sur les disciplines de ligne et le code tty.

Voir aussi les documentations suivantes :

Token–Ring Network Architecture Reference, référence SC30–3374.

Albitz, Paul and Liu, Cricket, [1992], *DNS and BIND in a Nutshell*, O'Reilly & Associates, Inc., Sebastopol, CA, ISBN 0–56592–010–4.

Comer, Douglas E., [1991], *Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architectures*, Prentice Hall, Englewood Cliffs, NJ, ISBN 0–13–468505–9.

Comer, Douglas E. and Stevens, David L., [1991], *Internetworking with TCP/IP, Volume II: Design, Implementation, and Internals*, Prentice Hall, Englewood Cliffs, NJ, ISBN 0–13–472242–6.

Costales, Bryan, Eric Allman, and Neil Rickert, *sendmail*, O'Reilly & Associates, Inc., Sebastopol, CA, 1993.

Hunt, Craig, [1992], *TCP/IP Network Administration*, O'Reilly & Associates, Inc., Sebastopol, CA, ISBN 0–93–717582–X.

Stern, Hal, [1991], *Managing NFS and NIS*, O'Reilly & Associates, Inc., Sebastopol, CA, ISBN 0–93–717575–7.

Stevens, Richard W., [1990], *UNIX Network Programming*, Prentice Hall, Englewood Cliffs, NJ, ISBN 0–13–949876–1.

Tanenbaum, Andrew S., *Computer Networks*, Prentice Hall, Englewood Cliffs, NJ, ISBN 0–13–165183–8.

Vanel, Laurent, Steve Gardner, Praben Prima, Simon Robertson, and Oreste Villari, *AIX and Windows NT: Solutions for Interoperability*, International Business Machines, Inc. http://www.redbooks.ibm.com

Commande de manuels

Pour commander ce manuel, adressez–vous à Bull Electronics Angers S.A. CEDOC, dont l'adresse figure à la fin de ce manuel.

Pour commander d'autres exemplaires de ce manuel, précisez la référence 86 F2 31JX.

Si vous disposez de la brochure *AIX - Bibliographie*, consultez-la pour savoir comment vous procurer les publications qui vous intéressent.

Table des matières

Chapitre 1. Communications et réseaux : généralités

Ce chapitre présente les concepts de base pour la compréhension des systèmes en réseau. Il est destiné à l'administrateur système peu familiarisé avec les réseaux. Ceux qui maîtrisent déjà ces concepts sous UNIX peuvent passer directement au chapitre suivant.

Un réseau est la combinaison d'un ou plusieurs ordinateurs interconnectés. Le réseau *physique* regroupe les éléments matériels du réseau (cartes, câbles, concentrateurs, lignes téléphoniques, etc). Quant au réseau *logique*, il comporte les éléments logiciels et le modèle conceptuel du réseau.

Les concepts présentés sont les suivants :

Fonctions de communication

Les réseaux offrent diverses fonctions de communication dédiées aux applications et aux utilisateurs, notamment :

- Envoi de courrier électronique.
- Emulation d'un terminal ou connexion à un autre ordinateur.
- Transfert de données.
- Exécution de programmes résidant sur un noeud distant.

L'application de réseau la plus répandue est la messagerie électronique (e–mail). Elle permet à deux utilisateurs de se transmettre des messages, sur le même système (auquel cas, le réseau n'est pas nécessaire), sur deux sites différents ou à travers le monde.

Un réseau de communication permet également à un système d'en simuler un autre de façon à accéder aux informations comme s'il était un autre type d'ordinateur ou de terminal. La connexion par le réseau à un système distant donne accès aux mêmes programmes et fichiers qu'avec une connexion locale sans réseau.

Les données sont transférables par le réseau d'un système à un autre, qu'il s'agisse de fichiers, de répertoires ou de systèmes de fichiers complets. Elles peuvent être sauvegardées à distance et dupliquées sur plusieurs machines pour parer aux défaillances matérielles.

Plusieurs protocoles ont été établis pour permettre aux applications et aux utilisateurs d'un système d'appeler des procédures et des applications d'un autre système. Ce dispositif est très utile dans certains environnements, notamment pour alléger la charge des routines particulièrement lourdes des applications scientifiques et techniques.

Présentation des réseaux

La complexité des réseaux informatiques modernes a donné lieu à plusieurs modèles conceptuels de réseaux. Le plus connu est le modèle de référence pour l'interconnexion des systèmes ouverts (OSI) proposé par l'organisation internationale de normalisation (ISO), aussi appelé modèle OSI en sept couches. Ces couches sont numérotées à partir du niveau le plus bas (physique).

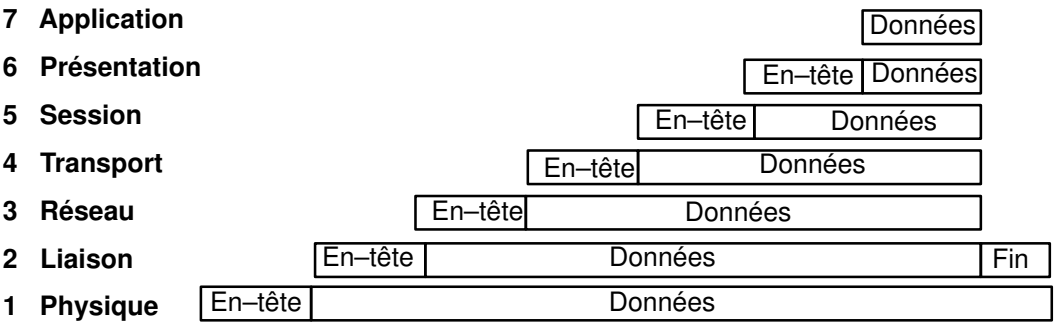
7	Application
6	Présentation
5	Session
4	Transport
3	Réseau
2	Liaison
1	Physique

Les niveaux 1 à 3 sont propres aux réseaux et varient en fonction du réseau physique utilisé. Les niveaux 4 à 7 couvrent les fonctions de haut niveau, indépendantes du réseau. Chacune de ces couches décrit une fonction de communication spécifique et non un protocole donné. Elle fonctionne comme suit :

Physique	Décrit le support physique du réseau (par exemple, le câble à fibre optique requis pour un réseau FDDI).
Liaison	Assure la transmission des données à travers la couche physique (qui, par nature, n'est pas fiable).
Réseau	Gère les connexions aux autres machines du réseau.
Transport	Assure l'acheminement des données sans erreur.
Session	Gère les connexions entre les applications.
Présentation	Met en forme les données pour les rendre cohérentes vis-à-vis des applications.
Application	Englobe les applications qui utilisent le réseau.

Le modèle de référence OSI, utile pour la présentation conceptuelle, n'est en pratique pas toujours scrupuleusement suivi par les protocoles de réseau. Par exemple, lors de la discussion du protocole TCP/IP, les fonctions Application et Présentation peuvent être combinées à un niveau unique, de même que les couches Session et Transport, ainsi que les couches Liaison et Physique.

Chaque couche du modèle OSI communique avec la couche équivalente sur la machine distante (cf. figure Modèle de référence OSI). Elle transmet les données uniquement aux couches situées immédiatement au-dessus ou au-dessous d'elle. Chaque couche encapsule les informations héritées des couches supérieures et ajoute ses propres informations d'en-tête (et de fin pour la couche Liaison).



Les réseaux offrent nombre de possibilités aux entreprises et aux particuliers. Par exemple :

- Entrée de données,
- Recherche de données,
- Soumission par lots à distance,
- Partage des ressources,
- Partage des données,
- Courrier électronique.

L'entrée des données se fait directement dans des fichiers de données locaux ou distants, ce qui permet de réduire les étapes intermédiaires de type postage, enregistrement et validation. Par là-même, les risques d'échec ou d'erreur liés à un transfert en plusieurs étapes sont réduits. La recherche des données consiste à examiner des fichiers de données pour obtenir des informations particulières. Leur mise à jour consiste à modifier, ajouter ou supprimer des informations stockées dans des fichiers locaux ou distants. La soumission par lots à distance consiste à entrer à distance des trains de données traités le plus souvent durant la nuit ou une période de faible activité. Pour toutes ces fonctions, les communications et réseaux se révèlent non seulement souhaitables mais aussi indispensables.

Les réseaux autorisent également le partage des ressources : données, programmes, espace de stockage et périphériques (tels que les imprimantes, les modems, les terminaux et les disques inamovibles). Cette particularité accroît à la fois la rentabilité du système (périphériques partagés) et sa fonctionnalité (une seule copie des programmes et fichiers, évitant ainsi tout problème de cohérence inhérent aux copies multiples).

Les réseaux offrent enfin un outil de communication par courrier électronique (ou "e–mail"). Les utilisateurs peuvent correspondre au sein d'un même système ou à travers le monde.

Réseaux physiques

Le réseau physique est constitué par l'ensemble des câbles (coaxiaux, à paire torsadée, optiques ou téléphoniques) qui relient les unités matérielles, les cartes des systèmes hôtes raccordés et les éventuels concentrateurs, répéteurs, routeurs et ponts utilisés sur le réseau. (Le terme *hôte* est employé dans le sens d'ordinateur connecté au réseau.)

Les réseaux physiques varient en fonction de leur taille et du type de matériel qui les composent. On distingue généralement les *réseaux locaux* (LAN) des *réseaux longue distance* (WAN). Un réseau local couvre une zone géographiquement réduite (1 à 10 km), comme par exemple un immeuble de bureaux, un entrepôt, un campus, par opposition au réseau longue distance qui dessert une zone plus vaste (pays, continent, etc.). On assiste également à l'émergence d'un nouveau type de réseau, modèle intermédiaire appelé *réseau métropolitain* (MAN). Dans ce guide, les réseaux MAN sont généralement englobés dans les réseaux WAN.

Les réseaux locaux utilisent généralement des équipements Ethernet standard, IEEE 802.3 ou en anneau à jeton, et les réseaux longue distance et asynchrones utilisent les moyens de communication fournis par les entreprises de télécommunications. Dans les deux cas, les opérations effectuées sur le réseau physique sont généralement soumises à des normes de communications réseau telles que EIA 232D ou CCITT V.35.

Support de communication

Toute communication sur un réseau requiert un support matériel et logiciel. *Le matériel* est l'équipement physique connecté au réseau physique. *Le logiciel* regroupe les programmes et les pilotes de périphérique utilisés pour l'exploitation d'un système.

L'équipement matériel d'un système comprend les cartes et autres dispositifs qui donnent accès ou font office d'interface entre la partie logicielle du système et le réseau physique. Chacune de ces cartes doit être installée à un emplacement de carte d'entrée/sortie (E/S) sur le système. D'autres dispositifs, tels que les modems, peuvent être raccordés à un port standard de l'ordinateur.

Ces cartes sont compatibles avec les normes du réseau physique (par exemple, EIA 232D, Smartmodem, V.25 bis, EIA 422A, X.21 ou V.35) et avec les *protocoles* utilisés (par exemple, les protocoles SDLC, HDLC et bisynchrones). Le support logiciel, s'il n'est pas intégré à la carte, est fourni par le pilote de la carte.

Protocoles

Tout logiciel de communication fait appel à un *protocole* (ou plusieurs), ensemble de règles sémantiques et syntaxiques qui définissent comment les unités fonctionnelles assurent la communication : livraison de l'information, conditionnement des données pour en assurer l'intégrité jusqu'à destination, et chemin d'accès. Les protocoles se chargent également de coordonner le flux de messages et leur acquittement.

Les protocoles interviennent à différents niveaux du noyau et ne peuvent être manipulés directement. Leur activation s'effectue en fonction des programmes sollicités par l'utilisateur au niveau de l'interface de programmation d'application (API) lors de l'exécution des tâches (transfert de fichiers, connexion à distance, émulation de terminal, etc.).

Adresses

Les réseaux de communication ont une troisième caractéristique commune : la notion d'*adresse*. Les adresses, associées à la fois au logiciel et au matériel, indiquent à la station expéditrice ou au poste de contrôle comment identifier la station destinataire : elles permettent de localiser les emplacements de stockage et de réception. Une adresse physique est un code unique attribué à chaque unité ou station connectée à un réseau.

Par exemple, sur un réseau en anneau à jeton, la commande **netstat –iv** affiche l'adresse de la carte dédiée à ce type de réseau. Il s'agit de l'adresse physique. La commande **netstat –iv** procure également des informations d'adressage au niveau de l'utilisateur et de la classe. Les adresses sont souvent définies par le logiciel, mais il arrive qu'elles soient créées également par l'utilisateur.

Domaines

Liée au concept d'adresse, la notion de *domaine* est commune à un grand nombre de réseaux de communication. La structure d'Internet, par exemple, illustre comment les domaines définissent l'adresse IP (Internet Protocol). Internet est un réseau extensif qui regroupe de nombreux réseaux de moindre envergure. Les adresses Internet sont structurées hiérarchiquement en domaines pour faciliter le routage et l'adressage. Au sommet de la structure se trouvent les catégories les plus générales, par exemple `com` pour le secteur commercial, `edu` pour le secteur de l'enseignement et `gov`.

Le domaine `com` est divisé en domaines plus restreints correspondant aux entreprises individuelles, `ibm`, par exemple. Ce domaine `ibm.com` est à son tour divisé en sous-domaines qui, cette fois, correspondent aux adresses Internet des divers sites, par exemple `austin.ibm.com` ou `raleigh.ibm.com`. C'est à ce niveau que commencent à apparaître le nom des *hôtes*. Dans ce contexte, les hôtes sont les ordinateurs connectés au réseau. Par exemple, le domaine `austin.ibm.com` peut comporter les systèmes `hamlet` et `lear`, aux adresses respectives `hamlet.austin.ibm.com` et `lear.austin.ibm.com`.

Passerelles et ponts

Le réseau Internet regroupe une grande variété de réseaux faisant intervenir divers matériels et logiciels.*La communication entre ces réseaux hétérogènes s'effectue par le* biais de *passerelles* et de *ponts.* Un pont est une unité fonctionnelle qui relie deux réseaux locaux pouvant utiliser la même procédure de contrôle de liaison logique (LLC), Ethernet par exemple, mais des procédures de contrôle d'accès au support (MAC) différentes. La passerelle, quant à elle, couvre un champ plus large : elle intervient au-dessus de la couche Liaison et assure, s'il y a lieu, la conversion des protocoles et des interfaces pour permettre à deux protocoles de communiquer entre eux. Elle permet le transfert des données à travers les divers réseaux qui composent Internet.

Routage

L'utilisation de noms de domaines pour l'adressage et de passerelles pour le transfert facilite grandement le *routage*, opération qui consiste à définir le parcours d'un message jusqu'à sa destination. En effet, c'est le nom du domaine qui définit la destination : dans un réseau étendu comme Internet, l'information est acheminée d'un réseau de communication au suivant jusqu'à destination. Chacun des réseaux vérifie le nom du domaine en fonction de ceux qu'il connaît et achemine l'information, jusqu'à l'extrémité logique suivante. Ainsi, chaque réseau par lequel les données transitent participe au processus de routage.

Noeud local et noeud distant

Un réseau physique est utilisé par les systèmes hôtes qui y résident. Chacun de ces systèmes hôtes peut être considéré comme un *noeud* sur le réseau. C'est-à-dire un point adressable du réseau qui offre des services de traitement hôte. L'intercommunication entre ces différents noeuds engendre les notions de *local* et de *distant*. *Local* s'applique aux unités, fichiers ou systèmes directement accessibles à partir de votre système, sans recourir à une ligne de communication. *Distant* s'applique aux unités, fichiers ou systèmes accessibles à partir de votre système via une ligne de communication. En effet, les fichiers locaux sont implantés sur votre système alors que les fichiers distants résident sur un serveur de fichiers ou un autre noeud accessible via un réseau physique, par exemple, un réseau Ethernet, un réseau en anneau à jeton ou des lignes téléphoniques.

Serveur et client

Le concept de *client-serveur* est lié aux notions de "local" et de "distant". Un serveur est un ordinateur qui fournit des données et services aux autres ordinateurs du réseau. Les types de serveur les plus courants sont les serveurs de fichiers dans lesquels sont stockés des fichiers, les serveurs de noms, qui stockent les noms et adresses, et les serveurs de code qui stockent les programmes et applications.

Un client est un ordinateur qui sollicite des services ou des données auprès d'un serveur. Par exemple, un client peut demander un code de programme mis à jour ou une application auprès d'un serveur de code. Pour obtenir un nom ou une adresse, le client contacte un serveur de noms. Un client peut également interroger un serveur de fichiers pour retrouver des fichiers et des données, et effectuer des opérations (saisie de données, recherches, mise à jour d'articles).

Communication avec d’autres systèmes d’exploitation

Un réseau peut relier divers types d’ordinateurs (modèles ou constructeurs hétérogènes). Des programmes de communication sont alors utilisés pour pallier les disparités entre les systèmes d’exploitation installés sur ces machines.

Certains programmes peuvent nécessiter la présence sur le réseau d’un autre programme ou de protocoles de connexion (tels que TCP/IP ou SNA).

Avec les versions d’AIX 4.3.2 et ultérieures, par exemple, AIX Fast Connect for Windows permet aux clients PC d’accéder aux fichiers et aux imprimantes AIX à l’aide du logiciel réseau du client PC natif. Les utilisateurs PC peuvent accéder directement aux sytèmes de fichiers distants à partir de leurs machines comme si ces fichiers étaient sauvegardés en local. De plus, ils peuvent lancer des tâches d’impression sur des imprimantes utilisant le système de spoulage, visualiser celles qui sont disponibles et configurer une imprimante en réseau.

Chapitre 2. Messagerie électronique

La messagerie fournit un outil d'échange du courrier électronique entre les utilisateurs d'un même système ou de systèmes distincts connectés via un réseau. Ce chapitre décrit le système de messagerie et l'interface utilisateur.

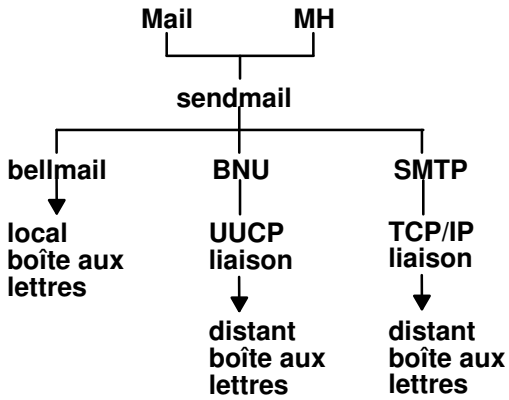
La messagerie fournit un outil d'échange du courrier électronique (e–mail) entre les utilisateurs d'un même système ou de systèmes distincts connectés via un réseau. Ce chapitre décrit le système de messagerie, l'interface utilisateur standard, et les protocoles IMAP (Internet Message Access Protocol) et POP (Post Office Protocol).

La messagerie, outil de livraison de messages interréseau, comprend une interface utilisateur, un programme de routage et un programme de livraison des messages (aussi appelé programme facteur). L'acheminement des messages est assuré entre deux utilisateurs d'un même système hôte ou de systèmes hôtes ou réseaux différents. L'outil comporte également une fonction d'édition limitée pour présenter les en-têtes dans un format reconnu par l'hôte récepteur.

Une *interface utilisateur* permet aux utilisateurs de créer, envoyer et recevoir des messages. La messagerie propose deux interfaces : **mail** et **mhmail**. La commande **mail** est l'interface utilisateur standard des systèmes UNIX. La commande **mhmail** est l'interface utilisateur du gestionnaire de message (MH). Plus évoluée, cette dernière s'adresse aux utilisateurs chevronnés.

Un *programme de routage des messages* sert à acheminer les messages jusqu'à destination. Dans la messagerie présentée ici, il s'agit du programme **sendmail**. Cette commande, intégrée au système d'exploitation de base (BOS), est installée avec ce dernier. Il s'agit d'un démon qui utilise les informations des fichiers **/etc/sendmail.cf**, **/etc/aliases** et **/etc/sendmail.nl** pour effectuer le routage.

En fonction de la route, la commande **sendmail** fait appel à différents *programmes facteur* pour livrer les messages.



Comme l'illustre la figure :

- Pour acheminer un courrier local, le programme **sendmail** achemine les messages au programme **bellmail**. Ce dernier transmet le courrier au système local, dans la boîte aux lettres système de l'utilisateur, située dans le répertoire **/varspool/mail**.
- Pour acheminer le courrier via une liaison réseau UUCP, le programme **sendmail** achemine les messages à l'aide de BNU (Basic Network Utilities).
- Pour transmettre un courrier via TCP/IP, la commande **sendmail** établit une connexion TCP/IP au système distant et utilise le protocole SMTP (Simple Mail Transfer Protocol) pour effectuer le transfert.

Gestion du courrier

L'administrateur du courrier est responsable de l'exécution des tâches suivantes :

1. Pour que **sendmail** soit exécuté à l'amorçage du système, configurez le fichier **/etc/rc.tcpip** comme suit. Reportez-vous aux instructions suivant immédiatement cette liste.
2. Personnaliser le fichier de configuration **/etc/sendmail.cf**. Par défaut, il est défini pour permettre la livraison du courrier local. Ce fichier doit être modifié et recompilé pour pouvoir acheminer le courrier via une liaison TCP/IP ou BNU. Pour en savoir plus, reportez-vous à "sendmail.cf File" dans le document *AIX Files Reference*.
3. Définir les alias aux niveaux système et domaine dans le fichier **/etc/aliases.** Pour en savoir plus, reportez-vous à "Gestion des alias", page 2-3.
4. Gérer les files d'attente de messages. Pour le détail, reportez-vous à "Gestion des fichiers et répertoires de file d'attente courrier", page 2-7.
5. Gérer le journal des messages. Gérer les files d'attente de messages. Pour en savoir plus, reportez-vous à "Gestion de la journalisation", page 2-12.

Configuration du fichier /etc/rc.tcpip pour lancer le démon sendmail

Pour que **sendmail** soit exécuté à l'amorçage du système, configurez le fichier **/etc/rc.tcpip** comme suit :

1. Modifiez le fichier **/etc/rc.tcpip** avec l'éditeur de votre choix.
2. Recherchez la ligne introduite par **start /usr/lib/sendmail**. Par défaut, cette ligne ne doit pas être en commentaire, c'est-à-dire précédée du signe #. Si ce signe figure en début de ligne, supprimez-le.
3. Sauvegardez le fichier.

Le démon **sendmail** sera exécuté à l'amorçage du système.

Gestion des alias

Les alias mettent en correspondance des noms et des listes d'adresses par le biais de fichiers personnels, système ou domaine. Il existe trois types d'alias :

personnel Défini par l'utilisateur dans son fichier **$HOME/.mailrc**.

système local Défini par l'administrateur du système de messagerie dans le fichier **/etc/aliases**. Les alias de ce type s'appliquent au courrier traité par la commande **sendmail** sur le système local. Ils ont rarement besoin d'être modifiés.

domaine Les alias sont recherchés via NIS (Network Information Service). (NIS doit être configuré et l'option `O AliasFile` définie dans le fichier **sendmail.cf**). Pour pouvoir utiliser le mappage d'alias, NIS procédez comme suit :

1. Enlevez le commentaire de l'option `O AliasFile` dans le fichier **sendmail.cf**. Par ailleurs, précisez le nom de mappe des alias NIS.
2. Recompilez le fichier **sendmail.cf** à l'aide de la commande **sendmail –bz**.
3. Recompilez la base de données des alias à l'aide de la commande **sendmail –bi**.

Si vous utilisez une hiérarchie de domaines pour NIS+, un hôte de messagerie peut s'avérer nécessaire pour chaque domaine dans l'espace nom. En effet, les noms de domaines distincts risquent de ne plus être uniques. Pour plus d'informations sur les caractéristiques de NIS et de NIS+, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

Fichier /etc/aliases

Le fichier **/etc/aliases** comporte une série d'entrées au format suivant :

```
Alias: nom1, nom2, ... nomX
```

Alias étant une chaîne alphanumérique de votre choix (sans caractères spéciaux, tels que @ et !). *Les variables nom1* à *nomX* représentent une liste de noms de destinataire, qui peut s'étendre sur plusieurs lignes. Chaque ligne de suite doit commencer par un espace ou une tabulation. Les lignes blanches ou précédées d'un dièse (#) sont des commentaires.

Le fichier **/etc/aliases** doit comporter les trois alias suivants :

MAILER-DAEMON ID de l'utilisateur destinataire des messages adressés au démon du programme facteur. Ce nom est attribué initialement à l'utilisateur racine :

```
MAILER-DAEMON: root
```

postmaster ID de l'utilisateur chargé de l'exploitation de la messagerie locale. L'alias **postmaster** définit une adresse de boîte aux lettres unique valable sur chaque système du réseau. Cette adresse permet d'envoyer des requêtes à l'alias **postmaster** à partir de n'importe quel système, sans connaître l'adresse exacte de l'utilisateur sur ce système. Ce nom est attribué initialement à l'utilisateur racine :

```
postmaster: root
```

nobody ID destinataire des messages adressés aux programmes tels que **news** et **msgs**. Ce nom est attribué initialement à /**dev**/**null** :

```
nobody: /dev/null
```

Pour recevoir ces messages, déclarez l'alias comme utilisateur valide.

A chaque modification du fichier, vous devez le recompiler dans un format de base de données exploitable par la commande **sendmail**. Reportez-vous à "Création d'une base de données d'alias", page 2-5.

Création d'alias de système local

Pour créer ou modifier des alias de système local :

1. Modifiez le fichier /**etc**/**aliases** avec l'éditeur de votre choix.
2. Sur une ligne blanche, ajoutez un alias suivi de deux-points (:) et d'une liste de destinataires séparés par une virgule. Par exemple, pour définir l'alias `writers` pour les utilisateurs de ce groupe, entrez :

   ```
   writers: geo, mark@zeus, ctw@athena, brian
   ```

   Cette définition peut s'étendre sur plusieurs lignes, à condition que chaque ligne de suite commence par un espace ou une tabulation. Par exemple :

   ```
   writers: geo,
         mark@zeus,
         ctw@athena,
         brian
   ```

3. Déclarez un propriétaire pour chaque alias de liste de diffusion. Si la commande **sendmail** ne parvient pas à distribuer le courrier aux membres d'une liste de diffusion, un message d'erreur est envoyé au propriétaire de cette liste. Par exemple, la liste `editors` dont le propriétaire est `glenda@hera` peut se définir dans le fichier /**etc**/**aliases** par les entrées suivantes :

   ```
   editors: glenda@hera, davidm@kronos, perryw@athena
   owner-editors:  glenda@hera
   ```

4. Recompilez le fichier /**etc**/**aliases** comme indiqué à "Création d'une base de données d'alias".

Création d'une base de données d'alias

La commande **sendmail** n'utilise pas directement les définitions d'alias dans le fichier /**etc**/**aliases** du système local. Elle fait appel à une version de ce fichier générée par le gestionnaire de base de données. Pour compiler la base de données d'alias, vous avez le choix entre les méthodes suivantes :

- Lancez la commande /**usr**/**sbin**/**sendmail** assortie de l'indicateur **-bi**.
- Exécutez **newaliases**. Cette commande provoque la lecture, par **sendmail**, du fichier /**etc**/**aliases** du système local et la création de deux autres fichiers contenant les informations de la base d'alias :

  /**etc**/**aliases.dir**

  /**etc**/**aliases.pag**

- Lancez la commande **sendmail** assortie de l'indicateur **Rebuild Aliases**. Cette commande reconstruit automatiquement la base de données d'alias lorsqu'elle est périmée. Le reconstruction automatique peut être dangereuse sur des machines très chargées, contenant de gros fichiers d'alias. Si la reconstruction dure plus longtemps que le délai imparti (normalement, 5 minutes), il y a des chances que plusieurs processus la lancent simultanément.

Remarque

1. Sans ces fichiers, la commande **sendmail** ne peut pas traiter le courrier et génère un message d'erreur.
2. Si plusieurs bases de données d'alias sont spécifiées, l'indicateur **-bi** reconstruit tous les types qu'il peut interpréter (il peut, par exemple, reconstruire les bases de données NDBM, et non les bases NIS).

A partir d'AIX version 4.2, le fichier /**etc**/**netsvc.conf** contient l'ordonnancement des services système. Pour spécifier l'ordonnancement des services des alias, ajoutez la ligne suivante :

```
aliases=service, service
```

`service` pouvant être `files` ou `nis`. Par exemple :

```
aliases=files, nis
```

indique à la commande **sendmail** de tenter d'abord le fichier d'alias local puis, en cas d'échec, d'essayer `nis`. Si `nis` est défini comme un service, il doit être actif.

Pour en savoir plus sur le fichier /**etc**/**netsvc.conf**, reportez-vous à *AIX Files Reference*.

Gestion des fichiers et répertoires de file d'attente courrier

La file d'attente courrier est un répertoire qui stocke des données et gère les files d'attente de messages distribués par la commande **sendmail**. Son nom par défaut est **/var/spool/mqueue**.

Les messages peuvent être mis en attente pour diverses raisons. Si la commande **sendmail** est configurée pour exécuter la file d'attente à intervalles réguliers et non immédiatement, les messages y sont stockés temporairement. Par ailleurs, si un système hôte distant ne répond pas à une demande de connexion courrier, la messagerie met les messages en attente en vue d'une tentative ultérieure.

Impression de la file d'attente courrier

Pour imprimer le contenu de la file d'attente, lancez la commande **mailq** (ou spécifiez l'indicateur **-bp** avec la commande **sendmail**).

Une liste des ID de file d'attente est générée, indiquant la taille de chaque message, la date de son insertion dans la file et les noms d'expéditeur et de destinataire.

Fichiers de file d'attente courrier

Chaque message en attente est associé à un certain nombre de fichiers, désignés par :

```
Typef ID
```

ID est l'ID unique de file d'attente et *Type*, le type du fichier symbolisé par une lettre :

d Fichier de données contenant le corps du texte du message sans l'en-tête.

q Fichier de contrôle de file d'attente contenant les informations utiles au traitement du travail.

t Fichier temporaire correspondant à l'image du fichier **q** lors de sa reconstitution. Très vite renommé **q**.

x Fichier de transcription créé pour la durée d'une session, dans lequel sont consignés tous les événements de la session.

Par exemple, soit le message portant l'ID de file d'attente AA00269, les fichiers suivants sont générés et supprimés du répertoire de file d'attente courrier pendant que **sendmail** tente de livrer ce message :

dfAA00269	Fichier de données
qfAA00269	Fichier de contrôle
tfAA00269	Fichier temporaire
xfAA00269	Fichier de transcription

Fichier de contrôle q

Ce fichier contient une série de lignes commençant par les lettres suivantes :

B Spécifie le `body type`. Le reste de la ligne est une chaîne de texte définissant le `body type`. En l'absence de ce champ, le `body type` est supposé indéfini et aucun traitement particulier n'est entrepris. Valeurs possibles : **7BIT** et **8BITMIME**

C Contient l'adresse de contrôle. Syntaxe : *utilisateurlocal:nomalias*. Les adresses de destinataire suivant cette ligne sont assorties d'indicateurs, de sorte que les livraisons sont exécutées comme *utilisateurlocal* (un nom d'utilisateur inscrit dans le fichier **/etc/passwd**) ; *nomalias* est le nom de l'alias qui a été étendu à cette adresse (utilisé pour afficher les messages).

F Contient les bits d'indicateur, sous la forme d'une lettre par indicateur. Les bits d'indicateur définis sont **r**, indiquant l'existence d'un message de réponse, et **w**, indiquant qu'un message d'avertissement a été envoyé pour annoncer que le courrier est différé.

H Ligne(s) contenant la définition de l'en-tête. Le nombre de lignes est indifférent. L'ordre d'apparition des lignes `H` détermine leur disposition dans le message final. Elles utilisent la syntaxe de définition des en-têtes appliquée dans le fichier **/etc/sendmail.cf**.

I Numéro-i du fichier de données. Utile pour recouvrer la file d'attente courrier après un crash de disque.

K Heure (en secondes) de la dernière tentative de distribution.

M Contient un message imprimé par la commande **mailq**.

N Nombre total de tentatives de distribution.

O Spécifie la valeur MTS originale de la transaction SMTP. Utilisé exclusivement pour les Notifications d'état de distribution.

P Ligne précisant le niveau de priorité du message courant, lequel détermine l'ordre d'exécution des messages en file d'attente. Plus le numéro est élevé, plus la priorité est basse, autrement dit, la priorité croît à mesure que l'on descend dans la liste des messages. Le niveau de priorité initial est fonction de la classe et de la taille du message.

Q Destinataire initial tel que spécifié par le champ `ORCPT=` dans une transaction ESMTP. Utilisé exclusivement pour les Notifications d'état de distribution. Il ne s'applique qu'à la ligne "R" figurant immédiatement après.

R Lignes comportant chacune une adresse de destinataire.

S Contient l'adresse de l'expéditeur. (Une seule ligne.)

T Ligne indiquant l'heure de création, qui sert à calculer le délai de rétention du message en file d'attente.

V Numéro de version du format de fichier de file d'attente utilisé pour que les nouveaux fichiers binaires **sendmail** puissent lire les fichiers créés sous les versions antérieures. Valeur par défaut : **zero**. Si présent, doit figurer sur la première ligne du fichier.

Z ID enveloppe initiale (issu de la transaction SMTP). Utilisé exclusivement pour les Notifications d'état de distribution.

$** Contient une définition de macro. Les valeurs de certaines macros (**$r et **$s**) sont passées au cours de la phase d'exécution de la file.

Le fichier **q** associé au message adressé à `amy@zeus` se présenterait comme suit :

```
P217031
T566755281
MDeferred: Connection timed out during user open with zeus
Sgeo
Ramy@zeus
H?P?return-path: < <geo>
Hreceived: by george (0.13 (NL support)/0.01)
        id AA00269; Thu, 17 Dec 87 10:01:21 CST
H?D?date: Thu, 17 Dec 87 10:01:21 CST
H?F?From: geo
Hmessage-id: < <8712171601.AA00269@george>>
HTo: amy@zeus
Hsubject: test
```

où :

`P217031`	Priorité du message
`T566755281`	Temps de soumission en secondes
`MDeferred: Connection timed out during user open with zeus`	Message d'état
`Sgeo`	ID de l'expéditeur
`Ramy@zeus`	ID du destinataire
`H`*`Lines`*	Informations d'en-tête du message.

Spécification des délais au démon sendmail

Un format horaire spécial est prévu pour spécifier les délais associés au message et les intervalles de traitement des files d'attente. Ce format est le suivant :

```
–q NombreUnité
```

Nombre étant un entier et *Unité* une des lettres symbolisant l'unité utilisée :

s	secondes
m	minutes
h	heures
d	jours
w	semaines

L'unité de temps par défaut est les minutes (**m**). Voici trois exemples :

```
/usr/sbin/sendmail –q15d
```

Avec cette commande, **sendmail** traite la file d'attente tous les 15 jours.

```
/usr/sbin/sendmail –q15h
```

Avec cette commande, **sendmail** traite la file d'attente toutes les 15 heures.

```
/usr/sbin/sendmail –q15
```

Avec cette commande, **sendmail** traite la file d'attente toutes les 15 minutes.

Exécution forcée de la file d'attente courrier

Si vous trouvez qu'une file d'attente commence à saturer, vous pouvez forcer son exécution par le biais de l'indicateur **–q**. Vous pouvez également spécifier l'indicateur **–v** (verbose) pour voir ce qui se passe :

```
/usr/sbin/sendmail –q –v
```

Vous pouvez également limiter les travaux à ceux dotés d'un identificateur de file, d'un expéditeur ou d'un destinataire donné, via l'un des modificateurs de file d'attente.
Par exemple, **-qRsally** limite l'exécution de la file d'attente aux travaux dont l'adresse d'un des destinataires contient la chaîne **sally**. De même, **-qS** *chaîne* limite l'exécution à quelques expéditeurs et **-ql** *chaîne,* à quelques identificateurs de file d'attente.

Intervalle de traitement de la file d'attente

L'intervalle de traitement de la file d'attente courrier par le démon **sendmail** est déterminé par l'indicateur **-q**, qui est pris en compte au lancement du démon.

Généralement, **sendmail** est lancé par le fichier /**etc**/**rc.tcpip** au démarrage du système. Ce fichier contient la variable QPI (Queue Processing Interval), qui sert à attribuer une valeur à l'indicateur **-q** à l'exécution du démon **sendmail**. Par défaut, la valeur de **qpi** est 30 minutes. Pour la modifier :

1. Modifiez le fichier /**etc**/**rc.tcpip** avec l'éditeur de votre choix.
2. Recherchez la ligne qui définit cette valeur, par exemple :

   ```
   qpi=30m
   ```

3. Changez la valeur de *qpi* comme souhaité.

lancement du système. Ces modifications prendront effet au prochainPour une prise en compte immédiate, arrêtez puis relancez le démon **sendmail**. Pour plus d'informations, reportez-vous à"Arrêt du démon sendmail", page 2-11 et "Lancement du démon sendmail", page 2-10.

Transfert de file d'attente courrier

Si un système hôte est hors service pendant quelques temps, de nombreux messages envoyés ou en transit sur ce système sont peut-être stockés dans votre file d'attente courrier. Ce phénomène alourdit le traitement de la file d'attente au détriment des performances de votre système. Dans ce cas, vous avez la possibilité de transférer temporairement la file d'attente vers un autre emplacement et d'en créer une nouvelle. Vous pourrez ainsi traiter l'ancienne file une fois le système hôte remis en service. Pour effectuer ces opérations :

1. Arrêtez le démon **sendmail** comme indiqué à "Arrêt du démon sendmail", page 2-11.
2. Déplacez la totalité du répertoire de file d'attente :

   ```
   cd /var/spool
   mv mqueue omqueue
   ```

3. Relancez **sendmail** comme indiqué à "Lancement du démon sendmail", page 2-10.
4. Pour traiter l'ancienne file d'attente, entrez :

   ```
   /usr/sbin/sendmail -oQ/var/spool/omqueue -q.
   ```

   L'indicateur **–oQ** désigne le répertoire temporaire de la file transférée, et l'indicateur **–q** demande l'exécution de tous les travaux de la file. Pour obtenir un compte rendu du déroulement des opérations, précisez **-v**.

   Remarque : Cette opération peut durer un certain temps.

5. Supprimez fichiers journaux et répertoire temporaire une fois la file d'attente vidée :

   ```
   rm /var/spool/omqueue/*
   rmdir /var/spool/omqueue
   ```

Lancement du démon sendmail

Pour lancer le démon **sendmail**, entrez :

```
startsrc -s sendmail -a "-bd -q15"
```

OU

```
/usr/lib/sendmail -bd -q15
```

Si **sendmail** est déjà activé à l'exécution de ces commandes, un message vous indique que le démon ne peut être lancé plusieurs fois :

```
Le sous-système sendmail est déjà actif. Plusieurs sessions ne
peuvent être acceptées.
```

Sinon, un message vous confirme le lancement du démon.

Arrêt du démon sendmail

Pour arrêter le démon **sendmail**, exécutez la commande **stopsrc -s sendmail**. Sinon :

- Recherchez le pid de **sendmail**.
- Lancez **kill –9 sendmail_pid**.

Gestion de la journalisation

La commande **sendmail** consigne dans un journal les activités de la messagerie en faisant appel au démon **syslogd**. Le démon **syslogd** doit être configuré et exécuté pour permettre la journalisation. Dans le fichier **/etc/syslog.conf** notamment, la ligne ci-après doit être activée (et non mise en commentaire) :

```
mail.debug              /var/spool/mqueue/log
```

Si elle est désactivée, modifiez-la à l'aide de l'éditeur de votre choix, en prenant soin d'indiquer le chemin d'accès correct. Si vous modifiez le fichier **/etc/syslog.conf** au cours de l'exécution du démon **syslogd**, vous devez régénérer le démon comme suit :

```
refresh -s syslogd
```

Si le fichier **/var/spool/mqueue/log** n'existe pas, vous devez le créer via la commande :

```
touch /var/spool/mqueue/log
```

Les messages sont consignés dans le fichier journal au format suivant :

Chaque ligne d'un journal système comporte un horodateur, le nom de la machine qui l'a généré (pour les journaux concernant plusieurs machines d'un réseau local), le mot "sendmail:," et un message. La plupart des messages sont constitués d'une série de paires *nom=valeur*.

Deux lignes communes sont consignées lorsqu'un message est traité. La première indique la réception d'un message : il y en a une par message. Certains champs peuvent être omis. Les champs du message sont les suivants :

`from`	Adresse de l'expéditeur de l'enveloppe.
`size`	Taille du message (en octets).
`class`	Classe (priorité numérique) du message.
`pri`	Priorité initiale du message (pour le tri des files d'attente).
`nrcpts`	Nombre de destinataires de l'enveloppe pour ce message (après définition d'alias et transmission).
`proto`	Protocole utilisé pour la réception du message (par exemple, ESMTP ou UUCP).
`relay`	Machine d'où provient le message.

Une autre ligne est consignée à chaque tentative de livraison (il peut donc y en avoir plusieurs par message - si le message est différé ou qu'il y a plusieurs destinataires). Les champs du message sont les suivants :

`to`	Liste des destinataires, séparés par une virgule.
`ctladdr`	"Utilisateur contrôleur", c'est-à-dire nom de l'utilisateur dont les références sont utilisées pour la livraison.
`delay`	Délai total entre le moment où le message a été reçu et le moment où il a été délivré.
`xdelay`	Durée nécessaire pour cette tentative de livraison.
`mailer`	Nom du programme facteur utilisé pour délivrer à ce destinataire.
`relay`	Nom de l'hôte qui a effectivement accepté (ou rejeté) ce destinataire.
`stat`	Etat de la livraison.

Les informations qui peuvent être consignées sont nombreuses. Le journal est structuré en niveaux. Au niveau le plus bas, seules les situations très inhabituelles sont consignées. Au niveau le plus élevé, même les événements insignifiants le sont. Par convention, les niveaux inférieurs à 10 sont considérés ”utiles”. Les niveaux supérieurs à 64 sont réservés à la mise au point et les niveaux intermédiaires (11–64), dédiés aux informations détaillées.

Les types d'activité consignés par la commande **sendmail** dans le journal sont spécifiés via l'option **L** dans le fichier **/etc/sendmail.cf**.

Gestion du journal

Sans cesse alimenté par de nouvelles données, le journal peut prendre des proportions non négligeables. Par ailleurs, il arrive que certains incidents génèrent des entrées inattendues dans la file d'attente courrier. Pour limiter l'encombrement du journal et de la file d'attente, exécutez le script **shell /usr/lib/smdemon.cleanu.** Ce script force la commande **sendmail** à traiter la file d'attente et tient à jour quatre copies des fichiers journaux à des niveaux de mise à jour croissants **log.0**, **log.1**, **log.2** et **log.3**. A chaque exécution du script, le contenu des fichiers est transféré comme suit :

- **log.2** à **log.3**
- **log.1** à **log.2**
- **log.0** à **log.1**
- **log** à **log.0**.

Ces transferts permettent de reprendre la journalisation sur un nouveau fichier. Exécutez le script manuellement ou à intervalle régulier à l'aide du démon **cron.**

Journalisation du trafic

De nombreuses versions de SMTP n'implémentent pas complètement le protocole. Par exemple, certains SMTP basés sur PC ne savent pas interpréter les lignes de suite dans les codes de réponse. Ceci peut être très difficile à déceler. Si vous suspectez un problème de cet ordre, vous pouvez activer la journalisation du trafic via l'indicateur **-X**. Par exemple :

```
/usr/sbin/sendmail -X /tmp/traffic -bd
```

Cette commande consigne l'intégralité du trafic dans le fichier **/tmp/traffic.**

Cette opération consigne une énorme quantité de données en très peu de temps et ne doit jamais être effectuée dans le cadre de l'exploitation normale. Après avoir lancé un démon de ce type, forcez l'implémentation **errant** à envoyer un message à votre hôte. Tout le trafic entrant et sortant de **sendmail**, trafic SMTP entrant compris, sera consigné dans ce fichier**.**

Via **sendmail**, vous pouvez consigner un cliché des fichiers ouverts et du cache de connexion en lui envoyant un signal **SIGUSR1**. Les résultats sont consignés avec la priorité **LOG_DEBUG.**

Journalisation des données statistiques

La commande **sendmail** assure le suivi du volume de courrier traité par chaque programme facteur qui communique avec la commande (programmes définis dans le fichier **/etc/sendmail.cf**).

Pour lancer la collecte des données statistiques, créez le fichier **/etc/sendmail.st** comme suit :

```
touch /etc/sendmail.st
```

Si la commande **sendmail** rencontre des erreurs pendant l'enregistrement des données statistiques, elle inscrit un message via la sous-routine **syslog**. Ces erreurs n'entravent pas les autres opérations de **sendmail**.

La commande **sendmail** met les informations à jour chaque fois qu'un courrier est traité. La taille du fichier reste égale, mais les nombres dans le fichier augmentent. Ces nombres

représentent le volume de courrier accumulé depuis la création ou la réinitialisation du fichier **/etc/sendmail.st.**

Affichage des informations des programmes facteurs

Les données statistiques conservées dans le fichier **/etc/sendmail.st** sont sauvegardées sous un format de base de données, et ne peuvent donc être consultées comme un fichier texte. Pour les afficher, entrez :

```
/usr/sbin/mailstats
```

Cette commande lit les données du fichier **/etc/sendmail.st**, et les formate avant de les envoyer vers la sortie standard sous le format suivant :

```
  msgs_from bytes_from      msgs_to         bytes_to      Mailer
          1          2             1              201      local
```

Les champs proposés ont la signification suivante :

`msgs_from`	Nombre de messages reçus du programme facteur par la machine locale.
`bytes_from`	Nombre d'octets des messages reçus du programme facteur par la machine locale.
`msgs_to`	Nombre de messages émis par la machine locale à l'aide du programme facteur.
`bytes_to`	Nombre d'octets des messages émis par la machine locale à l'aide du programme facteur.

Si la commande **sendmail** envoie le courrier directement dans un fichier de type **$HOME/dead.letter** ou alias, le décompte des messages et des octets est imputé au programme facteur prog.

Mise au point de sendmail

Il existe de nombreux indicateurs de mise au point, intégrés à la commande **sendmail**. A chaque indicateur sont associés un numéro et un niveau, les niveaux supérieurs indiquant un accroissement des informations. Par convention, les niveaux supérieurs à 9 fournissent tellement d'informations que vous ne souhaiterez pas les consulter - sauf pour mettre au point un module particulier de code source. Les indicateurs de mise au point sont définis via l'indicateur **–d**, comme illustré dans l'exemple ci-dessous **:**

```
debug-flag: -d debug-list
debug-list debug-flag[.debug-flag]*
debug-flag: debug-range[.debug-level]
debug-range:integer|integer-integer
debug-level:integer
```

Par exemple :

```
-d12Set flag 12 to level 1
-d12.3Set flag 12 to level 3
-d3-17Set flags 3 through 17 to level 1
-d3-17.4Set flags 3 through 17 to level 4
```

Les indicateurs de mise au point disponibles sont les suivants :

–d0	Mise au point générale.
–d1	Affiche les informations d'envoi.
–d2	Prend fin avec *finis*( ).
–d3	Indique la charge moyenne.
–d4	Espace disque suffisant.
–d5	Affiche les événements.
–d6	Affiche le courrier non parvenu.
–d7	Nom du fichier de file d'attente.
–d8	Résolution de noms DNS.
–d9	Effectue un suivi des requêtes RFC1413.
–d9.1	Met le nom d'hôte sous forme canonique.
–d10	Affiche le courrier reçu par le destinataire.
–d11	Effectue un suivi des livraisons.
–d12	Affiche le mappage de l'hôte relatif.
–d13	Affiche les livraisons.
–d14	Affiche les virgules du champ d'en-tête.
–d15	Affiche l'activité des requêtes d'obtention (get) du réseau.
–d16	Connexions sortantes.
–d17	Affiche la liste des hôtes MX.

Protocoles IMAP (Internet Message Access Protocol) et POP (Post Office Protocol)

AIX Pour l'accès à distance à la messagerie, AIX propose deux serveurs de protocole de messagerie électronique basés sur Internet :

- POP (Post Office Protocol),
- IMAP (Internet Message Access Protocol).

Ces deux types de serveur stockent le courrier électronique et y donnent accès. Grâce à ces protocoles, l'ordinateur n'a plus besoin d'être allumé pour la réception du courrier.

L'installation comprend un serveur POP et un serveur IMAP.

Le serveur POP fournissant un système de courrier électronique hors ligne, par le biais du logiciel client POP, le client a accès à distance au serveur de messagerie pour réceptionner son courrier. Il peut télécharger son courrier et, ensuite, soit le supprimer immédiatement du serveur, soit le conserver sur le serveur POP. Le courrier, une fois chargé sur la machine cliente, est traité localement sur cette machine. Le serveur POP autorise l'accès à une boîte aux lettres utilisateur à un seul client à la fois.

Le serveur IMAP propose un "super-ensemble" de fonctions POP, mais avec une autre interface. (Ainsi, le système a des clients spécifiques IMAP et POP.) Le serveur IMAP fournit un service hors ligne, un service en ligne et un service déconnecté. Le protocole IMAP permet de manipuler des boîtes aux lettres à distance comme si elles étaient locales. Par exemple, les clients peuvent faire des recherches dans les messages et y insérer des indicateurs d'état tels que "deleted" ou "answered" ("supprimé" ou "répondu"). En outre, les messages peuvent être conservés dans la base de données du serveur tant qu'ils ne sont pas supprimés explicitement. Le serveur IMAP permet à plusieurs clients d'accéder de façon interactive et simultanée aux boîtes aux lettres utilisateur.

Les serveurs IMAP et POP sont exclusivement des serveurs d'accès au courrier. Pour l'envoi du courrier, ils utilisent le protocole SMTP (Simple Mail Transfer Protocol).

IMAP et POP sont tous deux des protocoles ouverts, qui reposent sur les normes décrites dans les RFC (Request For Comments) : RFC 1730 en ce qui concerne le serveur IMAP, et RFC 1725 pour le serveur POP. Les deux serveurs sont "orientés connexion" et utilisent des sockets TCP. L'écoute IMAP et POP a respectivement lieu sur les ports identifiés 143 et 110. En outre, le démon **inetd** gère les deux serveurs.

Configuration des serveurs IMAP et POP

Prérequis

Vous devez être utilisateur racine (root).

Procédure

1. Désactivez le commentaire des entrées **imapd** et **pop3d** dans le fichier **/etc/inetd.conf**.
2. Rafraîchissez le démon **inetd** avec la commande :

```
refresh -s inetd
```

Tests de configuration

Vous pouvez lancer quelques tests pour vous assurer que les serveurs imapd et pop3d sont opérationnels.

Vérifiez comme suit que leur écoute a lieu sur les ports identifiés :

```
netstat -a | grep imap
netstat -a | grep pop
```

En principe, le résultat de la commande **netstat** donne :

```
tcp     0       0     *.imap2          *.*         LISTEN
tcp     0       0     *.pop3           *.*         LISTEN
```

Si vous n'obtenez pas ce résultat, vérifiez à nouveau les entrées dans le fichier **/etc/inetd.conf**, puis relancez la commande **refresh –s inetd**.

Testez la configuration sur le serveur imapd, via telnet, au niveau du port imap2, `143`. Vous obtenez l'invite imapd. Vous pouvez entrer les commandes IMAP version 4 définies dans la RFC 1730. Pour ce faire, tapez un point (.) puis un espace suivi du nom de la commande. Par exemple :

```
. NomCommande
```

Notez l'écho des mots de passe quand telnet est utilisé vers le serveur imapd.

Dans l'exemple `telnet` suivant, vous devez indiquer votre propre mot de passe à la place de *id_password* dans la commande **login**.

```
telnet e-xbelize 143
Trying...
Connected to e-xbelize.austin.ibm.com.
Escape character is '^]'.
* OK e-xbelize.austin.ibm.com IMAP4 server ready
. login id id_password
. OK
. examine /usr/spool/mail/root
* FLAGS (\Answered \Flagged \Draft \Deleted \Seen)
* OK [PERMANENTFLAGS (\Answered \Flagged \Draft \Deleted \Seen \*)]
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 823888143]
. OK [READ-ONLY] Examine completed
. logout
* BYE Server terminating connection
. OK Logout completed
Connection closed.
```

Testez la configuration du serveur pop3d, via telnet, au niveau du port pop3, `110`. Vous obtenez l'invite pop3d. Vous pouvez entrer les commandes POP définies dans la RFC 1725. Pour ce faire, tapez un point (.) puis un espace suivi du nom de la commande. Par exemple :

```
. NomCommande
```

Notez l'écho des mots de passe quand telnet est utilisé vers le serveur pop3d.

Dans l'exemple `telnet` suivant, vous devez indiquer votre propre mot de passe à la place de *id_password* dans la commande **pass**.

```
telnet e-xbelize 110
Trying...
Connected to e-xbelize.austin.ibm.com.
Escape character is '^]'.
+OK e-xbelize.austin.ibm.com POP3 server ready
user id
+OK Name is a valid mailbox
pass id_password
+OK Maildrop locked and ready
list
+OK scan listing follows
.
stat
+OK 0 0
quit
+OK
Connection closed.
```

syslog

Le logiciel serveur IMAP et POP adresse des journaux à l'outil **syslog**.

Pour configurer la journalisation IMAP et POP sur votre système par le biais de **syslog**, vous devez être un utilisateur racine. Editez le fichier de configuration /**etc**/**syslog.conf** pour y ajouter une entrée pour ***.debug** comme suit :

```
*.debug /usr/adm/imapd.log
```

Le fichier `usr/adm/imapd.log` doit être existant avant la relecture par le démon **syslogd** du fichier /**etc**/**syslog.conf**. Pour créer **usr**/**adm**/**imapd.log**, utilisez la commande :

```
touch /usr/adm/imapd.log
```

Ensuite, rafraîchissez **syslogd** avec la commande suivante pour la relecture de son fichier de configuration :

```
refresh -s syslogd
```

Informations de référence du courrier

Cette section fournit un bref récapitulatif des commandes, fichiers et répertoires intervenant dans la messagerie.

Liste des commandes

Cette liste répertorie les commandes d'exploitation et de gestion de la messagerie.

bugfiler	Enregistre les comptes rendus d'anomalies dans des répertoires courrier spécifiques.
comsat	Avertit les utilisateurs de l'arrivée d'un courrier (démon).
mailq	Imprime le contenu de la file d'attente courrier.
mailstats	Affiche les statistiques relatives au trafic du courrier.
newaliases	Crée une copie de la base de données d'alias à partir du fichier **/etc/aliases**.
rmail	Gère le courrier distant reçu via la commande **uucp** de BNU.
sendbug	Envoie un compte rendu d'anomalies à une adresse spécifique.
sendmail	Délivre le courrier en local ou sur le réseau.
smdemon.cleanu	Epure la file d'attente **sendmail** pour les tâches de routine.

Liste des fichiers et répertoires courrier

Les fichiers et répertoires sont présentés par fonction.

Messagerie

/usr/share/lib/Mail.rc	Définit les valeurs par défaut du système local pour tous les utilisateurs de la messagerie. Fichier de texte modifiable pour définir les caractéristiques par défaut de la commande **mail**.
$HOME/.mailrc	Permet de modifier les valeurs par défaut du système local pour la messagerie.
$HOME/mbox	Stocke le courrier traité d'un utilisateur.
/usr/bin/Mail, **/usr/bin/mail**, ou **/usr/bin/mailx**	Indique trois noms associés au même programme. La messagerie est l'une des interfaces entre l'utilisateur et le système de messagerie.
/var/spool/mail	Indique le répertoire par défaut de dépôt du courrier. Le courrier est stocké par défaut dans le fichier **/var/spool/mail/nom-utilisateur**.
/usr/bin/bellmail	Prend en charge la livraison du courrier local.
/usr/bin/rmail	Assure l'interface courrier distant pour BNU.
/var/spool/mqueue	Contient le fichier journal et les fichiers temporaires associés aux messages de la file d'attente courrier.

Commande sendmail

/usr/sbin/sendmail	Commande **sendmail**.
/usr/ucb/mailq	Pointe sur le fichier **/usr/sbin/sendmail**. Equivaut à **/usr/sbin/sendmail –bp**.
/usr/ucb/newaliases	Pointe sur le fichier **/usr/sbin/sendmail**. Equivaut à **/usr/sbin/sendmail –bi**.
/etc/netsvc.conf	Spécifie l'ordre de certains services de résolution de noms.
/usr/sbin/mailstats	Formate et affiche les données statistiques **sendmail** recueillies dans le fichier par défaut **/etc/sendmail.st**, s'il existe. Vous pouvez spécifier un autre fichier.
/etc/aliases	Décrit une version texte du fichier d'alias pour la commande **sendmail**. Vous pouvez éditer ce fichier pour créer, modifier ou supprimer des alias de votre système.
/etc/aliasesDB	Décrit un répertoire contenant les fichiers de base de données d'alias, **DB.dir** et **DB.pag**, créés à partir du fichier **/etc/aliases** à l'exécution de la commande **sendmail –bi**.
/etc/aliasesDB1	Désigne un fichier de verrouillage pour la base de données **aliasesDB**.
/etc/sendmail.cf	Contient les informations de configuration de **sendmail** dans un format texte. Editez ce fichier pour modifier les informations.
/etc/sendmail.cfDB	Contient la version traitée du fichier de configuration **/etc/sendmail.cf**. Ce fichier est créé à partir du fichier **/etc/sendmail.cf** à l'exécution de la commande **/usr/sbin/sendmail –bz**.
/etc/sendmail.cfDBl	Désigne un fichier de verrouillage pour la base de données **etc/sendmail.cfDB**.
/etc/sendmail.nl	Contient les informations de configuration NLS (National Language Support) de **sendmail**, dans un format texte. Editez ce fichier pour modifier les informations.
/etc/sendmail.nlDB	Contient la version traitée du fichier de configuration **/etc/sendmail.nl**. Ce fichier est créé à partir du fichier **/etc/sendmail.nl** à l'exécution de la commande **/usr/sbin/sendmail –bn**.
/etc/sendmail.nlDBl	Désigne un fichier de verrouillage pour la base de données **etc/sendmail.nlDB**.
/usr/lib/smdemon.cleanu	Spécifie un fichier shell qui exécute la file d'attente courrier et tient à jour des fichiers journaux **sendmail** dans le répertoire **/var/spool/mqueue**.
/etc/sendmail.st	Rassemble les statistiques relatives au trafic du courrier. Ce fichier a une taille fixe. Utilisez la commande **/usr/sbin/mailstats** pour afficher son contenu. Supprimez-le si vous ne voulez pas recueillir ce type d'informations.
/var/spool/mqueue	Désigne le répertoire contenant les fichiers temporaires associés à chaque message en file d'attente. Ce répertoire peut contenir le fichier journal.
/var/spool/cron/crontabs	Désigne le répertoire contenant les fichiers lus par le démon **cron** pour déterminer le travail à exécuter. Le fichier **root** comporte une ligne d'exécution du script shell **smdemon.cleanu**.

Liste des commandes IMAP et POP

/usr/sbin/imapd	Process serveur IMAP (Internet Message Access Protocol).
/usr/sbin/pop3d	Process serveur POP3 (Post Office Protocol version 3.

Chapitre 3. Protocole TCP/IP

Ce chapitre décrit la suite de logiciels réseau TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP est un protocole normalisé souple et puissant, permettant de connecter plusieurs ordinateurs à d'autres machines.

Ce chapitre traite des points suivants :

Remarque : La plupart des tâches abordées dans ce chapitre nécessitent les droits d'utilisateur racine.

Préparation du réseau TCP/IP

TCP/IP étant un outil réseau très souple, vous pouvez intervenir à plusieurs niveaux afin de personnaliser votre réseau TCP/IP et l'adapter aux besoins spécifiques de votre organisation. Vous trouverez ci–dessous les principaux points à prendre en compte pour préparer votrre réseau. (Chaque point fait l'objet d'un étude détaillée dans la suite de ce manuel. Cette liste vous permettra simplement d'évaluer la portée des actions possibles.)

1. Choisissez le type de matériel réseau que vous souhaitez utiliser : anneau à jeton (token–ring), Ethernet Version 2, IEEE 802.3, interface FDDI (Fiber Distributed Data Interface), canal optique série ou protocole SLIP (Serial Line Interface Protocol).
2. Tracez l'implantation physique du réseau.

   Réfléchissez aux fonctions que devra assurer chaque machine. Par exemple, vous pouvez choisir à ce stade les machines qui serviront de passerelles avant de passer au câblage du réseau.
3. Optez selon vos besoins pour un réseau *plat* ou une structure de réseau *hiérarchisée*.

   Si votre réseau est de peite taille, concentré sur un seul site, et ne comprend qu'un réseau physique, un réseau plat conviendra probablement parfaitement. Si votre réseau est très étendu, complexe, avec de nombreux sites ou plusieurs réseaux physiques, il sera vraisemblablement plus pratique d'opter pour un réseau hiérarchisé.
4. Si votre réseau doit être raccordé à d'autres réseaux, réfléchissez à l'installation et à la configuration des passerelles qui seront nécessaires. Vous devez :
   a. choisir les machines qui serviront de passerelles ;
   b. décider si vous utiliserez le routage statique ou le routage dynamique, à moins que vous n'élisiez une combinaison des deux. Si vous optez pour le routage dynamique, choisissez les démons de routage que devra utiliser chaque passerelle, en tenant compte des différents types de protocoles de communication à prendre en charge.
5. Préparez un schéma d'adressage.

   Si votre réseau n'est pas destiné à faire partie d'un interréseau plus large, choisissez le schéma d'adressage convenant le mieux à vos besoins. Si vous souhaitez intégrer votre réseau au sein d'un interréseau plus étendu tel qu'Internet, vous devrez vous procurer un jeu officiel d'adresses.
6. Voyez s'il convient d'envisager la division de votre système en plusieurs sous–réseaux. Si oui, décidez du mode d'attribution des masques de sous–réseau.
7. Décidez des conventions de noms. Chaque machine du réseau doit posséder un nom d'hôte unique.
8. Décidez si votre réseau requiert un serveur de noms pour la résolution des noms ou si le recours au fichier /**etc**/**hosts** est suffisant.

   Si vous choisissez d'utiliser des serveurs de noms, voyez quel type de serveur vous sera nécessaire et combien de serveurs de noms vous devez prévoir pour être efficace.
9. Décidez des types de services que le réseau proposera aux utilisateurs distants : messagerie, connexion à distance, exécution de commandes à distance, partage de fichiers, etc.

Installation et configuration pour TCP/IP

Pour plus d'informations sur l'installation de TCP/IP, reportez-vous au *AIX Installation Guide*.

Configuration de TCP/IP

Une fois TCP/IP installé, la configuration du système peut être effectuée.

Pour configurer TCP/IP, vous pouvez :

- utiliser l'application Web-based System Manager wsm network (raccourci **wsm network**),
- utiliser SMIT (System Management Interface System),
- éditer un format de fichier,
- lancer une commande à partir de l'invite du shell.

Par exemple, le script shell **rc.net** effectue la configuration minimale du système hôte pour TCP/IP au démarrage du système (ce script est lancé à la seconde phase de l'amorçage par le gestionnaire de configuration). Si vous utilisez SMIT ou Web-based System Manager pour configurer le système hôte, le fichier **rc.net** est automatiquement configuré.

Vous pouvez également reconfigurer le fichier **rc.net** à l'aide d'un éditeur standard et ainsi utiliser les commandes traditionnelles de configuration de TCP/IP sous UNIX, telles que : **ifconfig**, **hostname** et **route**. Pour en savoir plus, reportez-vous à "Liste des commandes TCP/IP", page 3-169.

Certaines tâches, telles que la configuration d'un serveur de noms, ne peuvent être accomplies via SMIT ou via Web-based System Manager. Pour connaître les fonctions SMIT, reportez-vous à "Raccourcis SMIT pour TCP/IP" dans *AIX 4.3 Guide d'administration : système d'exploitation et unités*.

Configuration des systèmes hôte

Chaque système hôte du réseau doit être adapté aux besoins des utilisateurs et aux contraintes du réseau. Pour chaque hôte, vous devez configurer l'interface de réseau, définir l'adresse Internet, le nom d'hôte et les routes statiques vers les passerelles ou les autres systèmes hôte. Il faut également spécifier les démons à lancer par défaut et configurer le fichier **/etc/hosts** pour la résolution des noms (ou configurer l'hôte de telle sorte qu'il utilise le serveur de noms).

Configuration des hôtes en tant que serveurs

Si la machine hôte joue un rôle spécifique (passerelle, serveur de fichiers ou serveur de noms), la configuration de base doit être complétée.

Par exemple, si le réseau est organisé hiérarchiquement et que vous utilisez le protocole **DOMAIN** pour la résolution des noms dans les adresses Internet, vous devez configurer au moins un serveur de noms.

N'oubliez pas qu'un hôte serveur n'a pas besoin d'être une machine dédiée : elle peut également servir à d'autres fonctions. Par exemple, si la fonction de serveur de noms est relativement limitée, la machine peut également être utilisée comme station de travail ou serveur de fichiers sur le réseau.

Remarque : Si NIS ou NIS+ est installé sur votre système, ces services peuvent également vous aider à la résolution des noms. Pour plus d'informations, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

Configuration des passerelles

Si vous envisagez de connecter votre réseau à d'autres réseaux, il vous faut configurer au moins une machine hôte passerelle. Pour cela, vous devez déterminer les protocoles de communication nécessaires et les démons de routage (**routed** ou **gated**) correspondants.

Commandes de gestion système TCP/IP

Voici la liste des commandes utiles pour configurer et gérer le réseau TCP/IP :

arp	Affichage/modification des tables de traduction d'adresse Internet en adresse matérielle, utilisées par **ARP** (Address Resolution Protocol).
finger	Retour d'informations concernant les utilisateurs sur un hôte spécifique.
host	Affichage de l'adresse Internet d'un hôte spécifique ou d'un nom d'hôte figurant dans une adresse Internet spécifique.
hostname	Affichage ou définition du nom et de l'adresse Internet d'un système hôte local.
ifconfig	Configuration des interfaces de réseau.
netstat	Affichage des adresses locales et distantes, des tables de routage, des données statistiques sur le matériel et du compte rendu des paquets transférés.
no	Affichage ou définition des options courantes du noyau de réseau.
ping	Détermination de l'accessibilité d'un système hôte.
route	Manipulation des tables de routage.
ruptime	Affichage des informations d'état sur les hôtes connectés aux réseaux physiques locaux et exécutant le serveur **rwhod**.
rwho	Affichage des informations d'état sur les utilisateurs des hôtes connectés aux réseaux physiques locaux et exécutant le serveur **rwhod**.
setclock	Calage de l'heure et de la date de l'hôte local sur celles du service horaire du réseau.
timedc	Informations sur le démon **timed**.
trpt	Compte rendu de suivi du protocole sur les prises TCP.
whois	Service du répertoire de noms Internet.

Configuration d'une liste de contrôle du réseau TCP/IP

Suivez la procédure ci-dessous pour effectuer ou modifier la configuration du réseau. Prenez le temps nécessaire pour rassembler les informations et comprendre les instructions. Cette préparation vous évitera de perdre bien plus de temps encore à corriger les erreurs commises.

Une fois le réseau installé et opérationnel, cette liste de contrôle vous servira à déterminer et mettre au point les anomalies incontournables qui surviennent sur tous les réseaux.

Prérequis

1. Le matériel du réseau doit être installé et câblé (voir "Cartes de réseau TCP/IP", page 3-39.
2. Le logiciel TCP/IP doit être installé (voir le manuel *AIX Installation Guide*).

Procédure

1. Consultez ”Protocoles TCP/IP”, page 3-6, pour la structure de base de TCP/IP. Vous devez comprendre :
   - la structure en couches de TCP/IP (différents protocoles résidant sur différentes couches),
   - le mécanisme de flux des données à travers les couches.
2. Effectuez la configuration minimale de chaque machine hôte du réseau : ajout d’une interface réseau, affectation d’une adresse IP, attribution d’un nom d’hôte à chaque machine hôte et définition d’une route par défaut d’accès au réseau. Consultez tout d’abord les sections ”Interfaces de réseau TCP/IP”, page 3-50, ”Adressage TCP/IP”, page 3-56 et ”Définition des noms d’hôte”, page 3-104. Suivez ensuite les instructions de la section ”Configuration de TCP/IP”, page 3-97.

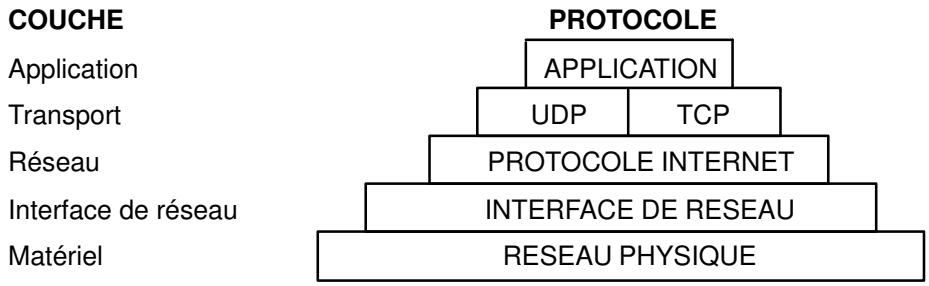
   Remarque : Chaque machine du réseau doit subir cette configuration minimale, qu’il s’agisse d’un hôte utilisateur, d’un serveur de fichiers, d’une passerelle ou d’un serveur de noms.
3. Configurez et lancez le démon **inetd** sur chaque machine hôte du réseau. Consultez la section ”Démons TCP/IP”, page 3-98, et procédez comme indiqué à ”Configuration du démon inetd”, page 3-101.
4. Configurez chaque machine hôte pour effectuer la résolution des noms en local ou utiliser le serveur de noms. Si vous installez un système hiérarchique de type DOMAIN, vous devez configurer au moins une machine hôte en tant que serveur de noms. Reportez-vous à ”Résolution de noms sous TCP/IP”, page 3-103.
5. Si votre réseau doit être connecté à d’autres réseaux distants, configurez au moins une machine hôte comme passerelle. Pour l’acheminement interréseau, la passerelle peut utiliser des routes statiques ou un démon de routage. Reportez-vous à ”Routage TCP/IP”, page 3-128.
6. Déterminez pour chaque machine hôte du réseau, les services accessibles. Par défaut, ils le sont tous. Pour changer cette configuration, procédez comme indiqué à ”Services réseau client”, page 3-101.
7. Désignez, parmi les machines hôtes, celles qui joueront le rôle de serveurs et définissez leurs services respectifs. Pour lancer les démons de serveur de votre choix, reportez-vous à ”Services réseau serveur”, page 3-102.
8. Configurez les serveurs d’impression à distance nécessaires. Pour en savoir plus, reportez-vous aux généralités sur les imprimantes dans *AIX Guide to Printers and Printing*.
9. Si vous le souhaitez, configurez une machine à utiliser comme serveur horaire maître pour le réseau. Pour en savoir plus, reportez-vous au démon **timed** dans le manuel *AIX Commands Reference*.

Protocoles TCP/IP

Cette section traite des points suivants :

Les protocoles sont des ensembles de règles de formats de message et de procédures qui permettent aux machines et aux applications d'échanger des informations. Ces règles doivent être observées par chaque machine impliquée dans la communication pour que le message puisse être interprété par le système destinataire.

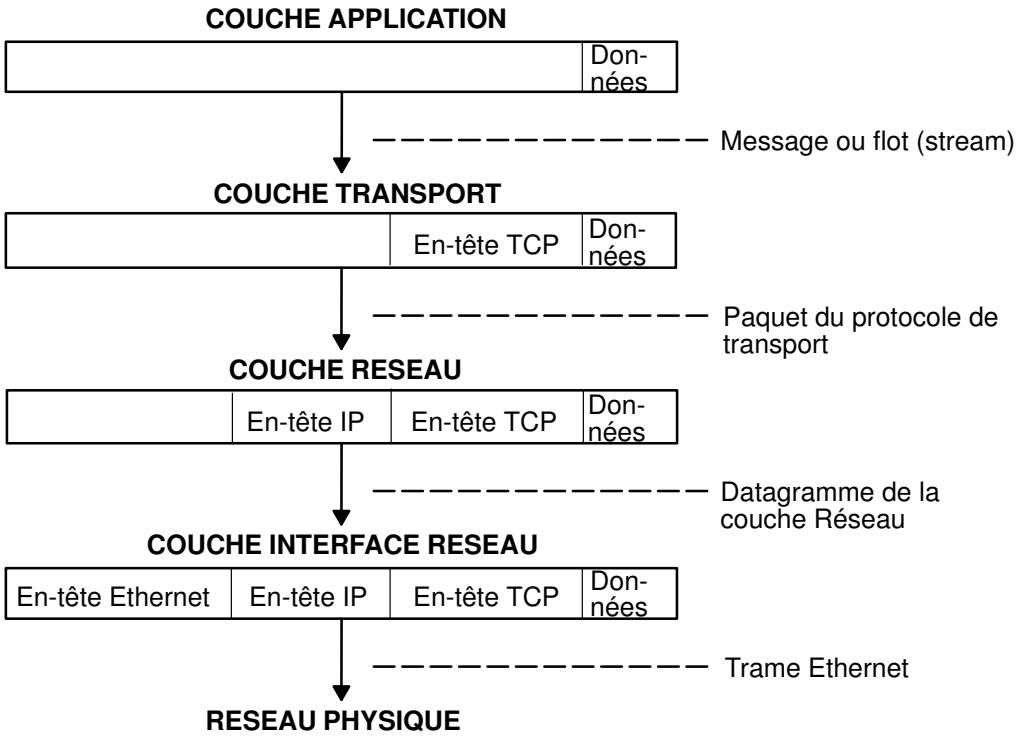
La *suite* de protocoles TCP/IP peut être représentée en couches (ou niveaux) comme suit :



TCP/IP définit précisément l'acheminement de l'information de l'émetteur au destinataire. Les messages ou trains de données sont envoyés par les programmes d'application à l'un des deux protocoles Internet de niveau transport : UDP (User Datagram Protocol) ou TCP (Transmission Control Protocol). A la réception des données, ces protocoles les divisent en *paquets*, y ajoutent une adresse de destination et les transmettent à la couche de protocole suivante, la couche Réseau Internet.

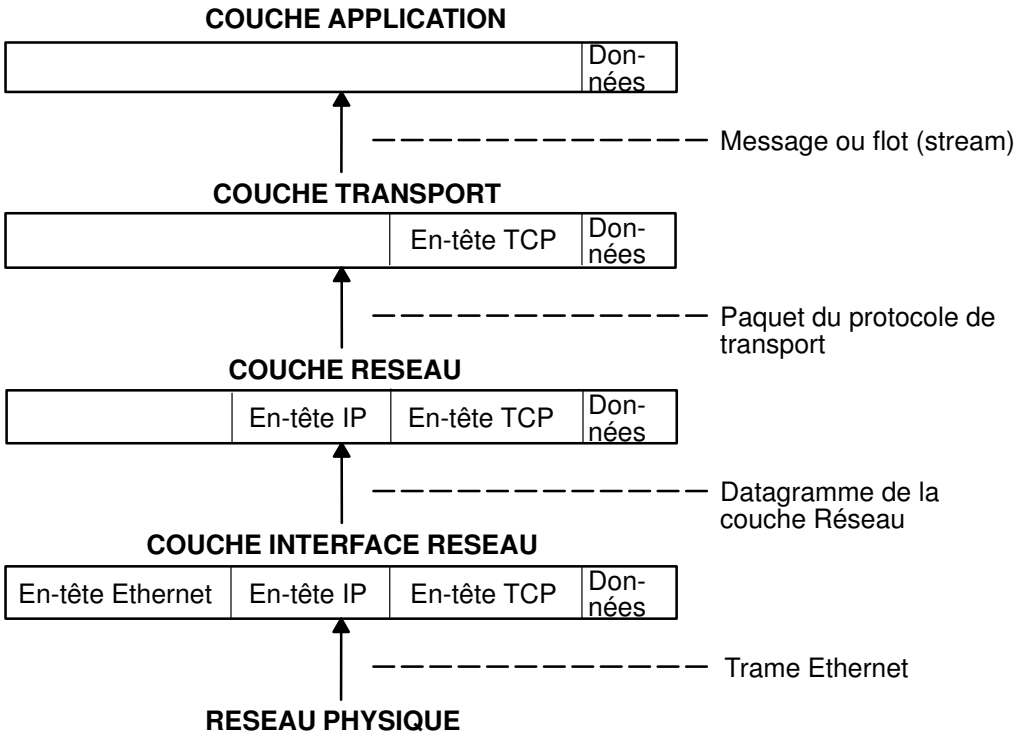
La couche Réseau Internet encapsule le paquet dans un datagramme IP (Internet Protocol), insère les données d'en-tête et de fin, décide de la destination du datagramme (directement à destination ou via une passerelle) et transmet le datagramme à la couche Interface réseau.

La couche Interface réseau réceptionne les datagrammes IP et les transmet sous forme de *trames* à travers un réseau spécifique (Ethernet ou anneau à jeton), comme illustré ci-dessous :



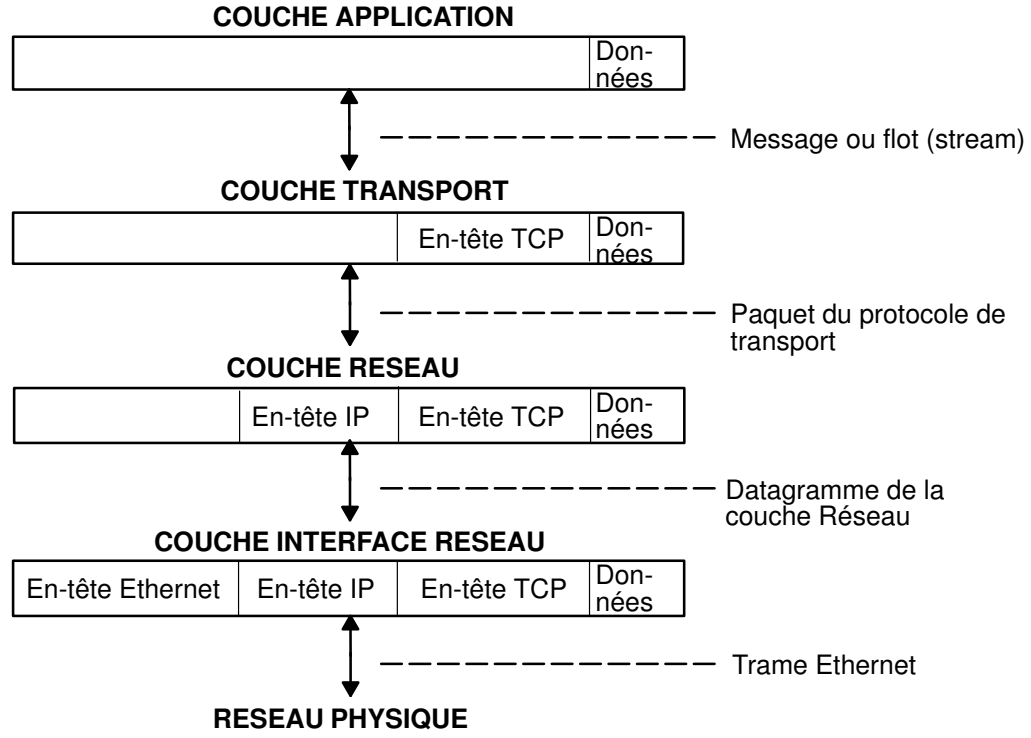
Déplacement des informations entre l'application expéditrice et l'hôte receveur

Les trames reçues par une machine hôte sont réexpédiées à travers les couches de protocoles dans le sens inverse. Chaque couche supprime l'information d'en-tête correspondante jusqu'à ce que les données atteignent de nouveau la couche Application (voir figure). Les trames arrivent dans la couche Interface réseau (dans le cas présent, une carte Ethernet). L'en–tête Ethernet est supprimé et le datagramme renvoyé vers la couche Réseau. Dans la couche Réseau, le protocole Internet supprime l'en-tête IP et envoie à son tour le paquet vers la couche Transport. A ce niveau, l'en-tête TCP est supprimé par le protocole TCP et les données sont envoyées vers la couche Application.



Déplacement des informations entre l'hôte et l'application

Les machines hôtes envoient et reçoivent des informations simultanément. En ce sens, le schéma ci-dessous (Transmission et réception des données hôtes), représente avec plus d'exactitude le mode de communication de l'hôte.



Remarque : Les en-têtes sont ajoutés puis supprimés au niveau de chaque couche de protocoles à la transmission et la réception des données par un hôte.

Transmission et réception des données hôte

IP version 6 - Généralités

IP (Internet Protocol) version 6 (IPv6 ou IP*ng*) est la prochaine génération IP, conçue comme une évolution d'IP version 4 (IPv4). Si IPv4 a permis le développement d'un Internet global, il n'est cependant pas capable de progresser davantage à cause de deux facteurs fondamentaux : espace d'adressage limité et complexité du routage. Les adresses 32 bits IPv4 ne fournissent pas suffisamment de flexibilité pour le routage global Internet. Le déploiement de CIDR (Classless InterDomain Routing) a étendu la durée de vie du routage IPv4 d'un certain nombre d'années, mais l'effort de gestion du routage continue toutefois à augmenter. Même si le routage IPv4 pouvait être augmenté, Internet finirait par être à court de numéros de réseau.

L'IETF (Internet Engineering Task Force) ayant reconnu qu'IPv4 ne serait pas capable d'assumer la croissance phénoménale d'Internet, le groupe de travail IETF IP*ng* a été formé. Parmi les propositions effectuées, SIPP (Simple Internet Protocol Plus) a été choisi comme étape dans le développement d'IP. Il a été renommé IP*ng*, et RFC1883 a été finalisé en décembre 1995.

IPv6 étend le nombre maximal d'adresses Internet de façon à gérer la croissance de la population utilisatrice d'Internet. Par rapport à IPv4, IPv6 présente l'avantage de permettre la coexistence des nouveautés et des éléments existants. Ceci permet une migration ordonnée d'IPv4 (adressage 35 bits) à IPv6 (adressage 128 bits) sur un réseau opérationnel.

Cette présentation est destinée à donner au lecteur une compréhension générale du protocole IP*ng*. Pour plus d'informations, veuillez vous reporter à RFC 1883, 1884, 1885, 1886, 1970, 1971 et 2133.

Routage et adressage étendus

IPv6 augmente la taille de l'adresse IP de 32 bits à 128 bits, prenant ainsi en charge davantage de niveaux dans la hiérarchie d'adressage, un nombre beaucoup plus grand de nœuds adressables et une configuration automatique plus simple des adresses.

Dans IPv6, il existe trois types d'adresses :

unicast Un paquet envoyé à une adresse unicast est livré à l'interface identifiée par cette adresse. Une adresse unicast a une portée particulière : local-liaison, local-site, global. Il existe également deux adresses unicast spéciales :

- ::/128 (adresse non spécifiée)
- ::1/128 (adresse en boucle)

Dans IPv6, il s'agit d'une seule adresse, et non d'un réseau entier.

multicast Un paquet envoyé à une adresse multicast est livré à l'interface identifiée par cette adresse. Une adresse multicast est identifiée par le préfixe ff::/8. Les adresses multicast ont une portée semblable à celle des adresses unicast : local–noeud, local–liaison, local–site et local–organisation.

anycast Une adresse anycast a un seul expéditeur, plusieurs auditeurs et un seul interlocuteur (normalement le "plus proche", conformément à la mesure de distance des protocoles de routage). Par exemple, il peut y avoir plusieurs serveurs Web à l'écoute d'une adresse anycast. Lorsqu'une requête est envoyée à cette adresse, un seul serveur répond.

Une adresse anycast ne se distingue pas d'une adresse unicast. Une adresse unicast devient une adresse anycast lorsque plus d'une interface est configurée avec cette adresse.

Remarque : Il n'existe pas d'adresse de diffusion dans IPv6. Cette fonction est remplacée par l'adresse multicast.

Configuration automatique

Les principaux mécanismes disponibles, permettant à un nœud de s'initialiser et de commencer à communiquer avec d'autres nœuds sur un réseau IPv4 sont le codage "hard–coding", BOOTP et DHCP. Ils fonctionnent assez bien, mais chacun présente quelques difficultés. Le codage "hard–coding" rend difficile la renumérotation non ordonnée, tandis que BOOTP et DHCP exigent une diffusion hôte et dépendent d'un serveur distant.

IPv6 introduit le concept de *portée* aux adresses IP, dont l'une est local-liaison. Un hôte peut ainsi établir une adresse valide à partir d'un préfixe prédéfini local-liaison et de son identificateur local, qui est en général l'adresse MAC (medium access control) de l'interface à configurer. A l'aide de cette adresse, le nœud peut adresser des envois multicast à un serveur, au lieu d'effectuer une diffusion, et dans le cas d'un sous-réseau totalement isolé, risque de ne nécessiter aucune autre configuration d'adresse.

Adresses significatives

Avec IPv4, la seule signification généralement identifiable dans les adresses est la diffusion (en général tout 1 ou tout 0), et les classes (par exemple, une classe D est multicast). Avec IPv6, il est possible d'examiner rapidement le préfixe pour déterminer la *portée* (par exemple, local-liaison), multicast ou unicast, et un mécanisme d'affectation (basé sur le fournisseur, sur l'implantation géographique, etc.).

Les informations de routage peuvent également être chargées explicitement dans les bits supérieurs des adresses, bien que l'IETF n'ait pas encore finalisé ce point (pour les adresses basées sur le fournisseur, les informations de routage sont implicitement présentes dans l'adresse).

Détection d'adresse en double

Lorsqu'une interface est initialisée, ou réinitialisée, elle se sert de la configuration automatique pour essayer d'associer une adresse de type local-liaison à cette interface (l'adresse n'est pas encore affectée à cette interface dans le sens traditionnel). A ce stade, l'interface rejoint les groupes multicast tous nœuds et nœuds sollicités, et leur envoie un message de découverte de voisinage. Avec l'adresse multicast, le noeud peut déterminer si cette adresse local-liaison particulière a été préalablement affectée, puis choisir une autre adresse. Ceci évite une des erreurs communes de gestion de réseau, c'est-à-dire l'affectation de la même adresse à deux interfaces différentes sur le même lien. (Il est encore possible de créer des adresses en double de portée globale pour les nœuds ne se trouvant pas sur le même lien.)

Configuration automatique de découverte voisinage/adresse sans état

Le protocole ND (Neighbor Discovery) pour IPv6 est utilisé par des nœuds (hôtes et routeurs) pour déterminer les adresses de couche liaison pour les voisins connus sur des liens rattachés, et maintient les tables de routage par destination pour les connexions actives. Les hôtes utilisent également ND pour découvrir des routeurs de voisinage désireux d'acheminer des paquets pour leur compte et détectent les adresses de couche liaison modifiées. NDP (Neighbor Discovery Protocol) utilise ICMP (Internet Control Message Protocol) version 6 avec ses propres types de messages uniques. D'une façon générale, le protocole ND IPv6 correspond à la combinaison du protocole ARP IPv4, RDISC (ICMP Router Discovery) et ICMP Redirect (ICMPv4), avec beaucoup d'améliorations.

IPv6 définit le mécanisme de configuration automatique d'une adresse avec et sans état. *La configuration automatique sans état* n'exige pas de configuration manuelle des hôtes, une configuration, éventuelle, minimale des routeurs; et pas de serveur supplémentaire. Le mécanisme sans état permet à un hôte de générer ses propres adresses à l'aide d'une combinaison d'informations disponibles localement et présentées par les routeurs. Les routeurs annoncent les préfixes qui identifient le(s) sous–réseau(x) associés à un lien, tandis que les hôtes génèrent un jeton d'interface qui identifie de façon unique une interface sur un sous–réseau. Une adresse est formée par la combinaison des deux éléments. En l'absence de routeurs, un hôte ne peut générer que des adresses de type local-liaison. Ces adresses sont toutefois suffisantes pour la communication entre nœuds rattachés au même lien.

Simplification de routage

Pour simplifier les problèmes de routage, les adresses IPv6 sont considérées comme deux parties : un préfixe et un ID. Ceci n'est pas très éloigné du découpage des adresses IPv4, mais présente deux avantages :

absence de classe — Il n'y a pas de nombre fixe de bits pour le préfixe ou l'ID, ce qui permet de réduire les pertes dues à une suraffectation.

imbrication — Il est possible d'utiliser un nombre arbitraire de divisions si l'on considère différents nombres de bits comme préfixe.

Cas 1 :

128 bits
Adresse de nœud

Cas 2 :

n bits	128–*n* bits
Préfixe de sous–réseau	ID interface

Cas 3 :

n bits	80-*n* bits	48 bits
Préfixe abonné	ID de sous–réseau	ID interface

Cas 4 :

s bits	*n* bits	*m* bits	128–*s*–*n*–*m* bits
Préfixe abonné	ID zone	ID de sous–réseau	ID interface

En général, IPv4 ne peut aller au delà du cas 3, même avec VLSM. (Il s'agit autant d'un artefact de la longueur d'adresse la plus courte que de la définition des préfixes de longueur variable, mais cela mérite cependant d'être noté.)

Simplification du format d'en-tête

IPv6 simplifie l'en-tête IP, soit par suppression complète soit par déplacement sur un en-tête d'extension de certains champs trouvés dans l'en-tête IPV4, et il définit un format plus souple pour les informations facultatives (en-têtes d'extension). Spécifiquement, notez l'absence de :

- longueur d'en-tête (la longueur est constante)
- identification
- indicateurs
- décalage de fragment (déplacé dans les en-têtes d'extension de fragmentation)
- total de contrôle d'en-tête (l'en-tête de protocole de couche supérieure ou d'extension de sécurité gère l'intégrité des données)

En–tête IPv4 :

Version	IHL	Type de service	Longueur totale	
Identificateur			Identificateur	Décalage fragment (Offset)
Durée de vie		Protocole	Total de contrôle d'en–tête (checksum)	
Adresse source				
Adresse de destination				
Options				Remplissage

En–tête Ipv6 :

Version	Prio	Libellé du flux		
Longueur charge utile			En–tête suivant	Limite de tronçon
Adresse source				
Adresse de destination				

IP*ng* inclut un mécanisme d'options amélioré par rapport à IPv4. Les options IPv6 sont placées dans des en-têtes d'extension séparés qui résident entre l'en-tête IPv6 et l'en-tête de couche transport dans un paquet. La plupart des en-têtes d'extension ne sont pas examinés ou traités par un routeur le long du chemin de livraison de paquets.
Ce mécanisme apporte une grande amélioration aux performance du routeur pour les paquets contenant des options. Dans IPv4, la présence d'options requiert l'examen de toutes les options par le routeur.

Une autre amélioration provient du fait que, contrairement aux options IPv4, les en-têtes d'extension IPv6 peuvent être d'une longueur arbitraire et le nombre total d'options transmises dans un paquet n'est pas limité à 40 octets. Cette fonction, ainsi que la façon dont elle est traitée, permet aux options IPv6 d'être utilisées pour les fonctions qui n'étaient pas pratiques dans IPv4, comme les options d'authentification et d'encapsulage de sécurité IPv6.

Pour améliorer les performances de gestion des en-têtes d'option suivants et du protocole de transport qui suit, les options IPv6 sont toujours un multiple entier de huit octets, pour conserver cet alignement pour les en–têtes suivants.

En utilisant des en-têtes d'extension au lieu d'un spécificateur de protocole et de champs d'options, l'intégration des extensions nouvellement définies est plus facile.

Les spécifications actuelles définissent les en-têtes d'extension comme suit :

- Options bond par bond s'appliquant à chaque bond (routeur) sur le chemin
- En-tête de routage pour un routage de source strict ou non (rarement utilisé)
- Un fragment définit le paquet comme un fragment et contient des informations à ce sujet (les routeur Ipv6 ne fragmentent pas les paquets)
- Authentification Sécurité IP
- Chiffrement Sécurité IP
- Options de destination pour le nœud de destination (ignoré par les routeurs)

Amélioration du contrôle trafic/qualité du service

La qualité du service peut être contrôlée à l'aide d'un protocole de contrôle comme RSVP, et IPv6 fournit une définition de priorité explicite pour les paquets en utilisant le champ de priorité dans l'en-tête IP. Un nœud peut définir cette valeur pour indiquer la priorité relative d'un paquet ou d'un ensemble de paquets, pouvant être alors utilisés par le nœud, un ou plusieurs routeurs, ou la destination pour indiquer que faire du paquet (l'abandonner ou non).

IPv6 spécifie deux types de priorités, une pour le trafic contrôle en cas de congestion, et une pour le trafic non contrôlé en cas de congestion. Il n'y a aucun ordre relatif entre ces deux types.

Le trafic contrôle en cas de congestion est un trafic répondant aux embouteillages par un algorithme de limitation. Dans ce cas, les priorités sont :

0	trafic non caractérisé
1	trafic "de remplissage" (par exemple, informations sur le réseau)
2	transfert de données non assisté (par exemple, messagerie automatique)
3	(réservé)
4	transfert de lot assisté (par exemple, FTP)
5	(réservé)
6	trafic interactif (par exemple, Telnet)
7	trafic de contrôle (par exemple, protocoles de routage)

Le trafic non contrôlé en cas de congestion est un trafic répondant à des situations d'embouteillage par l'abandon (ou simplement la non réexpédition) des paquets, par exemple le trafic vidéo, audio ou autre trafic en temps réel. Les niveaux explicites ne sont pas définis avec des exemples, mais l'ordre est semblable à celui utilisé pour le trafic contrôlé en cas de congestion.

- La valeur la plus basse doit être utilisée pour le trafic que la source est la plus désireuse de rejeter.
- La valeur la plus haute doit être utilisée pour le trafic que la source est la moins désireuse de rejeter.

Ce contrôle de priorité ne s'applique qu'au trafic provenant d'une adresse source particulière. Le contrôle de trafic à partir d'une adresse ne constitue pas une priorité explicitement supérieure à un transfert de lot assisté à partir d'une autre adresse.

Libellé du flux

En-dehors de la définition de priorité de base pour le trafic, IPv6 définit un mécanisme de spécification d'un flux particulier de paquets. En termes IPv6, un *flux* est "une suite de paquets envoyés à partir d'une source spécifique vers une destination spécifique (unicast ou multicast), pour laquelle la source recherche un traitement spécial par les routeurs intervenants."

Cette identification de flux peut servir pour le contrôle de priorité, mais peut également être utilisée pour un certain nombre de contrôles.

Le libellé de flux est choisi de façon aléatoire, et ne doit pas être utilisé pour identifier une caractéristique du trafic différente du flux correspondant. Un routeur ne peut donc pas déterminer qu'un paquet est d'un type particulier (par exemple, FTP) par le seul examen du libellé de flux. Il pourra cependant déterminer qu'il s'agit d'une partie de la même suite de paquets que le dernier paquet portant ce libellé.

Remarque : Dans AIX 4.3 et jusqu'à généralisation de l'utilisation d'IPv6, le libellé de flux est principalement expérimental. Les utilisations et les contrôles impliquant des libellés de flux n'ont pas encore été définis ni standardisés.

Jumbogrammes

La taille d'un paquet IPv4 est limitée à 64K. A l'aide de l'en-tête d'extension jumbo, un paquet IPv6 peut atteindre 2^{32} octets (légèrement plus de 4 giga-octets).

Utilisation de tunnel

La clé d'une transition IPv6 réussie est la compatibilité avec la base installée existante d'hôtes IPv4 et de routeurs. Le maintien de cette compatibilité permet un passage en douceur d'Internet sur IPv6.

Dans la plupart des cas, l'infrastructure de routage IPv6 évolue dans le temps. Pendant le déploiement de l'infrastructure IPv6, l'infrastructure de routage IPv4 existante peut rester fonctionnelle et peut servir à acheminer le trafic IPv6. L'utilisation de tunnels permet d'utiliser une infrastructure de routage IPv4 existante pour acheminer le trafic IPv6.

Les hôtes et routeurs IPv6/IPv4 peuvent utiliser des tunnels pour les datagrammes IPv6 sur des zones de la topologie de routage IPv4 en les encapsulant dans des paquets IPv4. Le tunnel peut être utilisé d'une multitude de façons.

Routeur-routeur	Les routeurs IPv6/IPv4 interconnectés par une infrastructure IPv4 peuvent faire passer dans un tunnel les reliant des paquets IPv6. Dans ce cas, le tunnel fractionne un segment du chemin complet qu'emprunte le paquet IPv6.
Hôte-routeur	Les hôtes IPv6/IPv4 peuvent faire passer dans un tunnel des paquets IPv6 vers un routeur intermédiaire IPv6/IPv4 accessible via une infrastructure IPv4. Ce type de tunnel fractionne le premier segment du chemin complet du paquet.

Hôte-hôte	Les hôtes IPv6/IPv4 interconnectés par une infrastructure IPv4 peuvent faire passer des paquets IPv6 dans un tunnel les reliant. Dans ce cas, le tunnel fractionne tout le chemin qu'emprunte le paquet.
Routeur-hôte	Les routeurs IPv6/IPv4 peuvent faire passer dans un tunnel des paquets IPv6 jusqu'à leur hôte final IPv6/IPv4. Dans ce cas, le tunnel ne fractionne que le dernier segment du chemin complet.

Les techniques de tunnel sont généralement classées en fonction du mécanisme par lequel le nœud d'encapsulage détermine l'adresse du nœud en fin de tunnel. Dans les méthodes routeur-routeur ou hôte-routeur, le paquet IPv6 est acheminé par tunnel vers un routeur. Dans les méthodes hôte-hôte ou routeur-hôte, le paquet IPv6 passe dans un tunnel tout le long jusqu'à sa destination.

Le noeud d'entrée du tunnel (noeud d'encapsulage) crée un en-tête IPv4 d'encapsulage et transmet le paquet encapsulé. Le noeud de sortie du tunnel (noeud de décapsulage) reçoit le paquet encapsulé, supprime l'en-tête IPv4, met à jour l'en-tête IPv6 et traite le paquet IPv6 reçu. Toutefois, le nœud d'encapsulage doit mettre à jour les informations sur l'état du logiciel pour chaque tunnel, par exemple MTU pour chaque tunnel, pour traiter les paquets IPv6 acheminés dans le tunnel.

Sécurité IPv6

Pour plus de détails sur la sécurité IP, versions 4 et 6, reportez-vous au Chapitre 4, page 4-1.

Support IPv6 des adresses locales du site et des liens Multihomed

Plusieurs interfaces peuvent être définies pour un hôte. Un hôte comportant deux ou plusieurs interfaces interactives est dit multihomed. Chaque interface est associée à une adresse de type local. Ces adresses sont suffisantes pour la communication entre nœuds rattachés à un même lien.

Un hôte multihomed est associés à deux ou plusieurs adresses de type local. Dans l'implémentation IPv6 AIX, 4 options permettent de déterminer comment la résolution des adresses de couche liaison s'effectue sur les hôtes multihomed. L'option 1 est activée par défaut.

Option 0 Aucune action multihomed n'est effectuée. Les transmissions sortent par la première interface de type local. Lorsque le protocole NDP doit résoudre les adresses, il envoie (multicast) un message de découverte de voisinage sur chaque interface pour laquelle est définie cette adresse de type local. NDP met le paquet de données en attente jusqu'à ce qu'il reçoive le premier message d'avis de voisinage (Neighbor Advertisement). Le paquet de données est alors transmis par cette liaison.

Option 1 Lorsque le protocole NDP doit résoudre une adresse (lorsqu'il envoie un paquet de données vers une destination et que les informations relatives à la liaison pour le tronçon suivant ne sont pas dans le cache de voisinage (Neighbor Cache), il envoie (multicast) un message de découverte de voisinage sur chaque interface pour laquelle est définie cette adresse de type local. NDP met alors le paquet de données en attente jusqu'à ce qu'il reçoive les informations concernant la liaison. NDP attend de recevoir la réponse de chaque interface. Ceci permet de garantir que les paquets de données sont envoyés par l'intermédiaire des interfaces sortantes appropriées. Si NDP répondait au premier avis de voisinage sans attendre les autres réponses, il pourrait arriver qu'un paquet de données soit envoyé sur une liaison non associée à l'adresse source du paquet. Comme NDP doit attendre toutes les réponses, on constate un certain délai avant l'envoi du premier paquet. De toute façon, un délai est également à prévoir lors de l'attente de la première réponse.

Option 2 Le fonctionnement multihomed est autorisé mais l'expédition d'un paquet de données est limitée à l'interface spécifiée par main_if6. Lorsque le protocole NDP doit résoudre les adresses, il envoie (multicast) un message de découverte de voisinage sur chaque interface pour laquelle est définie cette adresse de type local. Il attend alors le message d'avis de voisinage en provenance de l'interface spécifiée par main_if6 (voir la commande **no**). Dès qu'il reçoit la réponse de cette interface, le paquet de données est envoyé sur cette liaison.

Option 3 Le fonctionnement multihomed est autorisé mais l'expédition d'un paquet de données est limitée à l'interface spécifiée par main_if6 et les adresses de type local ne sont acheminées que pour l'interface spécifiée par main_site6 (voir la commande **no**). Le protocole NDP fonctionne comme avec l'option 2. Pour les applications qui acheminent des paquets de données en utilisant des adresses de type local, sur un hôte multihomed, seule l'adresse locale spécifiée par main_site6 est utilisée.

IPv6 dans AIX : Informations complémentaires

Définitions de format d'adresse

Adresse IPv6

Une adresse IPv6 a une longueur de 128 bits, et s'écrit sous la forme de 8 champs hexadécimaux de 16 bits séparés par des deux–points (:) :

```
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
```

Il est possible raccourcir une adresse IPv6 en comprimant les zéros. Ceci peut être fait une fois par adresse. Les zéros sont condensés par "`::`" (par exemple `4e80::54f:1234`).

Le préfixe correspond aux premiers bits de l'adresse. Il est représenté par la notation "<adresse IPv6>/<longueur>". Par exemple :

- Dans `4e80::123:456:789/10`, le préfixe correspond aux 10 premiers bits de l'adresse `4e80::123:456:789`.
- Le préfixe des adresses multicast est `FF00::/8`, ce qui signifie que toutes les adresses multicast commencent par `FF`.

Le préfixe définit soit :

- le type d'adresse,
- soit, grosso modo l'équivalent des portions d'adresse IPv4 "réseau" et "sous–réseau",
- soit l'ensemble qui définit la route.

L'ID d'interface correspond aux derniers bits de l'adresse et représente un identificateur d'hôte unique. Il est plus ou moins équivalent à la portion "host" de l'adresse IPv4 .

Adresse unicast globale cumulable

Le format d'adresse unicast globale cumuable IPv6 sera utilisé à l'avenir pour le schéma d'adressage du protocole IP.

Reportez–vous à **draft–ietf–ipngwg–unicast–aggr–04.txt** et **draft–ietf–ipngwg–tla–assignment–03.txt**.

EUI–64

EUI–64 est un ID d'interface 64 bits généré automatiquement à partir de l'adresse MAC IEEE 802.

Cette implémentation est décrite dans l'architecture d'adressage **draft–ietf–ipngwg–addr–arch–v2–02.txt**.

Adresses spéciales

Adresses mappées

Une adresse mappée est une adresse basée sur IPv4 utilisée pour la compatibilité avec les hôtes IPv4 :

- Un socket IPv6 peut communiquer avec un hôte exclusivement IPv4 en utilisant comme adresse de destination une adresse mappée.
- Un socket IPv6 peut établir une liaison avec une adresse mappée pour recevoir les paquets en provenance d'un hôte exclusivement IPv4.

Une adresse mappée est représentée sous la forme :

- `::FFFF:a.b.c.d` où `a.b.c.d` correspond à l'adresse IPv4.

ou

- `::FFFF:XXXX:YYYY` où `XXXXYYYY` est la représentation hexadécimale de l'adresse IPv4 `a.b.c.d`.

Adresse compacte

Une adresse compacte est une adresse basée sur IPv4 utilisée pour la compatibilité avec le routage IPv4 dans les tunnels SIT : lorsqu'un paquet IPv6 est envoyé à une adresse compacte, il est encapsulé dans un paquet IPv4. La destination doit décapsuler le paquet avant de le traiter.

Une adresse compacte est représentée sous la forme :

- `::a.b.c.d` où `a.b.c.d` correspond à l'adresse IPv4.

ou

- `::XXXX:YYYY` où `XXXXYYYY` est la représentation hexadécimale de l'adresse IPv4 `a.b.c.d`.

Adresse non spécifiée
L'adresse non spécifiée est composée de 16 octets nuls, représentés sous la forme "`0:0:0:0:0:0:0:0`", ou plus simplement "`::`".

Adresse de bouclage
L'adresse de bouclage, représentée sous la forme "`0:0:0:0:0:0:0:1`", (ou plus simplement "`::1`"), peut être utilisée par un nœud pour s'envoyer à lui–même un datagramme IPv6.

Adresse local–liaison
Les stations non encore configurées avec une adresse IPv6 peuvent utiliser l'adresse local–liaison.

Les adresses local–liaison ne sont définies qu'à l'intérieur d'une liaison et ne peuvent être utilisées par les stations connectées à la même liaison ou au même réseau local. Elles sont automatiquement configurées lors de initialisation de l'interface et permettent la communication entre nœuds voisins.

Ces adresses sont composées d'un préfixe local–liaison (`fe80::/64`) ajouté à un ID d'interface 64 bits généralement en format EUI. Par exemple :
`fe80::4260:8cff:fe2c:9c38`

Méthodes de configuration

La configuration d'un réseau IPv6 s'effectue de la manière suivante :

- Exécution de toute la configuration liée à IPv4
- Lancement de la commande **autoconf6** pour générer les adresses local–liaison et l'interface **sit0** (sur le réseau IPv4 existant), et pour installer les routes unicast et multicast de base.
- Exécution du démon **ndpd–host** pour écouter les avis de routage (RA – Router Advertisements). A mesure de la réception des RA, les adresses sont ajoutées aux interfaces appropriées et les routes sont créées en fonction des besoins.

Pour exécuter ces opérations en utilisant SMIT, procédez comme suit :

1. **smit tcpip**
2. Sélectionnez l'option **IPv6 configuration** et suivez le menu.
3. Sélectionnez l'option **IPv6 daemon/Process Configuration** afin de lancer le processus **autoconf6** et le sous–système **ndpd–host**.

Utilisation de tunnel

L'utilisation de tunnels permet de réaliser des communications IPv6 dans un réseau essentiellement IPv4, et permet une transition progressive vers IPv6.

Une route fait transiter un paquet au travers d'une interface de tunnel, qui encapsule le paquet (en ajoutant un en–tête IPv4 approprié), puis appelle la routine de sortie IPv4.

AIX 4.3 prend en charge deux types de tunnels IPv6 :

- les interfaces SIT (Simple Internet Transition),
- les interfaces CTI (Configured Tunnel Interface).

Tunnels SIT

Les tunnels SIT conviennent aux communications d'hôte à hôte au travers d'une hiérarchie de routage IPv4.

L'interface est configurée sous la forme d'une adresse compacte, à partir de l'adresse IPv4 de l'interface IPv4 associée. Tout le trafic destiné à une adresse compacte est acheminé via cette interface.

L'interface **sit0** est généralement ajoutée par **autoconf6** au démarrage du système.

Un tunnel SIT n'est pas fermé dans la mesure où seule l'extrémité locale est configurée.

Tunnels CTI

Les tunnels CTI sont adaptés aux communications entre routeurs.

L'interface est configurée à partir des adresses source et de destination IPv6 et IPv4 spécifiées par l'utilisateur. Le trafic est acheminé via l'interface CTI appropriée par une entrée particulière de la table de routage.

L'interface **cti0** (de même que toute autre interface cti) doit être ajoutée par l'administrateur système.

Un tunnel **cti** est un tunnel fermé dans la mesure où les deux extrémités du tunnel doivent être configurées.

Serveurs de noms

Les serveurs de noms fonctionnent pratiquement comme sous IPv4.

- La zone d'acheminement utilise des enregistrements IPv6 **AAAA** au lieu d'enregistrements **A** (voir l'exemple).
- La zone de retour utilise le domaine **IP6.INT** au lieu du domaine **in–addr.arpa**, tout en conservant les enregistrements **PTR** (voir l'exemple).
- Les enregistrements **PTR** du domaine **IP6.INT** correspondent à l'adresse IPv6 inversée, chaque partie étant séparée de la suivante par un point.
- Les connexions IPv4 sont utilisées pour transmettre les requêtes.

Exemple de fichier de la zone d'acheminement

```
$ORIGIN merl.century.com
ipv6    9999999 IN      SOA     gtw.merl.century.com.
root.gtw.merl.century.com.
(       1072 3600 300 3600000 3600)
     9999999 IN NS elvis.merl.century.com.
$ORIGIN ipv6.merl.century.com.
nobody-v6-11    IN      AAAA    fe80::99:9999:1997
danny-v6-co     IN      AAAA    ::9.3.114.56
danny-v6-11     IN      AAAA    fe80::260:97ff:fea3:9234
```

Exemple de fichier de la zone de retour

```
$ORIGIN INT.
IP6     9999999 IN      SOA     gtw.merl.century.com.
root.gtw.merl.century.com.
(       1072 3600 300 3600000 3600)
     9999999 IN NS elvis.merl.century.com.
$ORIGIN IP6.INT.
8.c.7.5.1.f.e.f.f.f.c.8.0.6.2.4.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f IN
PTRdaisy-v6-11.ipv6.merl.century.com
8.c.7.5.1.f.e.f.f.f.c.8.0.6.2.4.0.0.0.0.0.0.0.2.7.0.0.0.c.e.f IN
PTRdaisy-v6-sl.ipv6.merl.century.com
```

Clients du service de noms

Pour préserver la compatibilité binaire, les programmes de résolution ne retournent que des adresses IPv4, à moins que l'option de résolution **RES_USE_INET6** ne soit définie. Différentes méthodes permettent de définir cette option :

- Affecter à la variable d'environnement **RES_OPTIONS** la valeur **inet6** active l'option pour tous les processus exécutant le shell en cours.
- Appeler **res_init()** et configurer l'indicateur **RES_USE_INET6** dans **_res.options** (dans le code d'application) active l'option pour le processus appelant.

```
(void) res_init();
_res.options |= RES_USE_INET6;
```

Portage d'applications

Pour la plupart des jetons contenant "in" ou "inet", utilisez à la place le nom IPv6. Quelques exemples :

v4 token	v6 token
AF_INET	AF_INET6
sockaddr_in	sockaddr_in6
in_addr	in6_addr
<netinet/in.h>	<netinet/in.h>
<netinet/ip.h>	<netinet/ip6.h>
INADDRSZ	IN6ADDRSZ
sin_addr	sin6_addr
sin_len	sin6_len

Utilisez **inet_ntop()** et **inet_pton()** à la place de **inet_ntoa()** et **inet_aton()** pour les conversions entre formats ASCII et binaires.

Utilisez **gethostbyname2()** ou **getaddrinfo()** au lieu de **gethostbyname()**.

Lisez également la directive RFC 2133.

Recherche de MTU d'accès

L'algorithme de recherche de MTU d'accès est toujours activé dans IPv6.

Restrictions concernant les implémentations AIX

Interfaces réseau

IPv6 prend en charge les interfaces réseau suivantes :

- Token-ring
- Ethernet (Standard Ethernet et IEEE 802.3)
- FDDI

Applications

IPv6 prend en charge les applications suivantes :

- ping
- telnet/telnetd
- ftp/ftpd
- tftp/tftpd
- crash/ndb
- iptrace/ipreport/tcpdump
- traceroute
- resolver routines/named
- inetd
- rsh/rcp/rshd
- rexec/rexecd
- rlogin/rlogind
- ifconfig/netstat/route/nslookup

- mail/sendmail
- autoconf6/ndpd–host/ndp
- nslookup
- ndpd–router à partir de AIX 4.3.2 et ultérieures
- gated avec RIPng, BGP4+ à partir de AIX 4.3.2 et ultérieures

Routage dans AIX 4.3.0 et 4.3.1

- AIX IPv6 ne peut être utilisé que comme hôte IPv6 ou comme routeur IPv6/IPv4 avec un tunnel. IPv6 ne peut servir de routeur IPv6/IPv6.
- Il n'est pas possible d'envoyer et d'acheminer des paquets entre deux interfaces IPv6.
- Par ailleurs, les applications de routage ne sont pas encore capables de comprendre les protocoles de routage IPv6.
- Les avis de routage ne sont pas générés et l'application **ndpd–router** n'est pas prise en charge.

Routage à partir de AIX 4.3.2

- AIX IPv6 peut être à la fois hôte et routeur en permettant à la station d'être multihomed. IPv6 peut envoyer et acheminer des paquets entre deux interfaces IPv6.
- La commande **ndpd–router** est prise en charge.
- Le protocole de routage RIPng est pris en charge par les démons **npd–router** et **gated**.
- BGP4+ est pris en charge par le démon **gated**.

Adresse Anycast

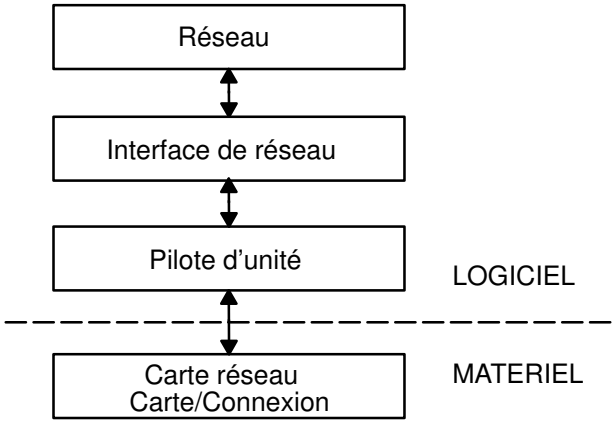
Cette fonction n'est pas prise en charge.

Suivi de paquet

Le suivi de paquet consiste à contrôler le parcours d'un paquet à travers les couches jusqu'à destination. La commande **iptrace** permet d'effectuer ce contrôle au niveau de la couche Interface de réseau. La commande **ipreport** génère en sortie un compte rendu de suivi aux formats hexadécimal et ASCII. La commande **trpt** effectue le contrôle au niveau de la couche transport pour le protocole TCP. La sortie de la commande **trpt** est plus détaillée : elle comprend des informations sur la date et l'heure, l'état TCP et la mise en séquence des paquets.

En-têtes de paquet au niveau interface de réseau

Au niveau de la couche Interface de réseau, des en-têtes sont associés aux données sortantes (voir figure). Les paquets transitent alors par la carte de réseau vers le réseau correspondant. Ils traversent parfois plusieurs passerelles avant d'atteindre leur destination. Une fois arrivés au réseau de destination, ces en-têtes sont supprimés et les données envoyées à l'hôte concerné.



Flux de paquets à travers l'interface de réseau

Ce processus s'applique aux informations d'en-tête de plusieurs interfaces de réseau courantes.

En-têtes de trame pour carte Ethernet

Le tableau ci-après représente un en-tête de trame IP (Internet Protocol) ou ARP (Address Resolution Protocol) pour la carte Ethernet.

En-tête de trame de carte Ethernet		
Zone	**Longueur**	**Définition**
DA	6 octets	Adresse de destination.
SA	6 octets	Adresse source. Si le bit 0 de cette zone est positionné à 1, l'information de routage (RI) est présente.
Type	2 octets	Type du paquet : IP ou ARP. IP ou ARP (le type est représenté par des numéros, comme indiqué ci-dessous).

Numéros de la zone Type :

IP	0800
ARP	0806

En-tête de trame pour réseau en anneau à jeton

L'en-tête MAC (Medium Access Control) pour carte anneau à jeton se compose des cinq zones ci-dessous :

En-tête MAC pour réseau en anneau à jeton		
Zone	**Longueur**	**Définition**
AC	1 octet	Contrôle d'accès. La valeur x'00' confère à l'en-tête la priorité 0.
FC	1 octet	Contrôle de la zone. La valeur x'40' indique une trame LLC (Logical Link Control).
DA	6 octets	Adresse de destination.
SA	6 octets	Adresse source. Si le bit 0 de cette zone est positionné à 1, l'information de routage (RI) est présente.
RI	18 octets	Information de routage. Les valeurs possibles sont fournies plus loin.

L'en-tête MAC comprend deux zones d'information de routage de 2 octets chacune : le contrôle de routage (RC) et les numéros de segment. Huit numéros de segment au maximum peuvent être utilisés pour désigner les destinataires d'une diffusion limitée. Les informations RC sont fournies aux octets 0 et 1 de la zone RI. Les deux premiers bits de la zone RC peuvent prendre les valeurs suivantes :

bit (0) = 0 Utilisation de la route de non–diffusion, spécifiée dans la zone RI.

bit (0) = 1 Création de la zone RI et diffusion vers tous les anneaux.

bit (1) = 0 Diffusion via tous les ponts.

bit (1) = 1 Diffusion via certains ponts.

L'en-tête LLC (contrôle de liaison logique) comporte les cinq zones suivantes :

En-tête LLC 802.3		
Zone	**Longueur**	**Définition**
DSAP	1 octet	Point d'accès au service de destination. La valeur est x'aa'.
SSAP	1 octet	Point d'accès au service source. La valeur est x'aa'.
CONTROL	1 octet	Commandes et réponses LLC (contrôle de liaison logique). Trois valeurs possibles (présentées plus loin).
PROT_ID	3 octets	ID de protocole. Cette zone est réservée. Sa valeur est de x'0'.
TYPE	2 octets	Type du paquet : IP ou ARP.

Valeurs de la zone CONTROL

x'03'	Trame d'information non numérotée (UI). Mode de transmission normale ou non séquentielle des données de la carte anneau à jeton sur le réseau. Les données sont mises en séquence par TCP/IP.
x'AF'	Trame XID (Exchange Identification). Elle transmet les caractéristiques de l'hôte émetteur.
x'E3'	Trame de test. Cette trame teste la route de transmission, et renvoie les données reçues.

En-têtes de trame 802.3

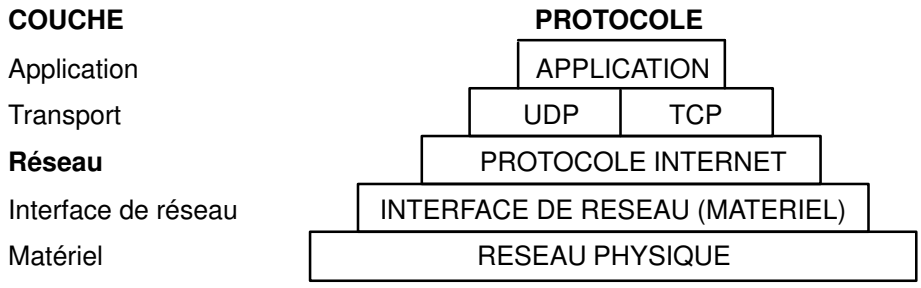
L'en-tête MAC (Medium Access Control) pour la carte 802.3 comprend les zones :

En-tête MAC 802.3		
Zone	**Longueur**	**Définition**
DA	6 octets	Adresse de destination.
SA	6 octets	Adresse source. Si le bit 0 de cette zone est positionné à 1, l'information de routage (RI) est présente.

L'en-tête LLC (Logical Link Control) pour la carte 802.3 est identique à l'en-tête MAC de l'anneau à jeton.

Protocoles Internet de niveau réseau

Les protocoles Internet de niveau réseau gèrent la communication entre les machines. Autrement dit, c'est la couche qui assure le routage TCP/IP. Ces protocoles réceptionnent les demandes de transmission de paquets (dotés de l'adresse réseau de la machine destinataire) issues de la couche Transport, convertissent les paquets en datagrammes et les communiquent à la couche Interface de réseau (voir figure).



Couche réseau des protocoles TCP/IP

TCP/IP fournit les protocoles requis pour être conforme à RFC 1100 *(Official Internet Protocols)*, ainsi que d'autres protocoles couramment utilisés par les machines hôtes en environnement Internet.

Remarque : Sous TCP/IP, l'utilisation des numéros de réseau, version, prise, service et protocole Internet est également conforme à RFC 1010 *(Assigned Numbers)*.

Protocole de résolution d'adresse

Le premier protocole intervenant au niveau réseau est le protocole de résolution d'adresse (ARP). Ce protocole est chargé de traduire dynamiquement les adresses Internet en adresses matérielles uniques sur les réseaux locaux.

Pour illustrer le fonctionnement d'ARP, prenons le cas de deux noeuds, `jim` et `fred`. Si le nœud `jim` désire communiquer avec `fred`, et que `jim` et `fred` ne résident pas sur le même réseau local, `jim` et `fred` doivent utiliser des *ponts*, *routeurs* ou *passerelles*, et des

adresses IP. Si `jim` et `fred` se trouvent sur le même réseau local l'adresse IP n'est pas suffisante. Au sein d'un réseau local, les nœuds requièrent en outre les adresses matérielles (niveau inférieur).

Les noeuds implantés sur le même segment d'un réseau local font appel au protocole ARP pour déterminer l'adresse matérielle d'autres noeuds. Tout d'abord, le noeud `jim` diffuse une demande ARP pour connaître l'adresse matérielle de `fred`. Cette demande comporte les adresses IP et matérielles de `jim` et l'adresse IP de `fred`. Lorsque `fred` reçoit la requête, il place une entrée destinée à `jim` dans sa mémoire cache ARP (utilisée pour établir rapidement l'équivalence entre l'adresse IP et l'adresse matérielle). Ensuite, `fred` renvoie directement à `jim` une réponse ARP avec l'adresse IP et l'adresse matérielle de `fred` Lorsque le nœud `jim` reçoit cette réponse, il place à son tour une entrée destinée à `fred` dans sa mémoire cache ARP.

Dès lors, `jim` peut correspondre directement avec `fred` sans recours au protocole ARP (à moins que l'entrée en mémoire cache ARP destinée à `fred` ne soit supprimée).

Contrairement à la plupart des protocoles, les en-têtes de paquet ARP n'ont pas un format fixe. Le message est conçu pour s'adapter à diverses technologies de réseau, telles que :

- Carte de réseau local Ethernet (qui prend en charge les protocoles Ethernet et 802.3)
- Carte de réseau en anneau à jeton
- Carte de réseau FDDI (Fiber Distributed Data Interface)

En revanche, ARP ne traduit pas les adresses pour SLIP ou convertisseur optique série, car il s'agit de connexions point à point.

Les tables de traduction sont tenues à jour par le noyau et les utilisateurs ou les applications n'ont pas d'accès direct à ARP. Lorsqu'une application envoie un paquet Internet à l'un des pilotes d'interface, le pilote demande l'équivalence d'adresse. Si cette équivalence ne figure pas dans la table, un paquet ARP de diffusion est envoyé aux hôtes du réseau local via le pilote d'interface demandeur.

Les entrées de la table d'équivalence (mappage) ARP sont supprimées au bout de 20 minutes et les entrées incomplètes au bout de 3 minutes. Pour insérer une entrée permanente dans la table, lancez la commande **arp** assortie du paramètre *pub* :

```
arp -s 802.3 host2 0:dd:0:a:8s:0 pub
```

Lorsqu'un hôte prenant en charge ARP reçoit un paquet de demande ARP, il note l'adresse IP et l'adresse matérielle du système demandeur et met à jour sa table d'équivalence. Si son adresse IP ne correspond pas à l'adresse demandée, il rejette le paquet. Sinon, il envoie un paquet de réponse au système demandeur. Le système demandeur enregistre la nouvelle équivalence pour l'appliquer aux paquets Internet similaires en attente.

Protocole ICMP

Le deuxième protocole intervenant au niveau réseau est le protocole de message de contrôle interréseau (ICMP). Ce protocole, partie intégrante de toute implémentation IP, gère les messages d'erreur et de contrôle pour IP. Il est utilisé par les passerelles et les systèmes hôtes pour transmettre les comptes rendus d'incidents aux machines émettrices d'un paquet. Il est chargé de :

- tester l'accessibilité d'une destination,
- signaler les erreurs de paramètres dans un en-tête de datagramme,
- effectuer la synchronisation horaire et évaluer le temps de transit,
- obtenir les adresses Internet et les masques de sous-réseau.

Remarque : ICMP utilise le support de base d'IP comme s'il était un protocole de niveau supérieur. ICMP fait partie intégrante du protocole IP et doit être mis en œuvre par tout module IP.

ICMP rend compte des anomalies de l'environnement de communications sans garantir pour autant la fiabilité du protocole IP. Autrement dit, il ne garantit pas la livraison d'un paquet IP ni l'envoi d'un message ICMP à l'hôte source en cas d'échec ou d'erreur de livraison.

Les messages ICMP sont émis dans les cas suivants :

- destination d'un paquet inaccessible,
- capacité tampon insuffisante sur l'hôte passerelle pour la réexpédition d'un paquet,
- passerelle capable d'obtenir que l'hôte achemine le courrier via un chemin plus court.

TCP/IP peut envoyer et recevoir plusieurs types de messages ICMP. Le protocole ICMP, intégré au noyau, ne dispose d'aucune interface API.

Types de messages ICMP

ICMP peut envoyer ou recevoir des messages du type :

echo request	Demande d'écho envoyée par les hôtes et les passerelles pour tester l'accessibilité de la destination.
information request	Demande d'information envoyée par les hôtes et les passerelles pour obtenir l'adresse Internet d'un réseau auquel ils sont connectés. Avec ce type de message, la portion réseau de l'adresse de destination IP est positionnée à 0.
timestamp request	Demande de l'heure courante à la machine de destination.
address mask request	Demande de masque d'adresse envoyée par l'hôte pour identifier son masque de sous-réseau. Cette demande est envoyée à une passerelle s'il en connaît l'adresse ou sous forme de message de diffusion.
destination unreachable	(Destination inaccessible) Message envoyé lorsqu'une passerelle ne parvient pas à livrer un datagramme IP.
source quench	Demande effectuée auprès de l'émetteur de datagrammes lorsque son débit d'émission est trop élevé pour que les passerelles ou hôtes puissent traiter les datagrammes entrants.
redirect message	Message de redirection envoyé lorsqu'une passerelle détecte qu'un hôte n'utilise pas une route optimale.
echo reply	Réponse d'écho renvoyée, par la machine réceptrice, à l'émetteur d'une demande d'écho.
information reply	Message envoyé par les passerelles en réponse aux demandes d'adresse (avec les zones source et destination du datagramme IP renseignées).
timestamp reply	Réponse indiquant l'heure courante.
address mask reply	Réponse de masque d'adresse envoyée aux machines qui requièrent des masques de sous-réseau.
parameter problem	Message envoyé lorsqu'un hôte ou une passerelle relève une anomalie dans un en-tête de datagramme.

time exceeded	Message envoyé lorsque les conditions ci–dessous sont réunies : • A chaque datagramme IP est associée une durée de vie (nombre de bonds), décrémentée par chaque passerelle. • Un datagramme est rejeté par une passerelle, sa durée de vie ayant atteint la valeur 0.
Internet Timestamp	Horodateur Internet utilisé pour enregistrer les dates et heures durant le parcours.

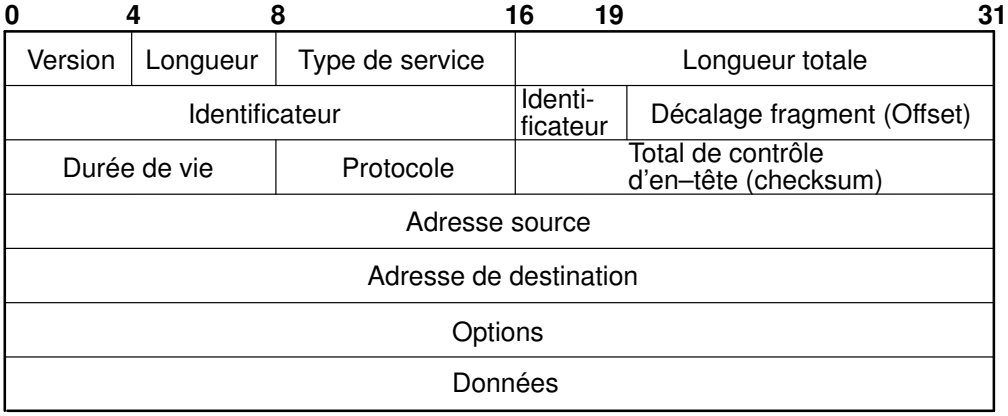
Protocole Internet

Le troisième protocole intervenant au niveau réseau est le protocole Internet (IP). Il effectue la livraison des paquets pour Internet, sans garantie de livraison (aucun acquittement de message n'est exigé auprès des hôtes émetteur, récepteur et intermédiaires) et sans connexion (chaque paquet d'informations est traité séparément).

IP assure l'interface avec les protocoles de niveau Interface de réseau. Les connexions physiques d'un réseau transmettent l'information sous forme d'une trame composée d'un en-tête et de données. L'en-tête contient les adresses source et destination. IP utilise un datagramme Internet, contenant des informations similaires à la trame physique (son en–tête comporte également les adresses source et destination des données).

IP définit le format des données acheminées sur le réseau Internet (voir figure).

Bits



En-tête de paquet IP

Définitions des zones d'en-tête IP

Version	Version IP utilisée. La version courante du protocole IP est 4.
Longueur	Longueur de l'en-tête du datagramme, en nombre de mots de 32 bits.
Type de service	Zone comprenant cinq champs qui définissent pour le paquet concerné, le type de priorité, le délai, le débit et le niveau de fiabilité souhaités. Cette demande n'est pas garantie par Internet. Les paramètres par défaut de ces cinq champs sont normaux. Actuellement, cette zone n'est pas utilisée par Internet de façon généralisée. La mise en œuvre d'IP est conforme à la spécification IP RFC 791, *Internet Protocol*.

Longueur totale	Longueur du datagramme, en octets, incluant l'en-tête et les données. La fragmentation en paquets au niveau des passerelles et le réassemblage à destination sont assurés. La longueur totale du paquet IP peut être configurée interface par interface à l'aide du raccourci Web-based System Manager **wsm network**, de la commande **ifconfig** ou via le raccourci **smit chinet**. Pour déclarer ces valeurs comme permanentes dans la base de données de configuration, utilisez Web-based System Manager ou SMIT, et pour les définir ou les modifier dans le système en exécution, utilisez la commande **ifconfig**.
Identificateur	Nombre entier unique identifiant le datagramme.
Indicateurs (flags) de fragment	Zone contrôlant, avec la zone Identification, la fragmentation du datagramme : indique si le datagramme doit être fragmenté et si le fragment courant est le dernier.
Décalage fragment (Offset)	Décalage du fragment dans le datagramme d'origine, en unités de 8 octets.
Durée de vie	Durée de rétention du datagramme sur Internet. Ce paramètre évite de conserver indéfiniment sur Internet les datagrammes qui n'ont pas abouti. La durée de rétention par défaut est de 255 secondes.
Protocole	Type de protocole de niveau supérieur.
Total de contrôle d'en–tête (checksum)	Nombre calculé pour assurer l'intégrité des valeurs d'en-tête.
Adresse source	Adresse Internet de l'hôte émetteur.

Adresse de destination
: Adresse Internet de l'hôte récepteur.

Options
: Options de test et de mise au point du réseau. Zone facultative pour certains datagrammes.

  End of Option List
  : (Fin de liste d'options) Utilisé à la fin de la liste des options (et non de chaque option) uniquement si la fin de la liste ne coïncide pas avec la fin de l'en–tête IP. Cette option n'est utilisée que si les options excèdent la longueur du datagramme.

  No Operation
  : Permet l'alignement avec d'autres options. Par exemple, alignement à 32 bits du début de l'option suivante.

  Loose Source and record Route
  : Informations de routage fournies par la source du datagramme Internet aux passerelles, qui les utilisent pour expédier le datagramme à destination et les enregistrent. Il s'agit d'une route source *libre* : en effet, la passerelle ou l'IP hôte peut utiliser n'importe quelle route via un nombre quelconque de passerelles intermédiaires pour atteindre l'adresse suivante dans la route.

  Strict Source and record Route
  : Informations de routage fournies par la source du datagramme Internet aux passerelles, qui les utilisent pour expédier le datagramme à destination et les enregistrent. Il s'agit d'une route source *imposée* : en effet, la passerelle ou l'IP hôte doit envoyer le datagramme directement à l'adresse suivante spécifiée par la route source en passant par le réseau direct indiqué dans l'adresse, pour atteindre la passerelle ou l'hôte suivant spécifié dans la route.

  Record Route
  : (Route de suivi). Cette option permet d'enregistrer le parcours suivi par le datagramme Internet.

  Stream Identifier
  : (Indicateur de flot). Cette option véhicule un identificateur de flot (stream) à travers des réseaux qui ne prennent pas en charge le concept de flot.

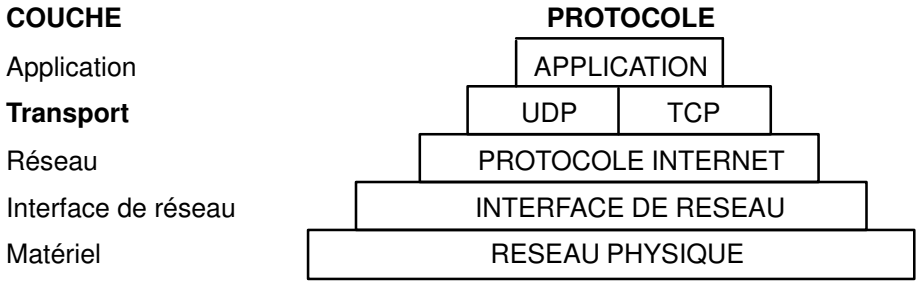
  Internet Timestamp
  : Enregistre la date et l'heure le long du parcours du datagramme.

L'en-tête IP est automatiquement préfixé aux paquets sortants, et supprimé des paquets entrants qui vont être envoyés aux protocoles de niveau supérieur. Le protocole IP procure un système d'adressage universel des hôtes sur le réseau Internet.

Protocoles Internet de niveau transport

Les protocoles TCP/IP de niveau transport (voir figure) permettent aux programmes d'application de communiquer entre eux. Les protocoles UDP (User Datagram Protocol) et

TCP (Transmission Control Protocol) en sont les principaux : ils autorisent l'interconnexion d'hôtes Internet et l'échange de messages entre applications implantées sur des hôtes différents. Le mécanisme est le suivant : lorsqu'une application envoie à la couche Transport une demande d'expédition de message, les protocoles UDP et TCP fragmentent l'information en paquets qu'ils dotent d'un en-tête portant l'adresse de destination. Ces paquets sont alors soumis par les protocoles à la couche réseau. Pour déterminer la destination exacte du message, les protocoles TCP et UDP se servent des ports de protocole de l'hôte.



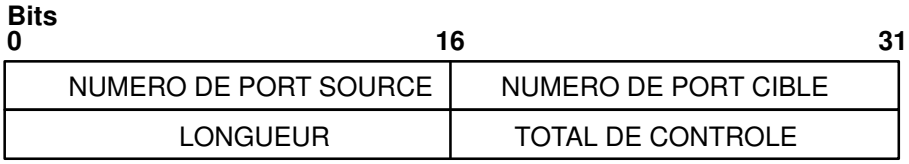
Couche Transport de la suite de protocoles TCP/IP

Les protocoles et applications de niveau supérieur utilisent UDP pour les connexions datagramme et TCP pour les connexion Stream (trains de données). Ces protocoles sont mis en œuvre par l'interface Sockets du système d'exploitation.

Protocole UDP

Le protocole UDP intervient lorsqu'une application de réseau doit envoyer des messages à une application ou un process d'un autre réseau : il fournit aux applications d'hôtes Internet le moyen de communiquer par datagramme. L'émetteur d'un message ne connaît pas les process actifs au moment de l'envoi, c'est pourquoi le protocole UDP utilise les ports de protocole de destination (ou sur un hôte, points de destination abstraits dans une machine), identifiés par des nombres entiers positifs, pour envoyer les messages à un ou plusieurs points de destination. A la réception des messages, les ports de protocole placent les messages dans des files d'attente, où ils seront récupérés en temps voulu par les applications du réseau récepteur.

UDP fait appel à l'IP sous–jacent pour envoyer ses datagrammes, il assure donc la livraison des messages sans connexion comme le protocole IP, sans garantie de livraison ni de protection contre la duplication. UDP présente cependant deux particularités : il autorise l'émetteur à spécifier le numéro des ports source et cible et calcule le total de contrôle de l'en-tête et des données. Il offre ainsi aux applications émettrices et réceptrices un moyen de fiabiliser la livraison (voir figure). Les applications qui exigent une garantie de livraison des datagrammes doivent exercer elles-mêmes un contrôle si elles utilisent UDP. Les applications qui exigent une garantie de livraison des flots de données doivent recourir à TCP.



En-tête de paquet UDP

Définitions des zones d'en-tête UDP

Numéro de port source	Adresse du port de protocole émetteur de l'information.
Numéro de port cible	Adresse du port de protocole récepteur de l'information.

Longueur	Longueur en octets du datagramme UDP.
Total de contrôle (Checksum)	Contrôle du datagramme UDP sur la base du même algorithme que le protocole IP.

L'interface de programmation d'applications (API) avec UDP est constituée d'un ensemble de sous-routines de bibliothèque fourni par l'interface Sockets.

Protocole TCP

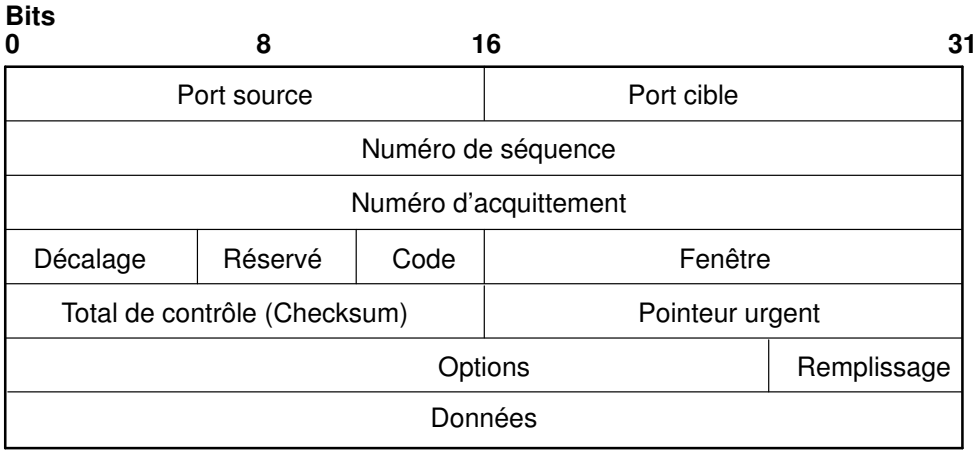
Le protocole TCP (Transmission Control Protocol) assure le transfert fiable des flots entre les hôtes Internet. Comme UDP, il fait appel au protocole sous-jacent IP pour véhiculer les datagrammes et en assurer la transmission par bloc en flot continu d'un port de process à l'autre. Contrairement à UDP, TCP garantit que les messages seront livrés au process destinataire sans que les données soient altérées, perdues, dupliquées ou restituées dans le désordre. Ainsi, les programmeurs d'applications ne sont pas contraints de gérer ce type d'erreurs dans leur logiciel.

TCP présente les caractéristiques suivantes :

Transfert de données de base	TCP peut véhiculer entre ses utilisateurs un flot continu d'octets 8 bits en regroupant des octets en segments pour les transmettre par Internet. Avec TCP, la taille des segments atteint au moins 1024 octets. En général, c'est TCP qui détermine le moment propice pour assembler et expédier les paquets.
Fiabilité	TCP doit récupérer les données altérées, perdues, dupliquées ou désorganisées par Internet. Pour ce faire, il affecte un numéro de séquence à chaque octet transmis et exige un accusé de réception positif (ACK) de la part du TCP récepteur. S'il ne reçoit pas cet accusé après un certain délai, les données sont retransmises. Ce délai est fixé dynamiquement pour chaque connexion, en fonction du temps de transmission aller-retour. Côté destinataire, les numéros de séquence servent à réordonner les segments et à éliminer les doublons. Les données altérées sont traitées grâce au total de contrôle ajouté à chaque segment : ce total est vérifié à la réception des segments et les segments altérés sont rejetés.
Contrôle de flux	TCP permet de réguler le débit des données émises, en associant à chaque accusé de réception une fenêtre indiquant l'intervalle de numéros de séquence admis au-delà du dernier segment reçu. La fenêtre précise le nombre d'octets que l'émetteur est autorisé à envoyer avant de recevoir la prochaine autorisation.
Multiplexage	TCP permet à un grand nombre de process d'un même hôte d'utiliser simultanément les fonctions de communication TCP. TCP reçoit un ensemble d'adresses de port pour chaque hôte et combine le numéro de port à l'adresse réseau et à l'adresse hôte pour pouvoir identifier chaque prise de façon unique (une paire de prises identifiant à son tour chaque connexion de façon unique).

Connexions	TCP doit initialiser et tenir à jour certaines informations d'état pour chaque flot de données. La combinaison de ces informations (prises, numéros de séquence, tailles de fenêtre) est appelée "connexion", chacune d'elles étant identifiée par une paire de prises uniques, une pour chaque extrémité.
Priorité et protection	Les utilisateurs de TCP peuvent spécifier un niveau de priorité et de protection pour leurs communications. Sinon, des valeurs par défaut sont prévues.

La figure d'un **en-tête de paquet TCP** illustre ces caractéristiques.



En-tête de paquet TCP

Définitions de zones d'en-tête TCP

Port source	Numéro de port du programme d'application source.
Port cible	Numéro de port du programme d'application cible.
Numéro de séquence	Numéro d'ordre du premier octet de données dans le segment.
Numéro d'acquittement	Numéro identifiant la position du plus grand octet reçu.
Décalage	Décalage (Offset) de la portion de données du segment.
Réservé	Zone réservée à un usage ultérieur.
Code	Bits de contrôle servant à identifier l'objet d'un segment :
	URG La zone Pointeur urgent est valide.
	ACK La zone Acquittement est valide.
	PSH Le segment requiert un PUSH.
	RTS Réinitialise la connexion.
	SYN Synchronise les numéros de séquence.
	FIN Fin du flot d'octets.
Fenêtre	Volume de données admissible par la destination.
Total de contrôle (Checksum)	Vérifie l'intégrité des données et de l'en-tête du segment.

Pointeur urgent Indique les données à livrer dès que possible. Le pointeur marque la fin des données urgentes.

Options

End of Option List
(Fin de liste d'options) Utilisé à la fin de la liste des options (et non de chaque option) uniquement si la fin de la liste ne coïncide pas avec la fin de l'en–tête TCP.

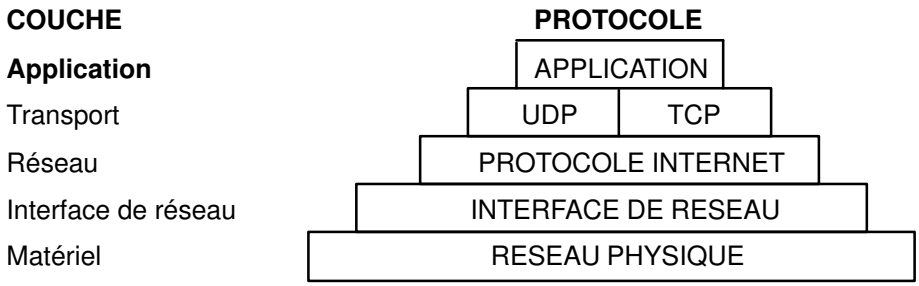
No Operation Indique la limite entre deux options. Par exemple, alignement du début d'une option suivante sur un mot. L'émetteur n'étant pas obligé d'utiliser cette option, le destinataire doit être prêt à traiter les options même ne commençant pas sur un mot.

Maximum Segment Size
Taille maximale de segment acceptable par TCP (indiquée dans la demande de connexion initiale).

L'interface de programmation d'applications (API) avec TCP est constituée d'un ensemble de sous-routines de bibliothèque fourni par l'interface Sockets.

Protocoles Internet de niveau application

Au niveau du programme d'application, TCP/IP met en œuvre des protocoles Internet de niveau supérieur (voir figure) : lorsqu'une application doit envoyer des données à une application sur un hôte différent, les informations sont envoyées aux protocoles de niveau transport pour être préparées à la transmission.



Couche Application de la suite de protocoles TCP/IP

Les protocoles Internet de niveau application officiels englobent :

- Protocole (DOMAIN)
- Protocole EGP (Exterior Gateway Protocol)
- Protocole FTP (File Transfer Protocol)
- Protocole FINGER
- Protocole TELNET
- Protocole TFTP (Trivial File Transfer Protocol).

TCP/IP met en œuvre d'autres protocoles de niveau supérieur, non officiels, mais couramment utilisés par la communauté Internet pour les programmes d'application :

- Protocole HELLO
- Protocole EXEC (Remote Command Execution Protocol)
- Protocole LOGIN

- Protocole SHELL
- Protocole RIP
- Protocole TIMED

TCP/IP ne fournit pas d'interface API à ces protocoles.

Protocole DOMAIN

Le protocole DOMAIN permet à un système hôte membre d'un domaine de jouer le rôle de *serveur de noms* auprès des autres systèmes hôtes de son domaine. Il utilise comme protocole sous-jacent le protocole UDP ou TCP et permet à un réseau local d'affecter des noms d'hôte dans son domaine indépendamment des autres domaines. Normalement, le protocole utilisé est UDP, mais si la réponse UDP est tronquée, DOMAIN fait appel au protocole TCP. Le protocole DOMAIN de TCP/IP prend en charge les deux.

Pour résoudre les noms et adresses Internet, les routines de résolution locales du système d'appellation hiérarchique DOMAIN peuvent recourir à la base de résolution de noms locale tenue par le démon **named**. Si le nom demandé par l'hôte ne figure pas dans cette base, la routine de résolution interroge un serveur de noms DOMAIN distant. Dans tous les cas, en cas d'échec, la routine tente d'utiliser le fichier **/etc/hosts.**

Remarque : TCP/IP configure les routines de résolution locales pour le protocole DOMAIN, si le fichier local **/etc/resolv.conf** existe. Sinon, TCP/IP les configure pour qu'elles utilisent la base de données **/etc/hosts**.

TCP/IP implémente le protocole DOMAIN dans le démon **named** et les routines de résolution, mais ne lui fournit pas d'interface API.

Protocole EGP

Le protocole EGP (Exterior Gateway Protocol) est le mécanisme qui permet à la passerelle extérieure d'un *système autonome* de partager les informations de routage avec des passerelles extérieures d'autres systèmes autonomes.

Systèmes autonomes

Un système autonome est un groupe de réseaux et de passerelles sous la responsabilité d'une autorité administrative. Les passerelles sont dites *intérieures limitrophes* si elles résident sur le même système autonome et *extérieures limitrophes* si elles résident sur des systèmes autonomes différents. Les passerelles qui échangent des informations de routage via le protocole EGP sont appelées *passerelles limitrophes* ou *homologues EGP.*
Le protocole EGP permet aux passerelles de systèmes autonomes d'accéder aux informations de leurs homologues EGP.

Via EGP, une passerelle extérieure peut demander à échanger des informations d'accès avec une autre passerelle extérieure. EGP vérifie en permanence que ses passerelles homologues répondent aux demandes, et les aident dans ces échanges par des messages de mise à jour de routage.

EGP limite la portée d'une passerelle extérieure aux réseaux de destination accessibles en tous points dans le système autonome de cette passerelle. Autrement dit, une passerelle extérieure utilisant EGP peut transmettre les informations aux passerelles EGP limitrophes, mais ne peut fournir des informations concernant ses passerelles limitrophes hors de son système autonome.

EGP n'interprète aucune distance métrique spécifiée dans les messages de mise à jour de routage issus d'autres protocoles. EGP utilise la zone de distance pour indiquer si un chemin existe (la valeur 255 signifiant qu'un réseau est inaccessible). La valeur spécifiée ne peut pas servir à déterminer le chemin le plus court entre deux routes, sauf si ces dernières sont situées dans un seul système autonome. C'est pourquoi, EGP n'est pas utilisé comme algorithme de routage et, de ce fait, un seul chemin peut être emprunté entre la passerelle extérieure et un réseau.

Contrairement au protocole RIP (Routing Information Protocol), qui peut être appliqué à un système autonome de réseaux Internet qui reconfigurent dynamiquement les routes, les routes EGP sont prédéterminées dans le fichier **/etc/gated.conf**, avec IP comme protocole sous-jacent implicite.

Types de messages EGP

Neighbor Acquisition Request	Demande émise par les passerelles extérieures pour devenir limitrophes.
Neighbor Acquisition Reply	Réponse favorable des passerelles extérieures pour devenir limitrophes.
Neighbor Acquisition Refusal	Réponse défavorable des passerelles extérieures pour devenir limitrophes. Les raisons du refus sont indiquées dans le message, par exemple `out of table space` (espace de table insuffisant).
Neighbor Cease	Demande émise par les passerelles extérieures pour mettre fin à une relation limitrophe. Les raisons sont indiquées dans le message, par exemple, `going down` (mise hors service).
Neighbor Cease Acknowledgment	Acceptation par les passerelles extérieures de la demande d'interruption d'une relation limitrophe.
Neighbor Hello	Message émis par une passerelle limitrophe pour vérifier qu'une connexion est active. Une passerelle émet un message `Hello` et la passerelle interrogée confirme la connexion en émettant la réponse `I Heard You`.
I Heard You	Réponse d'une passerelle extérieure au message `Hello`. Le message `I Heard You` s'accompagne des informations d'accès à la passerelle qui émet la réponse et, si la passerelle est inaccessible, d'un message d'explication, par exemple `You are unreachable due to problems with my network interface` (Vous êtes inaccessible du fait d'incidents survenus sur mon interface de réseau).
NR Poll	Interrogation émise par les passerelles extérieures auprès des passerelles limitrophes pour déterminer leur capacité d'accès aux autres passerelles.
Network Reachability	Réponse des passerelles extérieures au message `NR Poll`. Pour chaque passerelle interrogée, le message `Network Reachability` indique les adresses auxquelles la passerelle limitrophe lui donne accès.
EGP Error	Réponse émise par les passerelles extérieures aux messages EGP qui présentent des totaux de contrôle ou des valeurs de zones erronés.

TCP/IP implémente le protocole EGP dans le démon **gated** mais ne lui fournit pas d'interface de programmation d'applications (API).

Protocole FTP

Le protocole FTP (File Transfer Protocol) permet le transfert des données entre hôtes hétérogènes et le transfert indirect de fichiers entre deux hôtes étrangers. Il donne accès à la liste des répertoires distants, permet de changer de répertoire distant courant, de créer ou de supprimer des répertoires distants et de transférer plusieurs fichiers en une seule demande. Un système de protection par mot de passe et numéro de compte utilisateur est assuré au niveau de l'hôte étranger. Conçu à l'origine pour des applications, FTP est également utilisé pour les sessions interactives orientées utilisateur.

FTP a recours au transfert fiable de flot (TCP/IP) pour l'envoi des fichiers, et à une connexion Telnet pour le transfert des commandes et des réponses. FTP reconnaît plusieurs formats de fichiers de base, notamment NETASCII, IMAGE et Local 8.

TCP/IP implémente FTP dans les commandes **ftpet** (utilisateur) et **ftpd** (serveur) mais ne fournit pas d'interface de programmation d'applications (API) avec ce protocole.

Si vous créez des répertoires et utilisateurs ftp anonymes, veillez à ce que le répertoire personnel des utilisateurs ftp et anonymes (par exemple, /**u**/**ftp**) appartienne à un utilisateur racine mais ne soit pas accessible en écriture (par exemple, `dr-xr-xr-x`). Vous pouvez utiliser le script /**usr**/**samples**/**tcpip**/**anon.ftp** pour créer ces comptes, fichiers et répertoires.

Protocole Telnet

Le protocole TELNET fournit une méthode de communication standard pour les terminaux et process orientés terminal. TELNET est utilisé couramment par les programmes d'émulation de terminal pour la connexion à un hôte distant. Il sert à la communication de terminal à terminal et inter–process, et est sollicité par d'autres protocoles (par exemple, FTP) pour l'établissement d'un canal de contrôle de protocole

TCP/IP implémente TELNET dans les commandes utilisateur **tn, telnet,** ou **tn3270**. Le démon **telnetd** ne fournit pas d'interface API pour TELNET.

TCP/IP accepte les options Telnet négociées entre le client et le serveur :

BINARY TRANSMISSION (pour sessions **tn3270**)	Transmet les caractères sous forme de données binaires.
SUPPRESS GO_AHEAD (AIX supprime les options GO–AHEAD.)	Lors de la transmission de données, à la demande de l'expéditeur des données, ne transmet pas au destinataire d'option GO_AHEAD. Dans ce cas, les deux parties peuvent demander la suppression de l'option dans les deux sens, cette suppression doit alors être effectuée indépendamment de part et d'autre.
TIMING MARK (Reconnue mais reçoit une réponse négative)	Vérifie que les données transmises ont été entièrement traitées.
EXTENDED OPTIONS LIST	Fournit la possibilité de 256 options supplémentaires à la liste des 256 options TELNET.
ECHO (Commande modifiable par l'utilisateur)	Transmet les caractères d'écho déjà renvoyés à l'expéditeur d'origine.
TERM TYPE	Permet au serveur de déterminer le type de terminal connecté à un programme utilisateur TELNET. SAK
SAK (Secure Attention Key)	Sécurise la communication entre vous et le système.
NAWS (Negotiate About Window Size)	Dans une relation client–serveur, permet aux deux parties de négocier la taille de la fenêtre (si les applications l'autorisent).

Remarque : Telnet doit autoriser la transmission de caractères 8 bits en mode non binaire pour l'implémentation de la page de code ISO 8859 Latin. Cette condition est nécessaire pour l'internationalisation des commandes TCP/IP.

Protocole TFTP

Le protocole TFTP (Trivial File Transfer Protocol) peut lire et enregistrer des fichiers issus de ou destinés à un hôte distant. TFTP est généralement plus rapide que FTP car, pour acheminer les fichiers, il fait appel au protocole UDP qui ne garantit pas la livraison des fichiers. Comme FTP, TFTP peut traiter les fichiers sous forme de données NETASCII ou binaires 8 bits. En revanche, il ne permet pas de lister ou de modifier les répertoires d'un hôte distant et ne prévoit pas de protection de type mot de passe. De plus, sous TFTP, l'écriture et la recherche des données sont limitées aux répertoires publics.

TCP/IP implémente TFTP dans les commandes utilisateur **tftp** et **utftp,** et dans la commande serveur **tftpd**. La commande **utftp** est une variante de **tftp** utilisable dans les chaînages (pipes), mais ne fournit pas d'interface API pour ce protocole.

Protocole FINGER

FINGER est un protocole Internet de niveau application qui joue le rôle d'interface entre la commande **finger** et le démon **fingerd**. Le démon **fingerd** renvoie les informations sur les utilisateurs connectés à un hôte distant spécifique. Pour limiter la commande à un utilisateur donné, spécifiez-le (commande **finger**). Le protocole FINGER doit être disponible sur l'hôte distant et sur l'hôte demandeur. Il utilise TCP comme protocole sous-jacent.

Remarque : TCP/IP ne fournit pas d'interface API pour le protocole FINGER.

Protocole HELLO

Le protocole de réseau local distribué HELLO s'applique aux passerelles intérieures et doit être utilisé dans des systèmes autonomes. (Pour plus de détails, reportez-vous à "Systèmes autonomes", page 3-34.) HELLO, chargé de tenir à jour les informations de connectivité, de routage et d'horloge, permet à chaque machine de trouver le chemin le plus rapide vers la destination et met à jour dynamiquement l'information de routage vers cette destination.

Ce protocole est fourni par le démon **gated**.

Protocole REXEC

Le protocole d'exécution à distance, fourni par la commande utilisateur **rexec** et le démon **rexecd**, permet de lancer des commandes sur un hôte distant compatible.

Protocole LOGIN

Le protocole de connexion à distance LOGIN, fourni par la commande utilisateur **rlogin** et le démon **rlogind**, permet aux utilisateurs de se connecter à un hôte distant et d'utiliser leur terminal comme s'ils étaient connectés directement à cet hôte.

Protocole SHELL

Le protocole de commande à distance SHELL, fourni par la commande utilisateur **rsh** et le démon **rshd**, permet d'ouvrir un shell sur un hôte étranger compatible pour y exécuter des commandes.

Protocole RIP

Le protocole de routage RIP (Routing Information protocol) et les démons **routed** et **gated** qui le mettent en œuvre, sont chargés de suivre les informations de routage (en fonction du nombre de bonds effectués) et de tenir à jour les entrées de la table de routage du noyau.

Protocole TIMED

Le démon **timed** est chargé de la synchronisation horaire des hôtes. Il est fondé sur le concept de client/serveur.

Nombres réservés

Dans un souci de compatibilité avec l'environnement de réseau général, des nombres connus sont attribués aux versions, réseaux, ports, protocoles et options de protocoles Internet, de même qu'aux machines, réseaux, systèmes d'exploitation, protocoles, services et terminaux. TCP/IP applique les numéros et noms définis par la norme RFC 1010, *Nombres réservés.*

Une zone de 4 bits est prévue dans l'en-tête IP pour identifier la version du protocole interréseau utilisé. Le numéro de version d'IP en décimal est 4. Pour plus d'informations sur les nombres et noms réservés de TCP/IP, reportez–vous aux fichiers /**etc**/**protocols** et /**etc**/**services** inclus dans TCP/IP. Pour les noms et nombres réservés en général, reportez-vous à la norme RFC 1010 et au fichier /**etc**/**services**.

Cartes réseau TCP/IP

Cette section traite des points suivants :

La carte réseau est le dispositif matériel raccordé physiquement aux câbles du réseau. Elle est chargée de recevoir et de transmettre les données au niveau physique. Elle est contrôlée par le pilote de carte.

Chaque machine doit être équipée d'autant de cartes réseau (ou connexions) que de réseaux auxquels elle est connectée. Par exemple, si un hôte est raccordé à deux réseaux en anneau à jeton, il doit être équipé de deux cartes réseau.

TCP/IP utilise les cartes réseau et connexions suivantes :

- Ethernet standard version 2
- IEEE 802.3
- Anneau à jeton
- Cartes asynchrones et ports série natifs
- Interface FDDI (Fiber Distributed Data Interface)
- Convertisseur optique série
- ATM Turboways 100 et Turboways 155

Les technologies de réseau Ethernet et 802.3 utilisent le même type de carte.

Chaque machine offre un nombre limité d'emplacements d'extension, que vous pouvez utiliser pour les cartes de communication. En outre, chaque machine ne prend en charge qu'un nombre limité de cartes de communication d'un type donné : 8 cartes Ethernet/802.3 maximum, 8 cartes réseau en anneau à jeton maximum et une seule carte asynchrone de 64 ports maximum. Dès lors, vous pouvez installer sur votre machine n'importe quelle combinaison de ces cartes en respectant les contraintes logicielles (nombre et type de carte) et matérielles (nombre total d'emplacements d'extension disponibles).

Une seule interface TCP/IP doit être configurée, quel que soit le nombre de convertisseurs optiques série pris en charge par le système. Le pilote d'unité **Optique série** exploite les deux convertisseurs de canal même si une seule interface logique TCP/IP est configurée.

Installation d'une carte réseau

Pour installer une carte réseau :

1. Arrêtez l'ordinateur. Pour l'arrêt système, reportez-vous à la commande **shutdown**.
2. Mettez la machine hors tension.
3. Déposez le capot de l'ordinateur.
4. Insérez la carte réseau dans un emplacement libre du bus Micro Channel.
5. Assurez-vous que la carte est bien en place et remontez le capot.
6. Mettez la machine sous tension et relancez le système.

Configuration et gestion des cartes

Pour configurer et gérer les cartes pour réseau en anneau à jeton ou Ethernet, suivez les procédures du tableau suivant.

Configuration et gestion des tâches relatives aux cartes		
Raccourci Web-based System Manager, (application wsm network) OU	**wsm network**	
Tâche	*Raccourci SMIT*	*Commande ou fichier*

Configuration d'une carte	**smit chgtok** (anneau à jeton)
	smit chgenet (Ethernet)
		1. Recherchez le nom de la carte :[1]
		`lsdev -C -c adapter -t tokenring -H`
		ou
		`lsdev -C -c adapter -t ethernet -H`
		2. Redéfinissez la vitesse de l'anneau (anneau à jeton) ou le type de connecteur (Ethernet), si nécessaire. Par exemple :
		`chdev -l tok0 -a ring_speed=16 -P`
		ou
		`chdev -l ent0 -a bnc_select=dix -P`

Détermination de l'adresse matérielle	**smit chgtok** (anneau à jeton) **smit chgenet** (Ethernet)	`lscfg -l tok0 -v` (anneau à jeton)[2] `lscfg -l ent0 -v` (Ethernet)[2]

Définition d'une adresse matérielle secondaire	**smit chgtok** (anneau à jeton)
	smit chgenet (Ethernet)
		1. Entrez : Par exemple, pour une carte d'anneau à jeton :[2,3]
		`chdev -l tok0 -a alt_addr=0X10005A4F1B7F`
		Pour une carte Ethernet :[2,3]
		`chdev -l ent0 -a alt_addr=0X10005A4F1B7F -p`
		2. Commencez à utiliser l'adresse secondaire, pour anneau à jeton :[4]
		`chdev -l tok0 -a use_alt_addr=yes`
		Pour Ethernet :[4]
		`chdev -l ent0 -a use_alt_addr=yes`

Remarques :

1. Le nom de la carte réseau peut changer si vous l'installez à un autre emplacement ou que vous la retirez du système. Dans ce cas, veillez à mettre à jour la base de données de configuration via la commande **diag –a.**
2. Indiquez le nom de votre carte à la place de `tok0` et `ent0`.
3. Remplacez par l'adresse matérielle `0X10005A4F1B7F`.
4. Une interruption de communication peut se produire après cette opération jusqu'à ce que les hôtes vident leur mémoire cache ARP et enregistrent cette nouvelle adresse matérielle.

Cartes ATM Turboways 100 et 155

Les cartes Turboways 100 et 155, qui assurent la connexion aux réseaux ATM (Asynchronous Transfer Mode), implémentent des interfaces physiques multimode fibre. ATM est exploité dans les environnements réseau demandant une largeur de bande supérieure à celle offerte par les réseaux locaux (LAN) actuels.

La carte Turboways 100 fournit une connexion 100 Mbps en duplex intégral aux serveurs basés sur bus Micro-Channel et aux clients exploitant des circuits virtuels permanents (PVC) et commutés (SVC). L'implémentation PVC et SVC est conforme à la spécification "ATM Forum UNI 3.0". De même, la carte Turboways 155 fournit une connexion 155 Mbps en duplex intégral aux réseaux ATM. Une carte peut prendre en charge jusqu'à 1 024 circuits virtuels.

Technologie ATM

ATM (Asynchronous Transfer Mode) est une technologie de commutation de cellules, orientée connexion. Sur un réseau ATM, les terminaux sont raccordés au réseau via des connexions en duplex intégral dédiées. Les réseaux ATM sont construits sur la base de commutateurs interconnectés par des connexions physiques dédiées. Pour que le transfert de données puisse avoir lieu, des connexions de bout en bout doivent être établies. Une interface physique unique peut assurer des connexions multiples. Les stations émettrices transmettent les données en segmentant les unités PDU (Protocol Data Unit) en cellules de 53-octets. Ces cellules, transférées comme telles, sont réassemblées en PDU par les stations réceptrices. Les connexions sont identifiées par un identificateur de chemin virtuel (VPI) et un identificateur de canal virtuel (VCI). Le champ VPI occupe 1 octet de l'en–tête de 5 octets de la cellule ATM, tandis que le champ VCI en occupe 2. Une paire VPI:VCI identifie l'origine d'une cellule ATM. Le commutateur ATM a pour fonction d'identifier l'origine de la cellule, de déterminer le saut suivant et de diriger la cellule vers un port. La paire VPI:VCI change sur une base saut par saut. Aussi les valeurs VPI:VCI ne sont-elles pas universelles. Un circuit virtuel est décrit par la concaténation de valeurs VPI:VCI à travers le réseau.

Connexions ATM

L'architecture ATM intègre deux types de circuit virtuel : les PVC (Permanent Virtual Circuits) et les SVC (Switched Virtual Circuits).

Circuits virtuels permanents (PVC)

La configuration des PVC est statique et manuelle. Les commutateurs composant le réseau ATM doivent être configurés au préalable de façon à reconnaître la combinaison VPI:VCI de chaque terminal et à acheminer les cellules ATM de ces points via le réseau ATM. Une fois établie la liaison entre tous les terminaux, les cellules ATM peuvent transiter par le réseau et les commutateurs ATM : les commutateurs traduisent les valeurs VPI:VCI de façon que la cellule soit acheminée à destination.

Circuits virtuels commutés (SVC)

Les SVC sont configurés dynamiquement, sur la base des besoins. Les terminaux ATM sont affectés d'adresses de 20-octets. Deux concepts entrent en jeu : le panneau de contrôle et le panneau de données. Le panneau de contrôle utilise une paire de canaux de signalisation VPI:VCI 0:5. Les SVC initient sur demande une configuration d'appel, permettant à une station ATM d'envoyer des éléments d'information spécifiant l'adresse ATM de destination (et, éventuellement, l'adresse ATM source). Il existe beaucoup d'autres éléments d'information pour spécifier les paramètres de la couche d'adaptation ATM (AAL), les paramètres Bandwidth et QoS, etc. Généralement, la station appelante, le réseau et la station appelée interviennent dans la négociation. Finalement, un appel est soit accepté, soit rejeté. S'il est accepté, le réseau affecte des valeurs VPI:VCI au panneau de données des deux stations (appelante et appelée). Sur le panneau de contrôle, le réseau ATM achemine (ou commute) les paquets de signaux sur la base des adresses ATM. Pendant le routage de ces paquets, les commutateurs définissent les tables de routage des cellules du panneau de données. Sur le panneau de données, les réseaux ATM commutent les cellules sur la base des VPI:VCI, presque comme dans le cas des PVC. A la fin du transfert, la connexion est close.

L'adresse ATM est construite par enregistrement sur le réseau ATM et acquisition des 13 octets les plus significatifs. Les 6 octets suivants correspondent à l'adresse matérielle "gravée" dans la carte. L'octet le moins significatif est le sélecteur ; son utilisation est laissée à la discrétion de l'utilisateur final : les réseaux ATM ne l'interprètent pas.

TCP/IP et ATM

Les normes *Internet Engineering Task Force RFC1577: Classical IP et ARP over ATM* spécifient le mécanisme d'implémentation d'IP sur ATM. ATM étant une technologie orientée connexion et IP une technologie orientée datagramme, le mappage IP-ATM n'est pas évident.

Un réseau ATM est le plus souvent réparti en sous–réseaux IP logiques (LIS). Chacun est composé d'un certain nombre de stations ATM. Les LIS, analogues aux segments LAN, sont interconnectés par des routeurs. Une carte (sur une station ATM) peut faire partie de plusieurs LIS ; ceci peut être très utile pour implémenter des routeurs.

RFC1577 spécifie RFC1483 qui spécifie LLC/SNAP Encapsulation comme valeur par défaut. Dans les réseaux PVC, pour chaque station IP, tous les PVC doivent être définis manuellement, par configuration des valeurs VPI:VCI. Si l'encapsulage LLC/SNAP n'est pas utilisé, l'adresse IP de destination associée à chaque VPI:VCI doit être définie.
Si l'encapsulage LLC/SNAP est utilisé, la station IP peut connaître l'adresse IP distante par le biais d'un mécanisme InARP. Pour les réseaux SVC, RFC1577 spécifie un serveur ARP pour chaque LIS. L'objet de ce serveur est de convertir les adresses IP en adresses ATM sans utiliser de messages de diffusion. Chaque station IP est configurée avec l'adresse ATM du serveur ARP. Les stations IP configurent les SVC avec le serveur ARP, lequel, à son tour, envoie les demandes InARP aux stations IP. Sur la base de la réponse InARP, un serveur ARP configure IP en mappes d'adresses ATM. Les stations IP envoient les paquets ARP au serveur ARP pour convertir les adresses, lequel renvoie les adresses ATM.
Les stations IP configurent ensuite un SVC vers la station de destination, et le transfert des données démarre. Les entrées ARP dans les stations IP et le serveur ARP sont fondées sur un mécanisme bien défini. Pour l'environnement PVC comme pour l'environnement SVC, chaque station IP dispose d'au moins un circuit virtuel par adresse de destination.

La norme Internet Engineering Task Force RFC2225 remplace la norme RFC1577 et s'attache principalement au support de la liste des adresses de requêtes ATM ARP. Cette liste contient une ou plusieurs adresses ATM de serveurs ATMARP situés au sein du LIS. Le client RFC2225 élimine le seul point de défaillance lié aux services ATMARP des clients 1577. Les clients 2225 peuvent sauvegarder les serveurs ARP en cas de défaillance du serveur ATM ARP.

ESCALA définit la première entrée de la liste d'adresses des requêtes ATM ARP comme le serveur ATM ARP principal, les autres étant définies comme des serveurs ATM ARP secondaires.

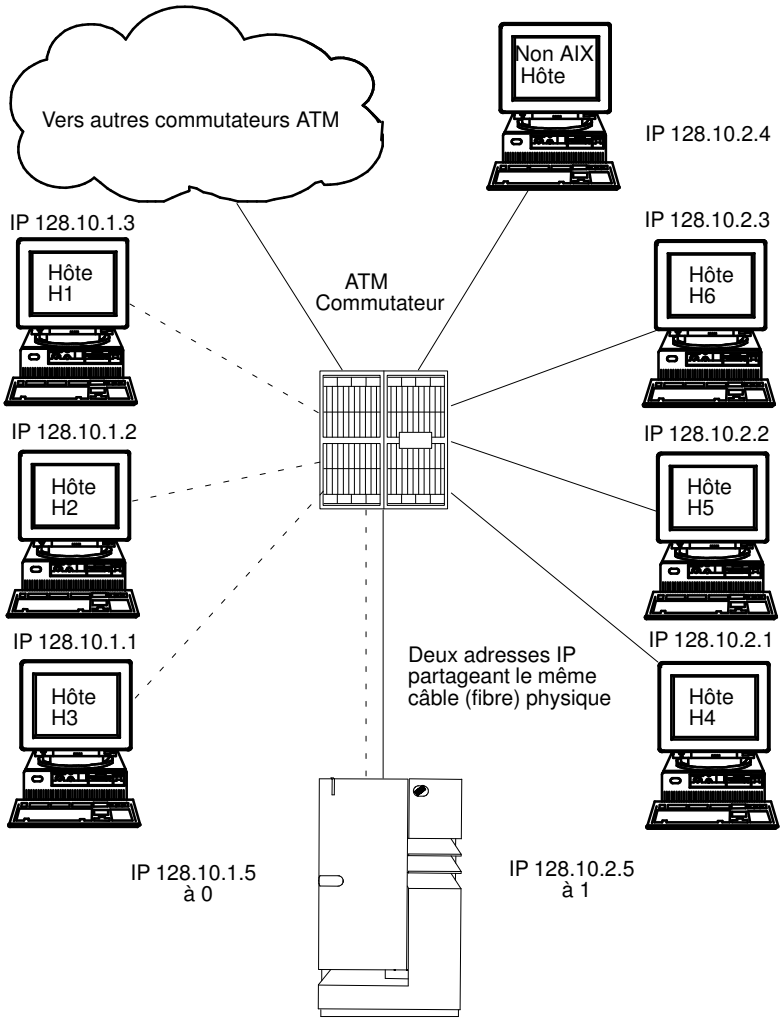
Le client essaie toujours d'utiliser le serveur ATM ARP principal. En cas d'échec de connexion à ce serveur, le client essaie de se connecter au premier serveur secondaire (la position dans la liste d'adresses des requêtes ATM ARP détermine l'ordre de celui–ci). En cas d'échec de la connexion au premier serveur ATM ARP secondaire, le client essaie de se connecter au serveur ATM ARP secondaire suivant, et ainsi de suite.

En cas d'échec de connexion au serveur ATM ARP principal, indépendamment du serveur ATM ARP secondaire auquel il est connecté ou tente de se connecter, le client fait, toutes les 15 minutes, une nouvelle tentative de connexion au serveur principal ATM ARP. En cas de réussite, la connexion au serveur ATM ARP secondaire est abandonnée.

La liste d'adresses des requêtes ATM ARP est saisie manuellement à l'aide du menu SMIT ou de la commande **ifconfig**. Cette liste ne peut pas être configurée avec la MIB (Management Information Base).

Réseau PVC

En vous basant sur la figure Réseau ATM type, configurez votre réseau.



Boîtier passerelle ATM avec une carte TURBOWAYS 155 ATM

Réseau ATM type

Dans la figure Réseau ATM type, un sous-réseau IP logique est représenté par des lignes de pointillés, reliant chaque hôte au commutateur. L'autre sous-réseau IP est représenté par des traits pleins.

Le tableau suivant indique comment configurer les hôtes AIX (H3 et H4) pour qu'ils puissent communiquer avec une passerelle et avec chaque hôte sur leur propre réseau IP logique.

Configuration type d'un hôte		
Pilote d'interface réseau	**VPI:VCI**	**Observations**
Hôte H3		
at0	0:40	Connexion à 128.100.1.5 (passerelle)
at0	0:42	Connexion à 128.10.1.2
at0	0:43	Connexion à 128.10.1.3
Hôte H4		
at0	0:50	Connexion à 128.10.2.5 (passerelle)
at0	0:52	Connexion à 128.10.2.2
at0	0:53	Connexion à 128.10.2.3
at0	0:54	Connexion à 128.10.2.4

Pour atteindre les hôtes d'un autre sous–réseau logique IP, il suffit de créer une connexion VPI:VCI vers la passerelle (les VPI:VCI indiqués sont de simples exemples).

Le boîtier de la passerelle ATM est équipé d'un ATM avec deux adresses IP partageant le même câble physique.

Réseau SVC

En vous basant sur la figure Réseau ATM type, imaginez que l'hôte AIX H3 souhaite appeler H4. H1 est le serveur ARP du sous-réseau 1 et H6, celui du sous–réseau 2. En supposant que le masque de sous-réseau est 255.255.255.0, les stations aux adresses 128.10.1.X sont membres d'un sous–réseau, tandis que les stations aux adresses 128.10.2.X sont membres d'un autre. Reportez-vous au tableau ci-après.

Liste de configurations type d'hôte				
Pilote d'interface réseau	**Adresse IP**	**Serveur ARP**	**Serveur ARP Adresse**	**Adresse passerelle**
Hôte H1				
at0	128.10.1.3	Oui		128.10.1.5
Hôte H3				
at0	128.10.1.1	Non	Adresse ATM de H1	128.10.1.5
Passerelle				
at0	128.10.1.5	Non	Adresse ATM de H1	
at1	128.10.2.5	Non	Adresse ATM de H6	
Hôte H4				
at0	128.10.2.1	Non	Adresse ATM de H6	128.10.2.5
Hôte H6				
at0	128.10.2.3	Oui		128.10.2.5

Remarque : Chaque sous–réseau requiert un et un seul serveur ARP.

H3 identifiant que l'adresse 128.10.2.1 ne se trouve pas sur son sous-réseau, consulte H1 pour convertir l'adresse IP de la passerelle par défaut en adresse ATM. H3 lance ensuite un appel à la passerelle. La passerelle identifie que les données sont associées au second sous-réseau et consulte H6 pour convertir effectivement l'adresse IP de H4 en adresse ATM. Des connexions sont ensuite établies entre H3 et la passerelle, et entre la passerelle et H4.

Configuration d'une carte ATM

Pour configurer une carte ATM 100, ATM 155 ou PCI ATM, utilisez le raccourci Web-based System Manager **wsm network** ou SMIT **smit chg_atm**. Sélectionnez un nom de carte, puis avec l'aide en ligne et les listes à choix multiples, décidez des modifications à apporter à votre configuration.

Statistiques sur la carte ATM

La commande **atmstat** permet d'obtenir des statistiques sur la carte ATM. Assortie de l'indicateur **–r**, elle remet les statistiques à zéro. Son format est **atmstat** *NomUnité*. Elle renvoie les ensembles de statistiques suivants :

Statistiques de transmission

`Packets:` Nombre de paquets (ou de PDU) transmis.

`Bytes:` Décompte des octets reçus (octets utilisateur). La charge ATM (en-tête de cellule ATM, "en-queue" AAL5 PDU, etc.), par exemple, est exclue.

`Interrupts:`
Non utilisé.

`Transmit Errors:`
Nombre d'erreurs de transmission pour l'unité.

`Packets Dropped:`
Nombre de paquets de transmission abandonnés, suite, par exemple, à un incident sur le tampon.

`Max Packets on S/W Transmit Queue:`
Non applicable à ATM.

`S/W Transmit Queue Overflow:`
Non applicable à ATM.

`Current S/W + H/W Transmit Queue Length:`
Longueur de la file d'attente de transmission courante.

`Cells Transmitted:`
Nombre de cellules transmises par cette unité.

`Out of Xmit Buffers:`
Nombre de paquets de transmission abandonnés, suite à un incident sur les tampons xmit.

`Current HW Transmit Queue Length:`
Nombre courant de paquets de transmission sur la file d'attente matérielle.

`Current SW Transmit Queue Length:`
Non applicable à ATM.

Statistiques de réception

`Packets:` Nombre de paquets (ou de PDU) reçus.

`Bytes:` Décompte des octets reçus (octets utilisateur). La charge ATM (en-tête de cellule ATM, ”en-queue” AAL5 PDU, etc.), par exemple, est exclue.

`Interrupts:`
Nombre d’interruptions effectuées par le système pour les indications carte-vers-système. Parmi les événements susceptibles de provoquer ces interruptions, citons des paquets reçus, des indications de transmission effectuée, etc.

`Receive Errors:`
Nombre d’erreurs de réception pour cette unité.

`Packets Dropped:`
Nombre de paquets de réception abandonnés, suite par exemple à un incident sur les tampons.

`Bad Packets:`
Non applicable à ATM.

`Cells Received:`
Nombre de cellules reçues par cette unité.

`Out of Rcv Buffers:`
Nombre de paquets abandonnés, suite à un incident sur les tampons de réception.

`CRC Errors:`
Nombre de paquets reçus ayant rencontré des erreurs CRC.

`Packets Too Long:`
Nombre de paquets reçus, qui excédaient la taille maximale du PDU.

`Incomplete Packets:`
Nombre de paquets incomplets reçus.

`Cells Dropped:`
Nombre de cellules abandonnées, pour des raisons diverses : HEC erroné, incident sur le tampon, etc.

Statistiques générales

`No mbuf Errors:`
Nombre de requêtes mbuf refusées.

`Adapter Loss of Signals:`
Nombre de pertes de signal rencontrées par la carte.

`Adapter Reset Count:`
Nombre de réinitialisations effectuées sur la carte.

`Driver Flags: Up Running Simplex`
Indicateurs NDD.

`Virtual Connections in use:`
Nombre de VC actuellement alloués ou en cours d’utilisation.

`Max Virtual Connections in use:`
Nombre maximal de VC alloués depuis la dernière remise à zéro des statistiques.

`Virtual Connections Overflow:`
Nombre de demandes d’allocation de VC refusées.

`SVC UNI Version:`
Version UNI courante du protocole de signalisation utilisé.

Statistiques ATM complémentaires

Pour des statistiques détaillées, lancez la commande **atmstat** assortie de l'indicateur **–d.**

Statistiques propres à la carte ATM Turboways :

`Packets Dropped – No small DMA buffer:`
Nombre de paquets de réception abandonnés suite à l'absence de petits tampons système pour DMA sur la carte.

`Packets Dropped – No medium DMA buffer:`
Nombre de paquets de réception abandonnés suite à l'absence de tampons système moyens pour DMA sur la carte.

`Packets Dropped – No large DMA buffer:`
Nombre de paquets de réception abandonnés suite à l'absence de grands tampons système pour DMA sur la carte.

`Receive Aborted – No Adapter Receive buffer:`
Nombre de paquets de réception abandonnés suite à l'absence de tampons de réception sur la carte.

`Transmit Aborted – No small DMA buffer:`
Nombre de paquets de transmission abandonnés suite à l'absence de petits tampons système pour DMA.

`Transmit Aborted – No medium DMA buffer:`
Nombre de paquets de transmission abandonnés suite à l'absence de tampons système moyens pour DMA.

`Transmit Aborted – No large DMA buffer:`
Nombre de paquets de transmission abandonnés suite à l'absence de grands tampons système pour DMA.

`Transmit Aborted – No MTB DMA buffer:`
Nombre de paquets de transmission abandonnés suite à l'absence de grands tampons système pour DMA.

`Transmit Aborted – No Adapter Transmit buffer:`
Nombre de paquets de transmission abandonnés suite à l'absence de tampons de transmission sur la carte.

`Max Hardware Transmit Queue Length:`
Nombre maximal de paquets de transmission en attente dans la file matérielle.

`Small Mbufs in Use:`
Nombre de petits tampons en cours d'utilisation. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`Medium Mbufs in Use:`
Nombre de tampons moyens en cours d'utilisation. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`Large Mbufs in Use:`
Nombre de grands tampons en cours d'utilisation. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`Huge Mbufs in Use:`
: Nombre de très grands tampons en cours d'utilisation. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`MTB Mbufs in Use:`
: Nombre de tampons MTB en cours d'utilisation. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`Max Small Mbufs in Use:`
: Nombre maximal de petits tampons qui ont été utilisés. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`Max Medium Mbufs in Use:`
: Nombre maximal de tampons moyens qui ont été utilisés. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`Max Large Mbufs in Use:`
: Nombre maximal de grands tampons qui ont été utilisés. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`Max Huge Mbufs in Use:`
: Nombre maximal de très grands tampons qui ont été utilisés. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`MTB Mbufs in Use:`
: Nombre maximal de tampons MTB qui ont été utilisés. Le pilote d'unité de carte alloue ces tampons en fonction des données de configuration fournies par les administrateurs système. Cette information peut servir à affiner les données de configuration.

`Small Mbufs overflow:`
: Nombre de fois qu'un petit tampon n'a pu être alloué. Cette information peut servir à affiner les données de configuration.

`Medium Mbufs overflow:`
: Nombre de fois qu'un moyen tampon n'a pu être alloué. Cette information peut servir à affiner les données de configuration.

`Large Mbufs overflow:`
: Nombre de fois qu'un grand tampon n'a pu être alloué. Cette information peut servir à affiner les données de configuration.

`Huge Mbufs overflow:`
: Nombre de fois qu'un très grand tampon n'a pu être alloué. Cette information peut servir à affiner les données de configuration.

`MTB Mbufs overflow:`
: Nombre de fois qu'un tampon MTB n'a pu être alloué. Cette information peut servir à affiner les données de configuration.

Statistiques propres à la carte ATM PCI :

```
Total Receive Buffers: 48   Using: 32
```

Message indiquant le nombre de tampons de réception alloués et le nombre de ceux en cours d'utilisation.

Interfaces de réseau TCP/IP

La couche interface de réseau TCP/IP convertit les datagrammes IP de la couche réseau en paquets interprétables et transmissibles par les technologies de réseau. Une interface de réseau est un logiciel spécifique d'un réseau qui permet la communication entre le pilote d'unité du réseau et la couche IP. Ainsi, la couche IP dispose d'une interface fiable pour communiquer avec toutes les cartes réseau en place.

La couche IP sélectionne l'interface de réseau correspondant à l'adresse de destination du paquet à transmettre. Chaque interface est dotée d'une adresse. La couche interface de réseau est chargée d'ajouter ou de supprimer l'en-tête appliqué par la couche liaison pour assurer la livraison du message. Le pilote de **carte réseau** contrôle la carte réseau.

Une interface de réseau est généralement associée à une carte réseau, mais ce n'est pas obligatoire (l'interface de bouclage (loopback), par exemple, ne l'est pas). Chaque machine doit être équipée d'autant de cartes que de réseaux (et non de types de réseau) auxquels elle est connectée. Cependant, la machine requiert seulement une copie du logiciel d'interface de réseau et une copie du pilote d'unité de réseau. Par exemple, si un hôte est raccordé à deux réseaux en anneau à jeton, il doit être équipé de deux cartes réseau. Cependant, il requiert seulement une copie du logiciel d'interface de réseau et une copie du pilote de réseaux en anneau à jeton.

TCP/IP accepte plusieurs types d'interface de réseau :

- Ethernet standard version 2 (en)
- IEEE 802.3 (et)
- Anneau à jeton (tr)
- SLIP (sl)
- Bouclage (lo)
- FDDI
- Optique série (so)
- ATM (at).
- Protocole point à point (PPP)

Les interfaces Ethernet, 802.3 et anneau à jeton sont destinées aux réseaux locaux (LAN) et l'interface SLIP (Serial Line Internet Protocol), aux connexions série. L'interface de bouclage (loopback) est utilisée par les hôtes pour que les messages qu'ils envoient leur soient réexpédiés. L'interface Optique série s'applique aux réseaux optiques point à point exploitant le gestionnaire d'unité de liaison optique série. L'interface ATM est utilisée pour les connexions ATM 100 Mbits/sec et 155 Mbits/sec.

Configuration automatique des interfaces de réseau

A l'installation d'une nouvelle carte réseau (physique), le système d'exploitation ajoute automatiquement l'interface correspondante. Par exemple, si vous installez une carte réseau en anneau à jeton, le système la nomme `tok0` et ajoute l'interface de réseau en anneau à jeton `tr0`. De même, si vous installez une carte Ethernet, le système la nomme `ent0` et ajoute l'interface Ethernet version 2 (`en0`) et l'interface IEEE 802.3 (`et0`).

Dans la plupart des cas, il existe une correspondance unique entre un nom de carte et un nom d'interface de réseau. Par exemple, la carte `tok0` correspond à l'interface `tr0`, la carte tok1, à l'interface `tr1`, etc. De même, la carte Ethernet `ent0` correspond aux interfaces `en0` (Ethernet version 2) et `et0` (IEEE 802.3), la carte `ent1` , aux interfaces `en1` (Ethernet version 2) et `et1` (IEEE 802.3).

Conformément à RFC1577, une station ATM peut faire partie de plusieurs sous-réseaux IP logiques. Dans ce cas, plusieurs interfaces sont associées à une unité, ce qui suppose d'ajouter une interface spécifique et de lui affecter un nom d'unité.

Remarque : En circonstances normales d'exploitation, vous n'aurez jamais à supprimer ou ajouter manuellement une interface de réseau. Mais vous pouvez être amené à le faire au cours d'une procédure de résolution d'incident. Dans ce cas, utilisez le raccourci Web-based System Manager **wsm network** ou SMIT **smit inet** pour supprimer et réajouter l'interface appropriée.

A chaque lancement du système, l'interface de réseau est automatiquement configurée en fonction des informations de la base de données ODM, avec des valeurs par défaut. La communication n'est possible que si une adresse Internet lui a été attribuée. C'est le seul attribut que vous ayez à définir. Les autres attributs peuvent conserver leur valeur par défaut. Le détail de ces valeurs est donné dans les paragraphes qui suivent.

Configuration Ethernet par défaut

Voici les attributs de carte réseau Ethernet qui peuvent être modifiés dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
netaddr		
state	down	up, down, detach
arp	yes	yes, no
netmask		
broadcast		

Voici les attributs de pilote d'unité réseau Ethernet et ses valeurs par défaut qui peuvent être modifiés dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
mtu	1500	60 à 1500

Configuration 802.3 par défaut

Voici les attributs de carte réseau 802.3 qui peuvent être modifiés dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
netaddr		
state	down	up, down, detach
arp	yes	yes, no
netmask		
broadcast		

Voici les attributs de pilote d'unité réseau 802.3 et ses valeurs par défaut qui peuvent être modifiés dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
mtu	1492	60 à 1492

Valeurs de configuration par défaut de l'anneau à jeton

Voici les attributs de carte réseau en anneau à jeton qui peuvent être modifiés dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
netaddr		
netmask		
state	down	up, down, detach
arp	yes	yes, no
hwloop	no	yes, no
netmask		
broadcast		
allcast	no	yes, no

Voici les attributs de pilote d'unité réseau en anneau à jeton et ses valeurs par défaut qui peuvent être modifiés dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
mtu (4Mbps)	1500	60 à 4056
mtu (16Mbps)	1500	60 à 17960

Remarque : Lorsque la communication transite par un pont, la valeur MTU par défaut (de 1500 octets) doit être ramenée à 8 octets en-dessous de la valeur maximum I-frame déclarée par le pont dans le champ de contrôle de routage. Par exemple, si la valeur de "maximum I-frame" est 3.810,00 cm dans le champ de contrôle de routage, celle de MTU doit être fixée à 1492 (pour les interfaces anneau à jeton seulement). Pour en savoir plus, reportez-vous à "Incidents sur un pont reliant deux réseaux en anneau à jeton", page 3-166.

Avec la carte en anneau à jeton IBM 16/4 PowerPC (ISA) ou la carte en anneau à jeton IBM PCMCIA 16/4, le mtu est limité à 2000.

Configuration SLIP par défaut

Voici les attributs de carte réseau SLIP qui peuvent être modifiés dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
netaddr		
dest		
state	up	up, down, detach
netmask		

Voici les attributs de pilote d'unité réseau SLIP et ses valeurs par défaut qui peuvent être modifiés dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
mtu	1006	60 à 4096

Configuration optique série par défaut

Voici les attributs du convertisseur de canal réseau optique série et leurs valeurs par défaut telles qu'elles s'affichent dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
netaddr		
state	down	up, down, detach
netmask		

Voici l'attribut du gestionnaire d'unité réseau optique série et ses valeurs par défaut qui s'affichent dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
mtu	61428	1 à 61428

Configuration ATM par défaut

Voici les attributs de carte réseau ATM et leurs valeurs par défaut qui s'affichent dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
netaddr		
netmask		
state	up	up, down, detach
Connection Type	svc_s	svc_c, svc_s, pvc
ATM Server Address		
Alternate Device		

idle timer	60	1 à 60
Best Effort Bit Rate (UBR) en kbits/sec	0	1 à 155.000

Voici l'attribut de pilote d'unité réseau ATM et ses valeurs par défaut qui s'affichent dans le menu SMIT Sélection d'une interface de réseau ou avec le raccourci Web-based System Manager **wsm network**.

Attribut	Valeur par défaut	Valeurs possibles
mtu	9180	1 à 64K

Remarque : La plus grande prudence est recommandée aux administrateurs réseau s'ils modifient la taille de MTU définie par défaut. La valeur de ce paramètre doit être compatible avec les autres stations du réseau.

Si des PVC sont utilisés sur une interface, les VPI:VCI doivent être définis via la dernière option, PVCs for IP over ATM Network, dans le menu Sélection d'une interface de réseau.

Réseaux avec plusieurs interfaces

Pour accroître la disponibilité et les performances du réseau, les administrateurs système ont parfois recours à une seconde carte réseau installée sur une machine. Ils peuvent par exemple décider de connecter deux cartes réseau en anneau à jeton à un même réseau physique. Cependant, cette configuration à interfaces multiples est déconseillée car :

1. Elle n'est pas conforme à l'architecture TCP/IP.

   Dans l'architecture TCP/IP, une machine hôte équipée de deux cartes réseau se définit comme un routeur IP. Des cartes réseau différentes doivent être connectées à des réseaux physiques différents. Dans le cas de réseau en anneau à jeton, TCP/IP considère plusieurs anneaux reliés par un pont comme un anneau logique unique (comme s'il s'agissait d'un seul anneau physique).

2. Deux interfaces peuvent alors générer des conflits de diffusion.

   Lorsqu'un hôte IP détecte des données destinées à un réseau doté d'une adresse IP différente du sien, il génère un paquet ICMP d'avertissement. Sur le réseau, chaque hôte perçoit cette erreur d'aiguillage et émet des paquets ICMP. Ce type d'erreur étant fréquent, le flux des paquets ICMP peut prendre des proportions telles que les performances du réseau s'en trouvent affectées.

Il est possible d'éviter ce type de conflit lorsque plusieurs interfaces sont utilisées, mais ce n'est toujours pas conforme à l'architecture TCP/IP. Il s'agit d'attribuer aux diverses interfaces du même réseau des adresses IP différentes. Ainsi, vous pouvez avoir deux cartes réseau en anneau à jeton sur le même réseau, nommées `tr0` et `tr1`. Vous devez attribuer à `tr0` et `tr1` des noms et des adresses IP distincts. (L'architecture TCP/IP exige en effet que chaque interface soit dotée d'une adresse et d'un nom IP uniques, faute de quoi des résultats imprévisibles peuvent survenir.) Vous pouvez, par exemple, attribuer à l'interface `tr0` l'adresse IP `10.10.10.1` et le nom `laurel.foo.bar.com`, et à l'interface `tr1`, l'adresse IP `10.10.10.2` et le nom `hardy.foo.bar.com`.

Gestion d’interfaces de réseau

Pour gérer des interfaces de réseau, utilisez les procédures du tableau suivant.

Gestion des tâches d’interfaces de réseau		
Raccourci Web-based System Manager, **wsm network** (application wsm network) – OU –		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Liste de toutes les unités de réseau	**smit lsinet**	**lsdev –C –c if**
Configuration d’une unité de réseau	`smit chinet`	Reportez-vous à la commande **ifconfig** et au fichier **rc.net**
Modification des informations d’interface réseau avec /**usr** monté à distance	**smit chdev**[1,2]	**chgif**[1,2]
Statistiques sur une interface de réseau		**netstat –v**

Remarques :

1. Les modifications apportées depuis un /**usr** monté à distance n’affectent que l’ODM tant que le réseau n’est pas réinitialisé ou tant que la commande **ifconfig** n’a pas été utilisée pour valider les modifications.
2. Avec /**usr** monté à distance, l’administrateur système doit veiller à ne pas changer l’interface car elle correspond à l’emplacement des bibliothèques, des commandes et du noyau.

Adressage TCP/IP

TCP/IP contient un schéma d'adressage Internet qui permet aux utilisateurs et aux applications d'obtenir l'identité d'un réseau ou d'un hôte pour établir une communication. Une adresse Internet fonctionne sur le même principe qu'une adresse postale : elle permet aux données d'être acheminées à destination. TCP/IP intègre des normes d'adressage de réseaux, sous-réseaux, hôtes, sockets, et des normes d'utilisation des adresses de diffusion et de bouclage.

Une adresse Internet est constituée d'une adresse réseau et d'une adresse d'hôte (locale). Ce format permet de spécifier dans la même adresse le réseau et l'hôte cible. Une adresse officielle unique est attribuée à chaque réseau qui se connecte à d'autres réseaux Internet. Pour les réseaux non connectés à d'autres réseaux Internet, l'adresse peut être déterminée selon la convenance locale.

Le schéma d'adressage Internet propose des adresses IP (Internet Protocol) et deux cas particuliers d'adresse IP : adresses de diffusion et adresses de bouclage.

Adresses Internet

Le protocole IP (Internet Protocol) utilise une zone d'adresse de 32 bits formée de deux parties. Les 32 bits sont répartis en groupes de quatre *octets* comme suit :

01111101 00001101 01001001 00001111

Ces nombres binaires correspondent à :

125 13 73 15

Les deux parties de l'adresse Internet sont respectivement l'adresse réseau et l'adresse hôte. Ainsi, un hôte distant peut expédier des informations en précisant le réseau distant et l'hôte destinataire sur ce réseau. Par convention, le numéro d'hôte 0 (zéro) désigne le réseau lui-même.

TCP/IP prend en charge trois classes d'adresses Internet : A, B et C, qui se distinguent par l'attribution des 32 bits. L'appartenance à une classe est déterminée par la taille du réseau.

Adresses de classe A

Une adresse de classe A se compose d'une adresse de réseau de 8 bits et d'une adresse hôte local de 24 bits. Le premier bit de l'adresse de réseau sert à désigner la classe du réseau et les 7 autres, l'adresse effective. Le nombre le plus élevé que peuvent représenter ces 7 bits en binaire est 128 ; la classe A offre donc 128 adresses possibles. Deux sont réservées à des cas particuliers : l'adressage de bouclage local pour l'une (code 127) et l'adressage de diffusion pour l'autre (adresse qui couvre la totalité des réseaux).

Il en résulte 126 adresses de réseau de classe A possibles et 16 777 216 adresses d'hôte local. Dans une adresse de classe A, le bit de poids fort est positionné à 0 (voir figure).

Adresse de réseau (8 bits)	**Adresse d'hôte local** (24 bits)		
01111101	00001101	01001001	00001111

Remarque : Le bit de poids fort (le premier) est toujours positionné à 0 dans une adresse de classe A.

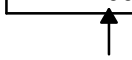
Adresse de classe A

Autrement dit, le premier octet d'une adresse de classe A est compris entre 1 et 126.

Adresse de classe B

Une adresse de classe B se compose d'une adresse de réseau de 16 bits et d'une adresse hôte local de 16 bits. Les 2 premiers bits de l'adresse de réseau désignent la classe de réseau et les 14 autres, l'adresse effective. Par conséquent, il y a 16 384 adresses de réseau possibles et 65 536 adresses hôte local. Dans une adresse de classe B, les bits de poids fort sont positionnés à 1 et 0 (voir figure).

Adresse de réseau (16 bits)		**Adresse d'hôte local** (16 bits)	
10011101	00001101	01001001	00001111



Remarque : Les 2 bits de poids fort (les deux premiers) sont toujours positionnés à 1 et 0 dans une adresse de classe B.

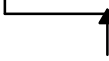
Adresse de classe B

Autrement dit, le premier octet d'une adresse de classe B est compris entre 128 et 191.

Adresse de classe C

Une adresse de classe C se compose d'une adresse de réseau de 24 bits et d'une adresse hôte local de 8 bits. Les 2 premiers bits de l'adresse de réseau désignent la classe de réseau et les 22 autres, l'adresse effective. Par conséquent, il y a 2 097 152 adresses de réseau possibles et 256 adresses hôte local possibles. Dans une adresse de classe C, les bits de poids fort sont positionnés à 1 et 1 (voir figure).

Adresse de réseau (24 bits)			**Adresse d'hôte local** (8 bits)
11011101	00001101	01001001	00001111



Remarque : Remarque : Les 2 bits de poids fort (les deux premiers) sont toujours positionnés à 1 dans une adresse de classe C.

Adresse de classe C

Autrement dit, le premier octet d'une adresse de classe C est compris entre 192 et 223.

Pour décider de la classe d'adresse, vous devez tenir compte du nombre d'hôtes locaux et de sous-réseaux prévus. Si l'organisation est réduite et que le réseau comporte moins de 256 hôtes, une adresse de classe C est probablement suffisante. Sinon, il faut envisager une adresse de classe A ou B.

Remarque : Les adresses de classe D (1-1-1-0 pour les bits de poids fort), prises en charge par UDP/IP sous AIX, sont utilisées comme adresses de diffusion.

Les machines lisent les adresses en code binaire. Par convention, les adresses hôtes Internet sont exprimées en *notation décimale à points* sur 32 bits répartis en quatre zones de 8 bits. Par exemple, la valeur binaire :

0001010 00000010 00000000 00110100

peut être exprimée comme suit :

010.002.000.052 ou 10.2.0.52

La valeur de chacune de ces zones, séparées par un point, est un nombre décimal.

Remarque : La commande **hostent** reconnaît les adresses suivantes : .08, .008, .09 et .009. Les adresses introduites par des zéros sont interprétées en base octale, laquelle exclut les chiffres 8 et 9.

TCP/IP requiert une adresse Internet unique pour chaque interface (carte) du réseau. Ces adresses, définies par la base de données de configuration, doivent concorder avec celles du fichier **/etc/hosts** ou, si un serveur de noms est utilisé, de la base de données **named**.

Adresses Internet avec zéros

Lorsque la zone d'adresse hôte d'une adresse Internet de classe C a la valeur zéro (par exemple, 192.9.200.0), TCP/IP envoie une adresse générique sur le réseau : toutes les machines dotées de l'adresse de classe 192.9.200.*X* (où *X* représente une valeur comprise entre 0 et 254) doivent répondre à la requête. Il en résulte que le réseau est inondé de requêtes adressées à des machines inexistantes.

Le même problème se pose pour une adresse de classe B du type 129.5.0.0 : toutes les machines dotées de l'adresse de classe 129.5.*X.X*. (où *X* représente une valeur comprise entre 0 et 254) doivent répondre à la requête. Mais, dans ce cas, le nombre de requêtes est bien plus important encore que sur un réseau de classe C car les adresses de classe B couvrent des réseaux plus vastes.

Adresses de sous-réseau

Grâce au mécanisme d'adressage de sous-réseau, un système autonome regroupant plusieurs réseaux peut disposer d'une même adresse Internet. Il est également possible de diviser un réseau en plusieurs réseaux logiques (sous-réseaux). Par exemple, une organisation sera dotée d'une adresse Internet unique connue par les utilisateurs extérieurs à l'organisation mais comportera en interne plusieurs sous-réseaux de service. Quel que soit le cas de figure, l'adressage de sous-réseau réduit le nombre d'adresses Internet requises et optimise le routage local.

La zone d'adresse du protocole IP est formée de deux parties : une adresse de réseau et une adresse locale. Cette dernière est constituée d'un numéro de sous–réseau et d'un numéro d'hôte, ce qui permet de définir des adresses de sous–réseau. L'identification du sous–réseau est suffisamment précise pour assurer le routage des messages de façon fiable.

Dans l'adresse Internet de classe A (voir figure), qui se compose d'une adresse de réseau de 8 bits et d'une adresse hôte local de 24 bits, l'adresse locale identifie la machine hôte spécifique sur le réseau.

Adresse de réseau (8 bits)	**Adresse d'hôte local** (24 bits)		
01111101	00001101	01001001	00001111

Adresse de classe A

Pour créer une adresse de sous-réseau pour réseau Internet de classe A, l'adresse locale est composée de deux éléments : le numéro d'identification du réseau physique (ou sous-réseau) et le numéro de l'hôte sur le sous-réseau. Les messages sont renvoyés à l'adresse de réseau indiquée et le système local se charge d'acheminer les messages vers ses sous-réseaux et hôtes. Le partitionnement de l'adresse locale en adresses sous-réseau et hôte s'effectue en fonction du nombre de sous-réseaux et d'hôtes correspondants.

Le tableau ci-dessous décrit l'adresse locale divisée en une adresse de sous-réseau 12 bits et une adresse hôte 12 bits.

Adresse de réseau (8 bits)	**Adresse d'hôte local** (24 bits)			
Adresse de réseau	**Adresse de sous-réseau**		**Adresse d'hôte**	
01111101	00001101	0100	1001	00001111

Remarque : Le bit de poids fort (le premier) est toujours positionné à 0 dans une adresse de classe A.

Adresse de classe A intégrant une adresse de sous-réseau

Vous bénéficiez d'une grande souplesse d'adressage des sous-réseaux et hôtes. Les bits de l'adresse locale peuvent être répartis en fonction de la croissance potentielle de l'organisation et de la structure de réseau. Les règles à respecter sont les suivantes :

- `adresse_réseau` correspond à l'adresse Internet.
- `adresse_sous-réseau` est une zone de longueur constante pour un réseau donné.
- `adresse_hôte` est une zone de 1 bit minimum.

Si la longueur de la zone `adresse de sous-réseau` est 0, le réseau n'est pas organisé en sous-réseaux, et l'adressage du réseau se fait par le biais de l'adresse de réseau Internet.

Il n'est donc pas nécessaire que ces bits soient contigus dans l'adresse, bien que ce soit généralement préférable. De même, il est conseillé de positionner les bits de sous-réseau comme bits de poids fort de l'adresse locale.

Masques de sous-réseau

Lorsqu'un hôte envoie un message, le système doit déterminer si la destination du message se trouve sur le même réseau que la source ou sur un réseau directement accessible par une des interfaces locales. Pour ce faire, il compare l'adresse de destination à l'adresse hôte sur la base d'un *masque de sous-réseau*. Lorsque la destination n'est pas locale, le message transite par une passerelle. La passerelle détermine si la destination est accessible localement en procédant à la même comparaison.

Le masque de sous-réseau fournit au système le schéma de partitionnement du sous-réseau. Ce masque de bits comporte la partie adresse de réseau et la partie adresse de sous-réseau de l'adresse Internet. Par exemple, le masque de sous-réseau de l'adresse de classe A répartie comme indiqué précédemment se présente comme suit :

Adresse de réseau (8 bits)	**Adresse d'hôte local** (24 bits)			
Adresse de réseau	**Adresse de sous-réseau**		**Adresse d'hôte**	
01111101	00001101	0100	1001	00001111

Adresse de classe A intégrant une adresse de sous-réseau

Adresse de réseau (8 bits)	**Adresse d'hôte local** (24 bits)			
Adresse de réseau	Adresse de sous-réseau		Adresse d'hôte	
Masque de sous-réseau			**Adresse d'hôte**	
01111101	00001101	0100	1001	00001111

Adresse de classe A intégrant un masque de sous-réseau

Le masque de sous-réseau est un ensemble de 4 octets, comme l'adresse interréseau. Il comporte des bits de poids fort (les 1) qui correspondent aux emplacements de bits de l'adresse de réseau et de sous-réseau, et des bits de poids faible (les 0) correspondant aux emplacements des bits de l'adresse hôte. Le masque de sous-réseau de l'adresse donnée ci-dessus se présente comme suit :

Adresse de réseau (8 bits)	**Adresse d'hôte local** (24 bits)	
Adresse de réseau	**Adresse de sous-réseau**	**Adresse d'hôte**
11111111	11111111 1111	0000 00000000

Exemple de masque de sous-réseau

Comparaison d'adresses

L'adresse de destination est comparée à l'adresse de réseau local en appliquant l'opérateur logique AND et l'opérateur d'exclusion OR sur le masque de sous-réseau de l'hôte source :

La procédure de comparaison se déroule comme suit :

1. Application de l'opérateur logique AND entre l'adresse de destination et le masque de l'adresse de sous-réseau local.
2. Application de l'opérateur d'exclusion OR entre le résultat de l'opération précédente et l'adresse de réseau local associée à l'interface locale.

   Si le résultat ne fournit que des zéros, la destination est supposée directement accessible via une des interfaces locales.
3. Si un système autonome est équipé de plusieurs interfaces (et donc de plusieurs adresses Internet), la comparaison est effectuée pour chaque interface locale.

Supposons, par exemple, que deux interfaces locales soient définies pour le réseau hôte T125. Leur adresse Internet et la représentation binaire de ces adresses doivent se présenter comme suit :

Adresses d'interface de réseau local

```
CLASSE A   73.1.5.2    =  1001001 00000001 00000101 00000010

CLASSE B   145.21.6.3  =  10010001 00010101 00000110 00000011
```

Les masques de sous-réseau correspondants des interfaces de réseau local se présentent comme suit :

Adresses d'interface de réseau local

```
CLASSE A   73.1.5.2    =  11111111 11111111 11100000 00000000

CLASSE B   145.21.6.3  =  11111111 11111111 11111111 11000000
```

Si le réseau source T125 est sollicité pour envoyer un message au réseau de destination avec 114.16.23.8 pour adresse hôte (représentée en binaire par 01110010 00010000 00010111 00001000), le système vérifie si la destination est directement accessible via une interface locale.

Remarque : Le mot clé **subnetmask** doit être défini dans la base de données de configuration de chaque hôte appelé à desservir des sous-réseaux. En effet, les sous-réseaux ne sont utilisables que s'ils sont pris en charge par chaque hôte du réseau. Vous devez donc déclarer le masque de sous-réseau comme permanent dans la

base de données de configuration, via le menu SMIT Sélection d'une interface de réseau ou via l'application Web-based System Manager wsm network. Vous pouvez également déclarer le masque de sous–réseau dans le système d'exploitation via la commande **ifconfig**. (si vous utilisez **ifconfig**, la modification n'est pas permanente).

Adresses de diffusion

TCP/IP peut transmettre des données à tous les hôtes du réseau local ou des réseaux directement connectés. Ces transmissions sont appelées *messages de diffusion*. Par exemple, le démon de routage **routed** fait appel à ce type de message pour lancer des requêtes de routage ou y répondre.

Les données à diffuser aux hôtes des réseaux directement connectés sont transmises par les protocoles UDP (User Datagram Protocol) et IP (Internet Protocol), avec, dans l'en-tête IP, tous les bits de l'adresse de destination hôte positionnés à 1. Dans le cas de données à diffuser aux hôtes d'un réseau spécifique, tous les bits de la partie adresse locale de l'adresse IP sont positionnés à 0.

L'adresse de diffusion peut être modifiée temporairement via le paramètre *broadcast* dans la commande **ifconfig**. Modifiez-la de façon permanente avec le raccourci Web-based System Manager **wsm network** ou avec le raccourci SMIT **smit chinet**. Ceci peut s'avérer utile pour la compatibilité avec des versions antérieures de logiciels qui utilisent des adresses de diffusion différentes (avec, par exemple, des ID hôte définies à 0).

Adresses de bouclage local

Le protocole IP déclare l'adresse de réseau spéciale 127.0.0.1 comme adresse de bouclage local. Les hôtes utilisent cette adresse pour s'envoyer des messages à eux-mêmes. L'adresse de bouclage local est définie par le gestionnaire de configuration lors du démarrage du système. Le bouclage local est appliqué dans le noyau et peut également être défini avec la commande **ifconfig**. Le bouclage est appelé au lancement du système.

Adresses Internet officielles

L'organisme IR (Internet Registry) est chargé de fournir aux réseaux des identificateurs officiels (numéros de réseau IP, numéros de système autonome, etc.). Le DDN NIC (Defense Data Network, Network Information Center) remplit actuellement cette fonction. Pour obtenir une adresse Internet officielle, contactez le NIC aux coordonnées suivantes : INFO@INTERNIC.NET ou 1–800–444–4345 (Etats–Unis).

Affectation des adresses et paramètres TCP/IP - Protocole DHCP

Le protocole TCP/IP permet la communication entre machines disposant d'adresses configurées. L'affectation des adresses et la distribution des paramètres pour toutes les machines du réseau est une des tâches incombant à l'administrateur de réseau. Généralement, ce processus consiste pour l'administrateur à imposer une configuration à chaque utilisateur, tout en permettant à l'utilisateur de configurer sa propre machine. Toutefois, des erreurs de configuration ou des malentendus peuvent générer des appels de service que l'administrateur doit traiter individuellement. Le protocole DHCP (Dynamic Host Configuration Protocol) offre à l'administrateur une alternative, permettant d'exclure l'utilisateur final des problèmes de configuration et de gérer la configuration du réseau à partir d'un site central.

DHCP est un protocole de couche application qui permet à une machine du réseau, le *client*, d'obtenir du serveur une adresse IP ainsi que d'autres paramètres de configuration. Les informations sont obtenues au moyen d'un échange de paquets réalisé entre un démon sur le client et un autre sur le serveur. La plupart des systèmes d'exploitation proposent à l'heure actuelle un client DHCP dans leur module de base.

Pour obtenir une adresse, le démon du client DHCP (**dhcpcd** sur AIX) diffuse un message de découverte DHCP, qui est reçu et traité par le serveur. (Il est possible de configurer à cet effet plusieurs serveurs sur le réseau.) S'il existe une adresse disponible pour ce client, un message DHCP de proposition est créé, contenant une adresse IP et d'autres options client. Le client reçoit cette proposition DHCP et la stocke en attendant d'autres propositions. Il choisit ensuite la meilleure et diffuse une demande DHCP indiquant au serveur la proposition retenue.

Tous les serveurs DHCP configurés reçoivent la demande. Chacun d'eux vérifie qu'il n'est pas le serveur demandé. Si ce n'est pas le cas, le serveur libère l'adresse qu'il a affecté au client. En revanche, le serveur demandé marque que l'adresse est affectée et renvoie un accusé de réception DHCP, qui finalise la transaction et attribue au client une adresse pour une durée (délai) définie par le serveur.

A échéance de la moitié de ce délai, le client tente de renouveler la réservation de son adresse en envoyant au serveur un paquet de *renouvellement*. Si le serveur accepte la demande, il envoie un accusé de réception DHCP. Si le client ne parvient pas à obtenir une réponse de son serveur attitré, il diffuse un paquet de nouvelle liaison DHCP afin de tenter de joindre le serveur (celui–ci a pu, par exemple, être déplacé d'un réseau à un autre). Si, à l'expiration de la totalité du délai, le client n'a pas renouvelé son adresse, l'interface est arrêtée et le processus recommence à zéro. Ce cycle permet d'éviter que plusieurs clients d'un réseau ne se voient affecter la même adresse.

Le serveur DHCP procède à l'attribution des adresses en fonction de *clés*. Les quatre clés les plus courantes sont le réseau, la classe, le fournisseur et l'ID de client. Le serveur se sert de ces clés pour obtenir une adresse et un jeu d'options de configuration qu'il envoie au client.

réseau
: Identifie le segment de réseau d'où est issu le paquet. La clé réseau permet au serveur de vérifier sa base de données d'adresses et d'attribuer une adresse correspondant au segment de réseau.

classe
: Elle est entièrement configurable par le client. Elle peut comprendre une adresse et des options. Cette clé peut être utilisée pour préciser la fonction d'une machine du réseau ou décrire le mode de regroupement des machines adopté à des fins administratives. Ainsi, l'administrateur du réseau peut créer une classe `netbios` contenant les options destinées aux clients NetBIOS ou une classe `comptabilité` représentant les machines du service Comptabilité qui ont besoin d'accéder à une imprimante spécifique.

fournisseur Facilite l'identification du client à l'aide de sa plate–forme matérielle/logicielle (par exemple, un client Windows 95 ou un client OS/2 Warp).

ID client Identifie le client, soit par le nom d'hôte de sa machine soit par son adresse de couche MAC (medium access control). L'ID client figure dans le fichier de configuration du démon **dhcpcd**. Par ailleurs, il peut être utilisé par le serveur pour transmettre des options à un client ou pour empêcher un client de recevoir des paramètres.

Ces clés peuvent figurer dans le fichier de configuration soit seules, soit en combinaison. Si un client fournit plusieurs clés et que plusieurs adresses peuvent être allouées, le choix porte sur une clé et le jeu d'options découle de la clé choisie en premier. Pour plus d'informations sur la sélection des clés et des adresses, reportez–vous à la section Configuration de DHCP, page 3-66.

L'autre élément de la figure est un agent relais BOOTP. Un agent de ce type est requis pour que les diffusions initiales du client puissent quitter le réseau local. Ces agents assurent le relais des paquets DHCP et BOOTP.

Le serveur DHCP

Pour AIX version 4.3.1, le serveur DHCP a été divisé en trois grandes parties : une base de données, un moteur de protocole et un ensemble de routines de service, chaque partie disposant de ses propres informations de configuration.

La base de données DHCP

La base de données **db_file.dhcpo** permet d'effectuer le suivi des clients et des adresses et de contrôler les accès (par exemple, pour autoriser certains clients exclusivement à accéder à certains réseaux ou pour désactiver les clients BOOTP sur un réseau particulier). Les options sont également enregistrées dans la base de données d'où elles peuvent être extraites et distribuées aux clients. La base de données est implémentée sous la forme d'un objet pouvant être chargé de façon dynamique, ce qui facilite les mises à niveau et la maintenance du serveur.

A partir des informations du fichier de configuration, la base de données est amorcée et sa cohérence est vérifiée. Un ensemble de fichiers de points de contrôle met à jour la base de données et réduit le volume d'écritures vers le fichier de stockage principal. La base de données contient également des pools d'adresses et d'options, mais ceux–ci sont statiques et sont étudiés dans la section Configuration de DHCP, page 3-66.

Le fichier de stockage principal et sa copie de sauvegarde sont de simples fichiers ASCII qui peuvent, si nécessaire, être modifiés. Leur format est le suivant :

```
DF01
"CLIENT ID" "0.0.0.0" State LeaseTimeStart LeaseTimeDuration
LeaseTimeEnd
  "Server IP Address" "Class ID" "Vendor ID" "Hostname" "Domain
Name"
"CLIENT ID" "0.0.0.0" State LeaseTimeStart LeaseTimeDuration
LeaseTimeEnd
  "Server IP Address" "Class ID" "Vendor ID" "Host Name" "Domain
Name"
...
```

La première ligne indique la version du fichier : `DF01c` . Les lignes qui suivent définissent des enregistrements client. Le serveur procède à la lecture de la seconde ligne jusqu'à la fin du fichier. (Les paramètres entre guillemets doivent être indiqués entre guillemets.)

"CLIENT ID"
ID utilisé par le client pour se présenter au serveur.

"0.0.0.0" est l'adresse IP actuellement attribuée au serveur DHCP. Si aucune adresse n'a été attribuée, "0.0.0.0" sera adopté par défaut.

State Etat actuel du client. Le moteur de protocole DHCP contient le jeu de valeurs attribuables et les états sont gérés dans la base de données DHCP. Le nombre en regard de *State* représente sa valeur. Les différents états possibles sont :

(1) FREE Représente les adresses qui sont disponibles. En général, les clients n'ont pas cet état, à moins qu'aucune adresse ne leur ait encore été attribuée. **dadmin** et la sortie de **lssrc** signalent pour cet état "Free".

(2) RESERVED
Indique qu'une liaison " lâche " existe entre le client et l'adresse. Le client a envoyé un message de découverte DHCP, auquel le serveur DHCP a répondu, et le client n'a pas encore répondu par une requête DHCP demandant cette adresse. **dadmin** et la sortie de **lssrc** indiquent pour cet état "Reserved".

(3) BOUND Indique que le client et l'adresse sont liés et que l'adresse a été attribuée au client il y a déjà un certain temps. **dadmin** et la sortie de **lssrc** indiquent pour cet état "Leased".

(4) RELEASED Indique que le client et l'adresse sont liés, à titre d'information uniquement. Le protocole DHCP conseille aux serveurs DHCP de gérer les informations concernant leurs clients précédents à des fins de référence ultérieure (principalement pour essayer de redonner à un client une adresse qu'il a déjà utilisée dans le passé). Cet état signale que le client a libéré l'adresse. Cette adresse peut donc être utilisée par d'autres clients si aucune autre adresse n'est disponible. **dadmin** et la sortie de **lssrc** indiquent pour cet état "Released".

(5) EXPIRED Indique que le client et l'adresse sont liés, à titre d'information uniquement, de la même manière que l'état " released ". Cet état signale toutefois que le client a laissé son bail arriver à expiration. Une adresse arrivée à expiration est disponible et est réaffectée lorsque toutes les adresses libres sont indisponibles et avant que les adresses libérées ne soient réattribuées. **dadmin** et la sortie de **lssrc** indiquent pour cet état "Expired".

(6) BAD Représente une adresse utilisée sur le réseau mais qui n'a pas été distribuée par le serveur DHCP. Cet état qualifie également les adresses qui ont été rejetées par les clients. Les clients ne doivent pas avoir cet état. **dadmin** et la sortie de **lssrc** indiquent pour cet état "Used" et "Bad", respectivement.

Le seul état non mentionné ci–dessus est UNKNOWN (valeur 0), qui représente les clients n'ayant pas d'adresse. Cet état ne doit jamais être appliqué aux adresses. **dadmin** signale "Unknown" et **lssrc** "Corrupt" pour cet état.

LeaseTimeStart Début du bail actuel (en nombre de secondes écoulées depuis le 1er janvier 1970).

LeaseTimeDuration
Durée du bail (en secondes).

LeaseTimeEnd Utilise le même format que *LeaseTimeStart*, pour indiquer la fin du bail. Certaines options de configuration utilisent des valeurs différentes pour le début et la fin d'un bail et il est possible de substituer à ces valeurs des options du fichier de configuration. Reportez–vous à Syntaxe du fichier de serveur DHCP pour la base de données db_file, page 3-83.

"*Server IP Address*"
Adresse IP du serveur DHCP détenteur de cet enregistrement.

"*Class ID*"

"*Vendor ID*"

"*Host Name*"

"*Domain Name*"

Valeurs utilisées par le serveur pour déterminer les options qui sont envoyées au serveur (stockées sous la forme de chaînes entre guillemets). Ces paramètres permettent d'améliorer les performances, puisque les listes d'options peuvent être générées à l'avance pour ces clients au démarrage du serveur DHCP.

Fichiers de points de contrôle

La syntaxe des fichiers de points de contrôle n'est pas spécifiée. En cas de panne du serveur, ou si vous devez l'arrêter sans avoir pu fermer normalement la base de données, le serveur peut utiliser les fichiers de points de contrôle et les fichiers de sauvegarde pour reconstruire une base de données correcte. La pire situation serait de perdre un client (si le client était en cours d'écriture dans le fichier de point de contrôle au moment de la panne). Les fichiers par défaut sont :

/etc/db_file.cr fonctionnement normal de la base de données

/etc/db_file.crbk sauvegardes de la base de données

/etc/db_file.chkpt et **/etc/db_file.chkpt 2**
fichiers de point de contrôle en alternance

Le serveur DHCP pour AIX Versions 4.3.1 et ultérieures est du type enchaîné. Pour garantir un débit élevé, les opérations sur la base de données (y compris les opérations de sauvegarde) sont optimisées pour le type enchaîné. Lorsqu'une sauvegarde est demandée, le fichier de points de contrôle existant est remplacé par le fichier de points de contrôle suivant, le fichier de base de données existant est copié dans le fichier de secours et un nouveau fichier de sauvegarde est créé. Chaque enregistrement client est consigné et un bit est modifié afin d'indiquer que le client doit utiliser le nouveau fichier de points de contrôle pour la journalisation. Lorsque tous les enregistrements client sont pris en compte, la sauvegarde est fermée et les anciens fichiers de secours et de points de contrôle sont supprimés. De cette manière, les clients peuvent toujours être traités et, si l'enregistrement du client a été sauvegardé, les modifications s'inscrivent dans un nouveau fichier de sauvegarde ou un nouveau fichier de points de contrôle.

Le moteur de protocole DHCP

Pour AIX Versions 4.3.1 et ultérieures, le moteur de protocole DHCP a été mis au niveau de la norme RFC 2131, mais reste compatible avec RFC 1541. (Le serveur peut également traiter des options définies dans RFC 2132.) Le moteur de protocole utilise la base de donnés pour déterminer quelles informations doivent être retournées au client.

La configuration des pools d'adresses fait intervenir certaines options qui affectent l'état de la machine. Par exemple, le serveur DHCP interroge (ping) les adresses avant de les attribuer. La durée d'attente de la réponse par le serveur peut désormais être configurée pour chaque pool d'adresses.

Opérations DHCP enchaînées

Le dernier élément du serveur DHCP est en fait un ensemble d'opérations qui permettent d'assurer la continuité des opérations. Comme le serveur DHCP est du type enchaîné, ces opérations sont en fait définies sous la forme de routines qui interviennent occasionnellement pour s'assurer du bon déroulement des opérations.

La première routine, ou routine **principale**, gère les requêtes SRC (par exemple **startsrc**, **stopsrc**, **lssrc**, **traceson** et **refresh**). Cette routine coordonne également toutes les opérations qui affectent toutes les routines et gère les signaux. Par exemple :

- A SIGHUP (–1) provoque un rafraîchissement de toutes les bases de données du fichier de configuration.
- A SIGTERM (–15) entraîne l'arrêt en douceur du serveur.

La routine suivante, **dadmin**, interface avec le programme client **dadmin** et le serveur DHCP. L'outil dadmin peut être utilisé pour obtenir des informations sur l'état de la base de données et la modifier, et évite de modifier manuellement les différents fichiers de la base de données. Les versions antérieures du serveur DHCP empêchaient l'attribution d'adresses aux clients lorsqu'une requête d'état était en cours. Grâce aux routines **dadmin** et **src**, le serveur est désormais en mesure de gérer les requêtes de services tout en continuant à traiter les requêtes des clients.

La routine suivante est **garbage** qui, à intervalles réguliers, nettoie la base de données, la sauvegarde, purge les clients ne possédant pas d'adresse et supprime les adresses réservées qui le sont depuis trop longtemps. Les intervalles peuvent être configurés (reportez–vous à la section Configuration de DHCP, page 3-66). Les autres routines correspondent à des processeurs de paquet. Leur nombre peut être configuré et il est de 10 par défaut. Chaque routine peut traiter une requête émise par un client DHCP. Le nombre de processeurs de paquets requis est fonction de la charge et de la machine. Si la machine assure d'autres services que DHCP, il n'est peut être pas très sage de lancer 500 routines.

Préparation de DHCP

Pour exploiter ce protocole, l'administrateur réseau doit configurer un serveur DHCP ainsi que les agents relais BOOTP sur les liaisons dépourvues de serveur DHCP. Une planification anticipée peut permettre de réduire la charge de DHCP sur le réseau. Par exemple, si vous configurez un seul serveur pour gérer tous les clients, tous les paquets doivent transiter par ce serveur. Si vous ne disposez que d'un routeur entre deux grands réseaux, il est plus sage de prévoir deux serveurs, un sur chaque liaison.

Un autre aspect à considérer est le fait que DHCP implique une trame de trafic. Par exemple, si vous définissez un délai par défaut inférieur à 2 jours et que vous arrêtez les machines pendant le week-end, le trafic DHCP connaîtra une pointe le lundi matin. Bien que le trafic DHCP ne constitue pas une charge supplémentaire considérable, il doit néanmoins être pris en compte au moment de décider du nombre et de l'emplacement des serveurs DHCP sur le réseau.

L'objectif de DHCP est de libérer le client de toute saisie une fois DHCP activé pour intégrer le client au réseau. Le client DHCP, `dhcpcd`, lit un fichier de configuration, **dhcpcd.ini**, qui contient des informations sur la journalisation ainsi que les paramètres requis pour démarrer. L'installation terminée, il vous faut sélectionner la méthode de configuration de TCP/IP : configuration minimale ou DHCP. Si vous optez pour DHCP, vous devez choisir une interface et vous pouvez spécifier des paramètres facultatifs. Pour l'interface, vous pouvez sélectionner le mot–clé **any**, qui indique à `dhcpcd` d'utiliser la première interface en état de fonctionnement qu'il rencontre. Cette méthode minimise la quantité d'entrées côté client.

Configuration de DHCP

Par défaut, la configuration du serveur DHCP est effectuée par la lecture du fichier **/etc/dhcpsd.cnf**, qui spécifie la base de données initiale d'adresses et d'options du serveur. Le serveur est lancé dans le fichier **/etc/rc.tcpip**, à partir de Web-based System Manager, de SMIT, ou à l'aide de commandes SRC. Vous pouvez configurer un client DHCP via Web-based System Manager, SMIT ou en éditant un fichier ASCII plat.

La configuration de DHCP constitue la tâche la plus délicate dans le cadre de l'utilisation de DHCP dans votre réseau. Vous devez d'abord déterminer le nombre de réseaux qui devront accueillir des clients DHCP. Chaque sous–réseau du réseau principal représente un pool d'adresses que le serveur DHCP doit ajouter à sa base de données. Par exemple :

```
database db_file
{

    subnet 9.3.149.0 255.255.255.0
      {  option 3 9.3.149.1 # Passerelle par défaut que les
clients de ce réseau doivent utiliser
         option 6 9.3.149.2 # Serveur de noms que les clients de
ce réseau doivent utiliser
      }
    ... options ou autres conteneurs ajoutés ultérieurement
}
```

L'exemple ci–dessus représente un sous–réseau, `9.3.149.0` , avec un masque de sous–réseau `255.255.255.0` . Toutes les adresses de ce sous–réseau, de 9.3.149.1 à 9.3.149.254, sont contenues dans le pool. Eventuellement, il est possible de spécifier un intervalle à la fin de la ligne, ou d'inclure un intervalle ou une instruction d'exclusion dans le conteneur de sous–réseau. Pour plus d'informations sur les définitions et méthodes de configuration classiques, reportez–vous à Options connues du fichier de serveur DHCP, page 3-76.

La clause de base de données mentionnant `db_file` indique la méthode à utiliser pour le traitement de cette portion du fichier de configuration. Les commentaires sont introduits par le symbole #. Tout le texte placé entre le # et la fin de la ligne est ignoré par le serveur DHCP. Chaque ligne `option` est utilisée par le serveur pour indiquer au client ce qu'il doit faire. La section Options connues du fichier de serveur DHCP, page 3-76 décrit les options reconnues et prises en charge à l'heure actuelle. Pour savoir comment définir des options inconnues du serveur, reportez–vous à la section Syntaxe du fichier de serveur DHCP pour le fonctionnement général du serveur, page 3-80.

Si le serveur ne comprend pas comment analyser une option, il utilise des méthodes par défaut pour transmettre l'option au client. Ceci permet au serveur DHCP d'envoyer des options spécifiques à certains sites, qui ne sont pas définies dans les normes RFC, mais sont utilisables par certains clients ou certaines configurations de client.

Le fichier de configuration

Le fichier de configuration comprend une section d'adresses et une section de définition d'options, basées sur le concept des conteneurs, qui renferment les options, les modificateurs et, le cas échéant, d'autres conteneurs.

Un *conteneur* (qui est finalement une méthode de regroupement des options) fait appel à un identificateur pour classer les clients en plusieurs groupes. Les types de conteneur sont le sous–réseau, la classe, le fournisseur et le client. A l'heure actuelle, il n'existe pas de conteneur générique définissable par l'utilisateur. L'Identificateur définit le client de manière unique, de sorte qu'il soit possible de suivre sa trace même s'il est déplacé vers un autre sous–réseau. Il est possible d'utiliser plusieurs types de conteneur pour définir les droits d'accès du client.

Les *options* sont les identificateurs qui sont retournés au client, par exemple la passerelle par défaut et l'adresse de DNS.

Les *modificateurs* sont des instructions isolées qui modifient l'aspect d'un conteneur, par exemple la valeur par défaut de la durée du bail.

Conteneurs

Lorsque le serveur DHCP reçoit une requête, le paquet est analysé et les clés d'identification permettent de déterminer les conteneurs, les options et les adresses à extraire.

L'exemple précédent présente un conteneur de sous–réseau. La clé d'identification est la position du client au sein du réseau. Si le client fait partie de ce réseau, alors il est intégré à ce conteneur.

Chaque type de conteneur utilise une option différente pour identifier les clients :

- Le conteneur sous–réseau utilise le champ giaddr ou l'adresse de l'interface réceptrice pour déterminer le sous–réseau d'origine du client.
- Le conteneur classe utilise la valeur de l'option 77 (User Site Class Identifier – identificateur de la classe du site utilisateur).
- Le conteneur fournisseur utilise la valeur de l'option 60 (Vendor Class Identifier – identificateur de la classe du fournisseur).
- Le conteneur client utilise la valeur de l'option 61 (Client Identifier – identificateur du client) pour les clients DHCP et le champ chaddr du paquet BOOTP pour les clients BOOTP.

Sauf pour les sous–réseaux, chaque conteneur accepte la spécification de la valeur de correspondance à l'aide d'expressions régulières.

A ces conteneurs, il faut ajouter un conteneur implicite, le conteneur *global*. Sauf spécification contraire ou refus explicite, les options et modificateurs placés dans le conteneur global s'appliquent à tous les conteneurs. La plupart des conteneurs peuvent être inclus dans d'autres conteneurs, ce qui implique une certaine visibilité. Les conteneurs peuvent ou non être associés à des plages d'adresses. Tel est le cas, par nature, des sous–réseaux.

Les règles de base s'appliquant aux conteneurs et sous–conteneurs sont les suivantes :

- Tous les conteneurs sont valides au niveau général.
- Les sous–réseaux ne doivent jamais être inclus dans d'autres conteneurs.
- Des conteneurs restreints ne peuvent englober des conteneurs réguliers du même type. (Par exemple, un conteneur doté d'une option autorisant uniquement la classe `Comptabilité` ne peut receler un conteneur doté d'une option autorisant toutes les classes commençant par la lettre "c". Ceci n'est pas autorisé.)
- Les conteneurs client restreints ne peuvent englober de sous–conteneurs.

En tenant compte des règles ci–dessus, vous pouvez générer une hiérarchie de conteneurs qui répartissent les options en différents groupes pour des clients ou des ensembles de clients spécifiques.

Comment sont gérées les options et adresses lorsqu'un client correspond à plusieurs conteneurs ? Le serveur DHCP reçoit les messages, il transmet la requête à la base de données (fichier **db_file** en l'occurrence) et une liste de conteneurs est générée. La liste est organisée par ordre de profondeur et de priorité. La priorité se définit comme une hiérarchie implicite au sein des conteneurs. Les conteneurs stricts ont une priorité supérieure à celle des conteneurs réguliers. Les clients, les classes, les fournisseurs et enfin, les sous–réseaux sont triés, dans cet ordre, et à l'intérieur de chaque conteneur en fonction de leur profondeur. Ceci aboutit à une liste allant du plus spécifique au moins spécifique. Par exemple :

```
Sous-réseau 1
--Classe 1
--Client 1
Sous-réseau 2
--Classe 1
----Fournisseur 1
----Client 1
--Client 1
```

Cet exemple présente deux sous–réseaux, `Sous-réseau 1` et `Sous-réseau 2`. Il y a un nom de classe, `Classe 1`, un nom de fournisseur, `Fournisseur 1` et un nom de client, `Client 1`. `Classe 1` et `Client 1` sont définis en plusieurs endroits. Comme ils résident dans des conteneurs différents, leurs noms peuvent être identique mais leurs valeurs, différentes. Si `Client 1` envoie un message au serveur DHCP depuis `Sous-réseau 1` avec `Classe 1` spécifiée dans sa liste d'options, le serveur DHCP va générer le chemin de conteneur suivant :

```
Sous-réseau 1, Classe 1, Client 1
```

Le conteneur le plus spécifique apparaît en dernier. Pour obtenir une adresse, la liste est étudiée dans l'ordre inverse de la hiérarchie et la première adresse disponible est retenue. Ensuite, l'étude de la liste de poursuit en remontant dans la hiérarchie afin d'obtenir les options. Les options peuvent remplacer des valeurs précédentes, sauf si une option *deny* a été incluse dans le conteneur. Par ailleurs, puisque `Classe 1` et `Client 1` figurent dans `Sous-réseau 1`, ils sont ordonnés en fonction de la priorité de leur conteneur. Si le même client se trouve dans `Sous-réseau 2` et envoie le même message, la liste de conteneur générée sera :

`Sous-réseau 2, Classe 1, Client 1` (au niveau de `Sous-réseau 2`), `Client 1` (au niveau de `Classe 1`)

`Sous-réseau 2` apparaît en premier, suivi de `Classe 1` , puis de `Client 1` au niveau de `Sous-réseau 2` (car cette instruction client ne se trouve qu'à un niveau en dessous dans la hiérarchie). Cette hiérarchie implique qu'un client correspondant à la première instruction client est moins spécifique que le client correspondant à `Client 1` de `Classe 1` au sein de `Sous-réseau 2`.

La priorité sélectionnée en fonction de la profondeur dans la hiérarchie prend le pas sur la priorité des conteneurs eux–mêmes. Par exemple, si le même client émet le même message, en précisant cette fois un identificateur de fournisseur, la liste de conteneur devient :

`Sous-réseau 2, Classe 1, Fournisseur 1, Client 1` (au niveau de `Sous-réseau 2`), `Client 1` (au niveau de `Classe 1`)

La priorité au niveau des conteneurs améliore les performances en matière de recherche car elle correspond à un concept général selon lequel les conteneurs client constituent le moyen le plus spécifique de définir un ou plusieurs clients. Le conteneur client contient des adresses plus spécifiques qu'un conteneur classe, lui–même plus spécifique qu'un conteneur fournisseur, le conteneur sous–réseau étant le moins spécifique de tous.

Adresses et plages d'adresses

Les plages d'adresses, obligatoires pour les conteneurs sous–réseau, peuvent être associées à tout type de conteneur. Chaque plage définie pour un conteneur doit être un sous–ensemble de la plage du conteneur parent et ne doit pas présenter de chevauchement avec la plage d'un autre conteneur. Par exemple, si une classe définie dans un sous–réseau est associée à une plage d'adresses, cette plage doit constituer un sous–ensemble des adresses de la plage du sous–réseau. En outre, le conteneur de la classe ne doit pas recouvrir, même partiellement, d'autres plages d'adresses au même niveau.

Les plages peuvent être définies sur la ligne du conteneur et modifiées au moyen d'instructions de plages et d'exclusion afin que des jeux d'adresse non contigus puissent être associés à un conteneur. Ainsi, si les dix premières adresses d'un sous–réseau sont disponibles, ainsi que les dix suivantes, le sous–réseau peut spécifier ces adresses par plage dans la clause de sous–réseau afin de réduire l'utilisation de la mémoire et les risques de collision d'adresses avec d'autres clients ne se trouvant pas dans les plages spécifiées.

Dès qu'une adresse est sélectionnée, tout conteneur suivant dans la liste contenant les plages d'adresses est retiré de la liste, avec ses enfants. La raison en est que les options spécifiques au réseau dans les conteneurs supprimés ne sont pas valides si l'adresse n'est pas utilisée à partir de ce conteneur.

Options

Une fois la liste ponctionnée pour déterminer les adresses, un ensemble d'options est généré pour le client. Lors de ce processus de sélection, les nouvelles options remplacent les options précédemment sélectionnées, sauf si une clause *deny* est rencontrée, auquel cas l'option refusée est retirée de la liste envoyée au client. Cette méthode autorise les héritages à partir des conteneurs parents afin de réduire la quantité de données à spécifier.

Modificateurs

Les modificateurs sont des éléments qui modifient l'aspect de certains conteneurs, par exemple le type d'accès ou la durée du bail. Après avoir défini les pools d'options et d'adresses, réfléchissez aux modificateurs à ajouter aux conteneurs. Les plus courants sont **leasetimedefault**, **supportBootp** et **supportUnlistedclients**.

leasetimedefault
: Définit la durée pendant laquelle une adresse est louée à un client.

supportBootp Détermine si le serveur doit répondre aux clients BOOTP.

supportUnlistedclients
: Indique si un client doit être explicitement défini par une instruction de client pour recevoir une adresse. La valeur de supportUnlistedClients peut être **none (aucun)** , **dhcp**, **bootp** ou **both (les deux)**. Vous pouvez ainsi restreindre l'accès des clients bootp et autoriser tous les clients DHCP à obtenir des adresses.

Pour connaître les autres modificateurs, reportez–vous à Syntaxe du fichier de serveur DHCP pour la base de données db_file, page 3-83.

Journalisation

Une fois les modificateurs sélectionnés, configurez la fonction de journalisation. Les paramètres de journalisation sont précisés dans un conteneur tel que la base de données, mais le mot de passe du conteneur est : **logging_info**. Au démarrage, il est conseillé d'activer le niveau de journalisation le plus élevé. En outre, il est préférable de configurer cette fonction préalablement à toute autre afin que les erreurs de configuration puissent être consignées après initialisation du sous–système de journalisation. Le mot–clé **logitem** active le niveau de journalisation ; si vous supprimez **logitem,** le niveau de journalisation sera désactivé. Les autres mots–clé concernant la journalisation permettent d'indiquer le nom du fichier journal, sa taille et le nombre de journaux utilisés en alternance.

Options spécifiques au serveur

Le dernier groupe de paramètres concerne les options spécifiques au serveur, et permet à l'utilisateur de contrôler le nombre de processeurs de paquets, la fréquence d'exécution des routines de nettoyage, etc.

Voici deux exemples d'options spécifiques au serveur :

reservedTime Indique pendant combien de temps une adresse doit rester à l'état réservé après l'envoi d'une OFFRE au client DHCP

reservedTimeInterval
: Indique à quelle fréquence le serveur DHCP doit analyser les adresses pour vérifier si certaines ne sont pas à l'état réservé depuis une durée supérieure à celle définie par **reservedTime**.

Ces options sont pratiques si vous avez plusieurs clients qui diffusent des messages DISCOVER, mais qui n'envoient pas de message REQUEST ou que leur message REQUEST se perd sur le réseau. Ces paramètres permettent d'éviter la réservation indéfinie des adresses pour un client non conforme.

Une autre option particulièrement importante, **SaveInterval**, permet de définir la fréquence de sauvegarde. Toutes les options spécifiques au serveur sont abordées dans la section Syntaxe du fichier de serveur DHCP pour le fonctionnement général du serveur, page 3-80, avec les mots–clés de journalisation.

Considérations de performance

Vous n'êtes pas sans savoir que certains mots–clé de configuration ainsi que la structure du fichier de configuration ont une incidence sur l'utilisation de la mémoire et les performances du serveur DHCP.

Premièrement, il est possible d'éviter toute sollicitation excessive de la mémoire en appréhendant le modèle d'héritage des options des conteneurs parents vers les conteneurs enfants. Dans un environnement qui ne prend pas en charge les clients non répertoriés, l'administrateur doit expressément lister chaque client du fichier. Lorsque des options sont répertoriées pour chaque client en particulier, le serveur sollicite plus de capacité mémoire pour stocker cette structure de configuration arborescente que lorsque des options sont héritées d'un conteneur parent (conteneurs de sous–réseau, de réseau ou conteneurs globaux, par exemple). Par conséquent, l'administrateur doit vérifier la répétition ou non des options relatives au client au sein du fichier de configuration. Si tel est le cas, il doit décider si ces options peuvent ou non être définies dans le conteneur parent et partagées par l'ensemble des clients.

Deuxièmement, l'utilisation des entrées **logItem** INFO et TRACE entraîne la consignation de nombreux messages au cours du traitement de chaque message du client DHCP. L'ajout d'une ligne au journal peut s'avérer une opération onéreuse. C'est pourquoi, la limitation du volume de journalisation améliore les performances du serveur DHCP. En cas de présomption d'erreur sur le serveur DHCP, la journalisation peut être dynamiquement réactivée à l'aide des commandes SRC traceson ou dadmin.

Troisièmement, la sélection d'une valeur **numprocessors** doit dépendre de la taille du réseau DHCP, du paramètre de configuration **pingTime db_file** et du délai de propagation type sur le réseau. Etant donné que chaque routine de processeur de paquet émet une requête d'écho ICMP pour vérifier l'état de l'adresse serveur avant de l'attribuer à un client, le délai de réponse affecte directement la durée de traitement d'un message DISCOVER. La routine de processeur de paquet se borne essentiellement à attendre une réponse ou le **pingTime**. Par conséquent, la réduction de la valeur **numprocessors** améliore le temps de réponse du serveur, et réduit par là–même le nombre de retransmissions par clients, sans pour autant sacrifier les avantages que présentent le ping inhérent à la conception du serveur.

Pour optimiser les performances, sélectionnez une valeur **pingTime** basée sur le délai de propagation des réseaux distants pris en charge par le serveur DHCP. Sélectionnez également **numprocessors** en fonction de la valeur **pingTime** et de la taille du réseau. La sélection d'une valeur trop basse peut entraîner l'arrêt de toutes les routines de traitement de paquet dans l'attente des réponses d'écho tandis que les messages client DHCP entrants sont mis en attente sur le port du serveur. Celui–ci traite alors les messages client par lots au lieu de les traiter en continu.

Afin d'éviter ce cas de figure, la valeur de **numprocessors** doit être supérieure au nombre prévu de messages DISCOVER pouvant être reçus dans un intervalle **pingTime** au cours d'une période de forte activité client sur le DHCP. Toutefois, ne définissez pas une valeur trop élevée pour **numprocessors** car la gestion de routines risquerait d'encombrer le noyau.

A titre d'exemple, les valeurs **numprocessors 5** et **pingTime 300** offrent de faibles performances dans un environnement pouvoir recevoir 10 messages DISCOVER par seconde. En effet, en cas de forte sollicitation, 5 messages seulement peuvent être traités toutes les 3 secondes. Cet environnement doit être configuré avec des valeurs se rapprochant de **numprocessors 20** et de **pingTime 80**.

Personnalisation d'un fichier de configuration

De nombreux administrateurs réseau ont à gérer des réseaux comprenant plusieurs types de clients : ainsi, on peut trouver dans le même réseau des ordinateurs Windows 95, des ordinateurs AIX, des ordinateurs OS/2, des clients Java et des machines IBM Thin Client. Chaque type de machine requiert des identificateurs de fournisseurs uniques (c'est ce champ qui permet d'indiquer le type de machine au serveur DHCP). Les clients Java et les machines Thin Client peuvent exiger des paramètres qui leur sont propres, par exemple bootfiles, et il est possible que vous deviez adapter les options de configuration en conséquence. En revanche, les ordinateurs Windows 95 ne vont pas gérer correctement les options spécifiques à Java. Il est donc possible d'encapsuler les options spécifiques à chaque machine au sein de son conteneur fournisseur.

Pour reprendre notre exemple, imaginez une tâche principale dédiée à certaines machines en fonction de leurs utilisateurs. Par exemple, le personnel de développement peut travailler sur des clients AIX pour effectuer des travaux de programmation, le personnel du service marketing peut utiliser des clients OS/2, les membres du service des ventes peuvent préférer les clients Java et les machines IBM Thin Client, tandis que la comptabilité a adopté des machines Windows 95. Chacune de ces familles d'utilisateurs peut avoir besoin d'options de configuration différentes (imprimantes, serveurs de noms ou serveurs Web par défaut, etc.) Dans un tel cas, il est possible d'inclure ces options dans le conteneur fournisseur, puisque chaque groupe utilise un type de machine différent. Si le même type de machine était utilisé par plusieurs groupes, il serait possible de placer les options au sein d'un identificateur de classe subordonné, ce qui permettrait, par exemple, aux directeurs du marketing d'utiliser un groupe d'imprimantes non accessible au reste du personnel.

Remarque : L'exemple suivant représente une portion d'un fichier de configuration. Les commentaires sont précédés d'un symbole # et indiquent l'effet de chaque ligne sur l'installation.

```
vendor ”AIX_CLIENT”
{
# Pas d’option spécifique, les différents éléments sont traités
en fonction de leur classe
}

vendor ”OS/2 Client”
{
# Pas d’option spécifique, les différents éléments sont traités
en fonction de leur classe
}

vendor ”Windows 95”
{ option 44 9.3.150.3          # Serveur de noms NetBIOS par
défaut
}

vendor ”Java OS”
{ bootstrapserver 9.3.150.4    # Serveur TFTP par défaut pour les
boîtes Java
  option 67 ”javaos.bin”       # Fichier de démarrage de la boîte
Java OS
}

vendor ”IBM Thin Client”
{ bootstrapserver 9.3.150.5    # Serveur TFTP par défaut pour les
boîtes Thin Client
  option 67 ”thinos.bin”       # Fichier de démarrage par défaut
pour les boîtes Thin Client
}

subnet 9.3.149.0 255.255.255.0
{ option 3 9.3.149.1           # Passerelle par défaut pour le
sous-réseau
  option 6 9.3.150.2           # Serveur de noms pour le
sous-réseau
  class accounting 9.3.149.5-9.3.149.20
  {       # La classe de facturation est limitée à la plage
d’adresses  9.3.149.5-9.3.149.20
          # L’imprimante destinée à ce groupe fait également
partie de cette plage, elle est donc exclue.
     exclude 9.3.149.15
     option 9 9.3.149.15       # Serveur LPR (serveur
d’impression)
     vendor ”Windows 95”
     {
     option 9 deny              # Cette installation de Windows
95 ne prend pas en charge
                                # cette imprimante, l’option est
donc refusée.
     }
  }
 . . .
}
```

DHCP et DDNS (Dynamic Domain Name System – Système de noms de domaine dynamique)

Le serveur DHCP fournit des options permettant le fonctionnement en environnement DDNS. Pour utiliser DHCP dans l’environnement DDNS, vous devez définir et utiliser une zone dynamique sur un serveur DNS.

Une fois le serveur DDNS configuré, vous devez décider si le serveur DHCP doit effectuer des mises à jour d’enregistrement A, des mises à jour d’enregistrement PTR, des mises à

jour pour les deux types d'enregistrement ou aucune mise à jour. Cette décision dépendra de la part de travail que peut prendre en charge la machine client.

- Si le client peut assumer une partie de la mise à jour, vous pouvez confier les mises à jour d'enregistrement PTR au serveur et les mises à jour d'enregistrement A au client.
- Si le client peut tout assumer, configurez le serveur de sorte qu'il n'effectue aucune mise à jour.
- Si le client ne peut se charger de rien, configurez le serveur de sorte qu'il effectue les deux types de mise à jour.

Le serveur DHCP dispose d'un jeu de mots–clés de configuration qui vous permettent de déclencher l'exécution d'une commande lorsqu'une mise à jour est requise. Ce sont les suivants :

updatedns (déconseillé) Représente la commande à exécuter pour effectuer n'importe quel type de mise à jour. Elle sera appelée pour les enregistrements A et les enregistrements PTR.

updatednsA Spécifie la commande de mise à jour de l'enregistrement A.

updatednsP Spécifie la commande de mise à jour de l'enregistrement PTR.

Ces mots–clés définissent des chaînes exécutables que le serveur DHCP exécute lorsqu'une mise à jour est nécessaire. Les chaînes de mot–clé doivent contenir quatre `%s` (symbole de pourcentage, lettre s). Le premier `%s` correspond au nom d'hôte ; le second, au nom de domaine ; le troisième, à l'adresse IP et le quatrième, à la durée du bail. Ils sont utilisés comme quatre premiers paramètres de la commande AIX **dhcpaction**. Les deux autres paramètres de **dhcpaction** indiquent l'enregistrement à mettre à jour (A, PTR, NONE ou BOTH) et si NIM doit être actualisé (NIM or NONIM). Pour plus d'informations sur les interactions NIM et DHCP, reportez–vous à DHCP et gestion NIM (Network Installation Management), page 3-96. Par exemple :

```
updatednsA "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' A NONIM"
          # Ceci applique la commande dhcpaction uniquement à
l'enregistrement A
          updatednsP "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s'
          PTR NONIM"
          # Ceci applique la commande uniquement à
l'enregistrement PTR
          updatedns "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s'
          BOTH NIM"
          # Ceci applique la commande aux deux enregistrements
          et actualise NIM
```

Le serveur DHCP dispose également d'un jeu de mots–clés pour supprimer les entrées DNS lorsqu'un bail est libéré ou arrive à expiration. Ce sont les suivants :

releasednsA Supprime l'enregistrement A.

releasednsP Supprime l'enregistrement PTR.

removedns Supprime les deux types d'enregistrement.

Ces mots–clés définissent des chaînes exécutables que le serveur DHCP exécute lorsqu'une adresse est libérée ou périmée. AIX fournit une commande, **dhcpremove**, qui fonctionne de la même manière que **dhcpaction**, mais n'accepte que trois paramètres :

1. L'adresse IP, spécifiée sous la forme d'un `%s` dans la chaîne de commande
2. L'enregistrement à supprimer (A, PTR, NONE ou BOTH).
3. L'actualisation éventuelle de NIM (NIM ou NONIM).

```
releasednsA "/usr/sbin/dhcpremove '%s' '%s' '%s' A NONIM"
          # Ceci applique la commande dhcpremove uniquement à
l'enregistrement A
         releasednsP "/usr/sbin/dhcpremove '%s' '%s' '%s'
         PTR NONIM"
         # Ceci applique la commande uniquement à
l'enregistrement PTR
         removedns "/usr/sbin/dhcpremove '%s' '%s' '%s' BOTH NIM"
         # Ceci applique la commande aux deux enregistrements
         et actualise NIM
```

Les scripts **dhcpaction** et **dhcpremove** effectuent quelques vérifications sur les paramètres, puis définissent un appel vers **nsupdate**, qui a été adapté pour fonctionner avec les serveurs DDNS AIX et OS/2. Pour plus d'informations, reportez–vous à la description de la commande **nsupdate**.

Si l'interaction NIM n'est **PAS** requise par la mise à jour des noms, le serveur DHCP peut être configuré afin d'utiliser un transfert de sockets entre le démon DHCP et la commande **nsupdate** afin d'améliorer les performances et de permettre la reprise des mises à jour DNS à la suite d'une défaillance. Pour configurer cette option, le premier mot cité dans le mot–clé **updateDNSA**, **updateDNSP**, **releaseDNSA** ou **releaseDNSP** doit être "nsupdate_daemon". Les paramètres et les indicateurs de mise à jour sont identiques à ceux qui sont acceptés par la commande **nsupdate**. De plus, les noms de variables suivants peuvent être utilisés en remplacement :

$hostname	Remplacé par le nom d'hôte du client lors de la mise à jour DNS ou par le nom d'hôte préalablement associé au client pour le retrait DNS.
$domain	Remplacé par le domaine DNS relatif à la mise à jour ou par le domaine préalablement utilisé pour le nom d'hôte du client dans le cas de retrait DNS.
$ipadress	Remplacé par l'adresse IP associée ou dissociée du nom du client DHCP.
$leasetime	Remplacé par la durée du bail (en secondes).
$clientid	Remplacé par la représentation en chaîne de l'identificateur du client DHCP ou par l'association du type de matériel et de l'adresse matérielle pour les clients BOOTP.

A titre d'exemple :

```
updateDNSA "nsupdate_daemon -p 9.3.149.2 -h $hostname -d $domain
-s"d;a;*;a;a;$ipaddress;s;$leasetime;3110400""

updateDNSP "nsupdate_daemon -p 9.3.149.2 -r $ipaddress
-s"d;ptr;*;a;ptr;$hostname.$domain.;s;$leasetime;3110400""

releaseDNSA "nsupdate_daemon -p 9.3.149.2 -h $hostname -d $domain
-s"d;a;*;s;1;3110400""

releaseDNSP "nsupdate_daemon -p 9.3.149.2 -r $ipaddress
-s"d;ptr;*;s;1;3110400""
```

Pour plus d'informations, reportez–vous à la description de la commande **nsupdate**.

Des dispositifs définis par l'administrateur ont également été ajoutés pour les échanges de noms d'hôte entre le serveur et les clients. Par défaut, le nom d'hôte retourné au client et utilisé pour une mise à jour DDNS correspond à l'option 12 (définie dans le fichier de configuration du serveur). Toutefois, ce nom d'hôte par défaut peut également être un nom d'hôte suggéré par le client, par le biais de l'option 81 (option DHCPDDNS) ou de l'option 12 (option HOSTNAME). L'administrateur a la possibilité de remplacer ce nom d'hôte par défaut en utilisant les mots–clés de configuration **hostnamepolicy**, **proxyarec** et

appenddomain. Ces options et leurs paramètres sont définies dans Syntaxe du fichier de serveur DHCP pour la base de données db_file, page 3-83.

Compatibilité DHCP avec les versions antérieures

Le serveur DHCP pour AIX Versions 4.3.1 et ultérieures reconnaît les fichiers de configuration et de base de données des versions antérieures, **dhcps.ar** et **dhcps.cr**. Il analyse les anciens fichiers de configuration et génère de nouveaux fichiers de base de données aux anciens emplacements. Les anciennes bases de données sont automatiquement converties au nouveau format. Le fichier de configuration lui–même n'est pas converti.

Le module de base de données du serveur DHCP, **db_file**, est capable de lire l'ancien format. Le serveur DHCP est en mesure de détecter si un conteneur de base de données est absent du fichier de configuration et considère dans ce cas que le fichier contient tous les paramètres de serveur, les paramètres de journalisation et les paramètres de base de données **db_file**.

Remarque : Une partie de la syntaxe de l'ancien fichier de configuration est déconseillée mais toujours prise en charge. Les autres éléments obsolètes sont les suivants :

- Le conteneur réseau est totalement obsolète. Pour obtenir une spécification correcte, convertissez la clause réseau en une plage au sein d'un conteneur de sous–réseau correct mentionnant une adresse de sous–réseau, un masque de sous–réseau et la plage d'adresses. Si le conteneur réseau renferme des conteneurs de sous–réseau, supprimez le mot–clé du conteneur réseau et ses accolades, puis placez le masque de sous–réseau à l'endroit approprié sur la ligne. Pour démarrer à l'aide du conteneur base de données, regroupez tous les éléments ayant trait au réseau et aux accès client dans un seul conteneur de base de données de type **db_file**.
- Les mots–clés **updatedns** et **removedns** sont obsolètes et seront remplacés de préférence par la spécification des actions à appliquer individuellement aux enregistrements A et PTR.
- Les mots–clés **clientrecorddb** et **addressrecorddb** ont été supplantés respectivement par **clientrecorddb** et **backupfile**.
- Les mots–clés **option sa** et **option ga** ont été remplacés respectivement par **bootstrapserver** et **giaddrfield**. Pour plus d'informations, reportez–vous à la section Syntaxe du fichier de serveur DHCP pour le fonctionnement général du serveur, page 3-80 et à Syntaxe du fichier de serveur DHCP pour la base de données db_file, page 3-83.

Options connues du fichier de serveur DHCP

Remarque : Les options du tableau suivant qui sont marquées non autorisées peuvent être spécifiées (Non dans la colonne Autorisée ?) dans le fichier de configuration mais seront remplacées par la valeur réelle. Pour une définition plus complète de chaque option, reportez–vous à la norme RFC 2132.

Numéro de l'option	Type de données par défaut	Autorisée ?	Description/Emploi
0	Aucun	Non	Complète le champ d'option, si nécessaire. Le serveur ajoute des caractères de remplissage le cas échéant.
1	Dotted quad (quatre numéros séparés par points)	Non	Masque du sous–réseau d'où est tiré l'adresse.
2	Entier 32 bits	Oui	Indique le décalage du sous–réseau du client, en secondes du système UTC (Coordinated Universal Time).

Numéro de l'option	Type de données par défaut	Autorisée ?	Description/Emploi
3	Un ou plusieurs "dotted quad"	Oui	Liste des adresses IP de la passerelle par défaut.
4	Un ou plusieurs "dotted quad"	Oui	Liste des adresses IP des serveurs horaires.
5	Un ou plusieurs "dotted quad"	Oui	Liste des adresses IP des serveurs de noms.
6	Un ou plusieurs "dotted quad"	Oui	Liste des adresses IP des DNS.
7	Un ou plusieurs "dotted quad"	Oui	Liste des adresses IP des serveurs de journaux.
8	Un ou plusieurs "dotted quad"	Oui	Liste des adresses IP des serveurs de "cookies".
9	Un ou plusieurs "dotted quad"	Oui	Liste des adresses IP des serveurs LPR.
10	Un ou plusieurs "dotted quad"	Oui	Liste des adresses IP des serveurs Impress.
11	Un ou plusieurs "dotted quad"	Oui	Liste des adresses IP des serveurs de localisation des ressources.
12	Chaîne ASCII	Oui	Nom d'hôte du client à utiliser.
13	Entier 16 bits non signé	Oui	Taille du fichier de démarrage.
14	Chaîne ASCII	Oui	Chemin d'accès du fichier Merit Dump.
15	Chaîne ASCII	Oui	Nom de domaine DNS par défaut.
16	Adresse IP	Oui	Adresse du serveur Swap.
17	Chaîne ASCII	Oui	Chemin d'accès racine par défaut.
18	Chaîne ASCII	Oui	Chemin d'accès aux extensions pour le client.
19	Yes, No, True, False, 1, 0	Oui	Indique si le réacheminement IP doit être activé ou non.
20	Yes, No, True, False, 1, 0	Oui	Indique si le routage source non local doit être utilisé.
21	Une ou plusieurs paires de "dotted quad", sous la forme *DottedQuad*:*DottedQuad*	Oui	Dispositifs de filtre pour les adresses IP.
22	Entier 16 bits non signé	Oui	Taille maximale autorisée pour les fragments de datagrammes.
23	Entier 8 bits non signé	Oui	TTL (time–to–live) IP.
24	Entier 32 bits non signé	Oui	Nombre de secondes à utiliser dans le délai de vieillissement du MTU d'accès.
25	Liste d'un ou plusieurs entiers 16 bits non signés	Oui	Table des valeurs MTU d'accès. Spécifie un ensemble de valeurs représentant les tailles MTU à utiliser lors de la recherche de MTU d'accès.
26	Entier 16 bits non signé	Oui	Taille MTU pour l'interface réceptrice.
27	Yes, No, True, False, 1, 0	Oui	Indique si tous les sous–réseaux sont locaux.
28	Une adresse IP ("dotted quad")	Oui	Diffuse une adresse pour l'interface.

Numéro de l'option	Type de données par défaut	Autorisée ?	Description/Emploi
29	Yes, No, True, False, 1, 0	Oui	Indique si la recherche de masque de réseau ICMP doit être utilisée.
30	Yes, No, True, False, 1, 0	Oui	Indique si le client doit devenir un fournisseur de masque de réseau ICMP.
31	Yes, No, True, False, 1, 0	Oui	Indique si les messages de recherche de routeur ICMP doivent être utilisés.
32	Une adresse IP (”dotted quad”)	Oui	Adresse à utiliser pour la sollicitation du routeur.
33	Une ou plusieurs paires d'adresses IP, sous la forme *DottedQuad:DottedQuad*	Oui	Chaque paire d'adresses représente une route statique.
34	Yes/No, True/False, 1/0	Oui	Indique si l'encapsulation de fin doit être utilisée.
35	Entier 32 bits non signé	Oui	Valeur du délai de cache ARP.
36	Yes/No, True/False, 1/0	Oui	Indique si l'encapsulation Ethernet doit être utilisée.
37	Entier 8 bits non signé	Oui	TTL (time–to–live) TCP.
38	Entier 32 bits non signé	Oui	Intervalle de garde en vie (keep alive) TCP.
39	Yes/No, True/False, 1/0	Oui	Indique si la garde en vie (keep alive) TCP doit être utilisée.
40	Chaîne ASCII	Oui	Domaine NIS par défaut.
41	Un ou plusieurs ”dotted quad”	Oui	Adresses IP des serveurs NIS.
42	Un ou plusieurs ”dotted quad”	Oui	Adresses IP des serveurs NTP.
43	Chaînes hexadécimales de chiffres, sous la forme hex ”*digits*”, hex ”*digits*” ou 0x*digits*	Oui, mais spécifiée en fait uniquement pour le conteneur fournisseur	Conteneur en option encapsulé pour le conteneur fournisseur.
44	Un ou plusieurs ”dotted quad”	Oui	Adresses IP des serveurs de noms NetBIOS.
45	Un ou plusieurs ”dotted quad”	Oui	Adresses IP des serveurs de distribution de datagramme NetBIOS.
46	Entier 8 bits non signé	Oui	Type de nœud NetBIOS.
47	Chaînes hexadécimales de chiffres, sous la forme hex ”*digits*”, hex ”*digits*” ou 0x*digits*	Oui	Portée NetBIOS.
48	Un ou plusieurs ”dotted quad”	Oui	Adresses IP des serveurs de polices X Windows.
49	Un ou plusieurs ”dotted quad”	Oui	Gestionnaire d'affichage X Windows.
50	Aucun	Non	Adresse IP demandée, utilisée par le client pour indiquer l'adresse souhaitée.

Numéro de l'option	Type de données par défaut	Autorisée ?	Description/Emploi
51	Entier 32 bits non signé	Oui	Durée du bail pour l'adresse retournée. Par défaut, le serveur DHCP utilise le mot–clé **leasetimedefault**, mais la spécification directe de l'option `51` prend le pas sur la valeur.
52	Aucun	Non	Options éventuelles. Le client utilise ce paramètre pour indiquer que les champs **sname** et **file** du paquet BOOTP peuvent avoir des options.
53	Aucun	Non	Le serveur ou le client DHCP utilise cette option pour indiquer le type de message DHCP.
54	Aucun	Non	Le serveur ou le client DHCP utilise cette option pour indiquer l'adresse du serveur ou le serveur auquel le message est envoyé.
55	Aucun	Non	Le client DHCP utilise ce paramètre pour indiquer les options souhaitées.
56	Chaîne ASCII	Oui	Chaîne que le serveur DHCP envoie au client. En général, elle peut être utilisée par le client et le serveur DHCP pour signaler des problèmes.
57	No	Non	Le client DHCP utilise cette option pour indiquer au serveur DHCP la taille de paquet DHCP maximale que le client peut recevoir.
58	Entier 32 bits non signé	Oui	Nombre de secondes pendant lesquelles le client doit attendre avant d'envoyer un paquet de renouvellement.
59	Entier 32 bits non signé	Oui	Nombre de secondes pendant lesquelles le client doit attendre avant d'envoyer un paquet de nouvelle liaison.
60	Aucun	Non	Le client DHCP utilise cette option pour indiquer son type de fournisseur. Le client DHCP utilise ce champ pour la correspondance avec les conteneurs fournisseur.
61	Aucun	Non	Le client DHCP utilise ce paramètre pour s'identifier de manière unique. Le serveur DHCP utilise ce champ pour la correspondance avec les conteneurs client.
64	Chaîne ASCII	Oui	Spécifie le domaine NIS+.
65	Un ou plusieurs "dotted quad"	Oui	Adresses IP des serveurs NIS+.
66	Chaîne ASCII	Oui	Spécifie le nom du serveur TFTP. Ce nom d'hôte est utilisé à la place du champ **siaddr** si le client comprend cette option.

Numéro de l'option	Type de données par défaut	Autorisée ?	Description/Emploi
67	Chaîne ASCII	Oui	Spécifie le nom du fichier de démarrage. Ce paramètre peut être utilisé à la place du mot–clé **bootfile**, qui insère le nom du fichier dans le champ **nom de fichier** du paquet.
68	Un ou plusieurs "dotted quad" ou NONE	Oui	Adresses des agents personnels.
69	Un ou plusieurs "dotted quad"	Oui	Serveurs SMTP par défaut à utiliser.
70	Un ou plusieurs "dotted quad"	Oui	Serveurs POP3 par défaut à utiliser.
71	Un ou plusieurs "dotted quad"	Oui	Serveurs NNTP par défaut à utiliser.
72	Un ou plusieurs "dotted quad"	Oui	Serveurs WWW par défaut à utiliser.
73	Un ou plusieurs "dotted quad"	Oui	Serveurs Finger par défaut à utiliser.
74	Un ou plusieurs "dotted quad"	Oui	Serveurs IRC par défaut à utiliser.
75	Un ou plusieurs "dotted quad"	Oui	Serveurs Street Talk par défaut à utiliser.
76	Un ou plusieurs "dotted quad"	Oui	Serveurs de renseignements Street Talk par défaut à utiliser.
77	Chaîne ASCII	Oui	Identificateur de la classe du site utilisateur. Le serveur DHCP utilise ce champ pour la correspondance avec les conteneurs classe.
81	Chaîne ASCII plus d'autres éléments	Non	Le client DHCP utilise cette option pour définir la politique que doit suivre le serveur DHCP vis à vis de DDNS.
255	Aucun	Non	Le serveur et le client DHCP utilisent cette option pour signaler la fin d'une liste d'options.

Syntaxe du fichier de serveur DHCP pour le fonctionnement général du serveur

Remarque : Les unités de temps (*time_units*) indiquées dans le tableau suivant sont facultatives et correspondent à un modificateur du temps réel. L'unité de temps par défaut est exprimée en minutes. Les valeurs autorisées sont les secondes (1), les minutes (60), les heures (3600), les jours (86400), les semaines (604800), les mois (2392000) et les années (31536000). Le nombre entre parenthèses est un multiplicateur appliqué à la valeur *n* spécifiée pour exprimer cette valeur en secondes.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
database	database *db type*	Oui	Aucune	Conteneur principal renfermant les définitions des pools d'adresses, options et instructions d'accès client. *db type* est le nom du module chargé pour traiter cette portion du fichier. La seule valeur disponible pour les versions actuelles d'AIX est **db_file**.
logging_info	logging_info	Oui	Aucune	Conteneur de journalisation principal définissant les paramètres de journalisation.
logitem	logitem NONE logitem SYSERR logitem OBJERR logitem PROTOCOL logitem PROTERR logitem WARN logitem WARNING logitem CONFIG logitem EVENT logitem PARSEERR logitem ACTION logitem ACNTING logitem STAT logitem TRACE logitem RTRACE logitem START	Non	Non activé pour tous par défaut.	Active le niveau de journalisation. Plusieurs lignes sont autorisées.
numLogFiles	numLogFiles *n*	Non	0	Indique le nombre de fichiers journaux à créer. Les journaux alternent lorsque le premier journal est rempli. *n* est le nombre de journaux à créer.
logFileSize	logFileSize *n*	Non	0	Indique la taille de chaque fichier journal, exprimée en unités de 1024 octets.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
logFileName	logFileName *path*	Non	Aucune	Indique le chemin d'accès au premier fichier journal. Le nom d'origine du fichier journal est *nomfichier* ou *nomfichier.extension*. *nomfichier* est limité à huit caractères. Lorsque la permutation des fichiers est effectuée, le premier fichier est renommé en conservant le base du nom, *nomfichier*, et en lui ajoutant un numéro, ou en remplaçant l'extension par un numéro. Par exemple, si le nom original du fichier est `file`, le nom du fichier après permutation devient `file01` . Si le nom du fichier d'origine est `file.log` , il devient `file.01` .
CharFlag	charflag yes charflag true charflag false charflag no	Non	true	Non applicable au serveur AIX DHCP, mais utilisé par le serveur DHCP OS/2 pour générer des fenêtres de débogage.
StatisticSnapShot	StatisticSnapShot *n*	Non	–1, jamais	Indique, en secondes, à quelle fréquence les statistiques sont écrites dans le fichier journal.
UsedIpAddress ExpireInterval	UsedIpAddressExpire Interval *n time_units*	Non	–1, jamais	Indique à quelle fréquence les adresses présentant l'état BAD sont recoupées et testées afin de vérifier leur validité.
leaseExpireInterval	leaseExpireInterval *n time_units*	Non	900 secondes	Indique à quelle fréquence les adresses à l'état BOUND sont vérifiées pour voir si elles sont arrivées à expiration. Si l'adresse est arrivée à expiration, l'état devient EXPIRED.
reservedTime	reservedTime *n time_units*	Non	–1, jamais	Indique pendant combien de temps les adresses peuvent rester à l'état RESERVED avant de reprendre l'état FREE.
reservedTime Interval	reservedTimeInterval *n time_units*	Non	900 secondes	Indique à quelle fréquence les adresses à l'état RESERVE sont vérifiées pour voir si elles peuvent reprendre l'état FREE.
saveInterval	saveInterval *n time_units*	Non	3600 secondes	Indique à quelle fréquence le serveur DHCP doit déclencher une sauvegarde des bases de données ouvertes. Pour les serveurs très chargés, cette valeur doit tourner autour de 60 ou 120 secondes.
clientpruneintv	clientpruneintv *n time_units*	Non	3600 secondes	Indique à quelle fréquence le serveur DHCP supprime des bases de données les clients non associés à une adresse (état UNKNOWN). Ceci permet d'économiser la mémoire du serveur DHCP.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
numprocessors	numprocessors *n*	Non	10	Indique le nombre de processeurs de paquets à créer. Le minimum est de un.
userObject	userObject *obj_name*	Oui	Néant	Indique que le serveur doit charger un objet partagé défini par l'utilisateur et appeler des routines au sein de cet objet par le biais de chaque interaction avec les clients DHCP. L'objet à charger est situé dans le répertoire `/usr/sbin` sous le nom de *`obj_name`*`.dhcpo`. Pour plus d'informations, reportez–vous au DHCP Server User–Defined Extension API.

Syntaxe du fichier de serveur DHCP pour la base de données db_file

Remarque : Les unités de temps (*time_units*) indiquées dans le tableau suivant sont facultatives et correspondent à un modificateur du temps réel. L'unité de temps par défaut est exprimée en minutes. Les valeurs autorisées sont les secondes (1), les minutes (60), les heures (3600), les jours (86400), les semaines (604800), les mois (2392000) et les années (31536000). Le nombre entre parenthèses est un multiplicateur appliqué à la valeur *n* spécifiée pour exprimer cette valeur en secondes.

Par ailleurs, les éléments spécifiés dans un conteneur peuvent être remplacés par ceux d'un sous–conteneur. Vous pouvez par exemple définir les clients BOOTP de manière globale, et, au sein d'un sous–réseau particulier, autoriser les clients BOOTP en indiquant le mot–clé supportBootp dans les deux conteneurs.

Les conteneurs client, classe et fournisseur acceptent les expressions régulières. Pour la classe et le vendeur, une chaîne entre guillemets dont le premier caractère à l'intérieur des guillemets est un point d'exclamation (!) indique que le reste de la chaîne doit être considéré comme une expression régulière. Le conteneur client accepte les expressions régulières dans les champs hwtype et hwaddr. Une chaîne unique est utilisée pour représenter les deux champs, selon la syntaxe suivante :

```
nombre_décimal-données
```

Si nombre_décimal est égal à zéro, les données constituent une chaîne ASCII. Pour tout autre nombre, les données sont des chiffres hexadécimaux.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
subnet	subnet *subnet id netmask* subnet *subnet id netmask range* subnet *subnet id netmask label*:*priority* subnet *subnet id netmask range label*:*priority*	Oui	Aucune	Spécifie un sous–réseau et un pool d'adresses. Toutes les adresses sont supposées faire partie du pool, sauf si une plage est spécifiée sur la ligne ou si les adresses sont modifiées ultérieurement dans le conteneur par une instruction de plage ou d'exclusion. La plage facultative est une paire d'adresses IP en format de "dotted quad" séparées par un tiret. Il est possible de préciser un label et une priorité. Ceux–ci sont utilisés dans les sous–réseaux virtuels pour identifier et classer les sous–réseaux du sous–réseau virtuel. Le label et la priorité sont séparés par un signe deux–points. Ces conteneurs ne sont autorisés qu'au niveau global ou au niveau du conteneur base de données.
subnet	subnet *subnet id range*	Oui	Aucune	Spécifie un sous–réseau qui s'inscrit dans un conteneur réseau. Il définit une plage d'adresses formant la totalité du sous–réseau, sauf si la plage facultative est indiquée. Le masque de réseau associé au sous–réseau est issu du conteneur réseau environnant. **Remarque :** Cette méthode est déconseillée au profit des autres formes de sous–réseaux.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
option	option *number data ...* option *number*deny option * deny	Non	Aucune	Spécifie une option à envoyer à un client ou, dans le cas d'un refus (deny), une option qui ne doit pas être envoyée à un client. La clause option * `deny` signifie que toutes les options non spécifiées dans le conteneur en cours ne doivent pas être retournées au client. option *number*deny ne refuse que l'option spécifiée. *number* est un entier 8 bits non signé. *data* est spécifique à l'option (voir ci–dessus) ou peut être définie sous la forme d'une chaîne entre guillemets (texte ASCII) ou 0x*hexdigits* ou hex"*hexdigits*" ou encore hex "*hexdigits*". Si l'option correspond à un conteneur fournisseur, elle sera encapsulée avec les autres options dans une option 43.
exclude	exclude *an IP address* exclude *dotted_quad–dotted_quad*	Non	Aucune	Modifie la plage sur le conteneur qui comporte l'instruction exclude. L'instruction exclude n'est pas valide au niveau des conteneurs de base de données ou au niveau général. L'instruction exclude supprime l'adresse ou la plage spécifiée de la plage actuelle sur le conteneur. Elle permet de créer des plages non contiguës pour sous sous–réseaux ou d'autres conteneurs.
range	range *IP_address* range *dotted_quad–dotted_quad*	Non	Aucune	Modifie la plage sur le conteneur qui comporte l'instruction range. L'instruction range n'est pas valide au niveau des conteneurs de base de données ou au niveau général. S'il s'agit de la première plage du conteneur qui ne spécifie pas une plage sur la ligne de définition du conteneur, la plage du conteneur devient alors la plage spécifiée par l'instruction range. Toute instruction range suivante, ou toutes les instructions range dans le cas d'un conteneur spécifiant des plages dans sa définition sont ajoutées à la page actuelle. Avec l'instruction range, il est possible d'ajouter à la plage existante une adresse unique ou un jeu d'adresses. La plage doit être incorporée dans la définition du conteneur de sous–réseau.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
client	client *hwtype hwaddr* NONE client *hwtype hwaddr* ANY client *hwtype hwaddr dotted_quad* client *hwtype hwaddr range*	Oui	Aucune	Spécifie un conteneur client qui empêche le client indiqué par *hwaddr* et *hwtype* d'obtenir une adresse. Si *hwtype* est 0, alors *hwaddr* est une chaîne ASCII. Sinon, *hwtype* correspond au type de matériel du client et *hwaddr* à l'adresse du matériel du client. Si *hwaddr* est une chaîne, des guillemets peuvent encadrer la chaîne. Si *hwaddr* est une chaîne hexadécimale, l'adresse peut être spécifiée sous la forme 0x*hexdigits* ou hex *digits*. *range* permet au client spécifié par *hwaddr* et *hwtype* d'obtenir une adresse faisant partie de cette *plage*. Pour faire référence à plusieurs clients, il faut utiliser une expression régulière.
class	class *string* class *string range*	Oui	Aucune	Spécifie un conteneur classe portant le nom *string*. La chaîne peut ou non être placée entre guillemets. Si oui, les guillemets sont supprimés avant la comparaison. Les guillemets sont obligatoires si la chaîne contient des espaces ou des tabulations. Ce conteneur est autorisé à tous les niveaux. Il est possible d'indiquer une plage pour spécifier le jeu d'adresses à proposer au client avec cette classe. La plage est soit une adresse IP en format de ”dotted quad”, soit deux adresses IP en format de ”dotted quad” séparées par un tiret.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
network	network *network id netmask* network *network id* network *network id netmask*	Oui	Aucune	Spécifie un ID de réseau à l'aide des informations de classe (par exemple 9.3.149.0 avec un masque de réseau de 255.255.255.0 correspond au réseau 9.0.0.0 255.255.255.0). Cette version du conteneur de réseau est utilisée pour englober les sous–réseaux partageant le même masque et le même ID de réseau. Lorsqu'une plage est fournie, toutes les adresses de la plage font partie du pool. La plage doit être comprise dans le réseau de l'ID de réseau. Elle fait appel à l'adresse intégrale de la classe. Elle n'est valide qu'au niveau général ou au niveau du conteneur de base de données. **Remarque :** le mot–clé network est déconseillé au profit du conteneur de sous–réseau.
vendor	vendor *vendor_id* vendor *vendor_id* hex"" vendor *vendor_id* hex "" vendor *vendor_id* 0xdata vendor *vendor_id* "" vendor *vendor_id range* vendor *vendor_id range* hex"" vendor *vendor_id range* hex "" vendor *vendor_id range* 0xdata vendor *vendor_id range* ""	Oui	Aucune	Spécifie un conteneur de fournisseur. Les conteneurs fournisseur sont utilisés pour retourner l'option 43 au client. L'id de fournisseur peut être spécifié sous la forme d'une chaîne entre guillemets ou d'un chaîne binaire du type 0x*hexdigits* ou hex"*digits*". Il est possible d'ajouter à l'id de fournisseur une plage facultative, en utilisant deux "dotted quad" séparés par un tiret. A la suite de la plage facultative, une chaîne hexadécimale également facultative peut être indiquée comme première partie de l'option 43. Si les options figurent dans le conteneur, elles sont annexées aux données de l'option 43. Une fois toutes les options traitées, une option End Of Option List (fin de la liste d'options) est ajoutée aux données. Pour retourner les options en dehors d'une option 43, utilisez une expression régulière correspondant à tous les clients pour spécifier les options normales à renvoyer en fonction de l'ID fournisseur.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
inoption	inoption *number option_data* inoption *number option_data range*	Oui	Néant	Indique un conteneur à rapprocher d'une option entrante arbitraire définie par le client. *number* indique le numéro de l'option. *option_data* définit la clé correspondant au conteneur à sélectionner lors du choix de l'adresse et de l'option pour ce client. La clé *option_data* se présente sous forme de chaîne entre guillemets, d'adresse IP ou de nombre entier pour les options connues mais peut également se présenter sous forme de chaîne hexadécimale d'octets si elle est précédée des caractères `0x`. Pour les options que le serveur connaît mal, il est possible de définir une chaîne hexadécimale d'octets sur le même schéma. En outre, la valeur *option_data* peut faire référence à une expression régulière à rapprocher de la représentation en chaîne des données d'option du client. Ces expressions régulières se présentent sous la forme d'une chaîne entre guillemets dont le premier caractère est un point d'exclamation `"!`. Les options peu connues du serveur se présentent sous forme de chaîne hexadécimale d'octets NON précédée des caractères `0x`.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
virtual	virtual fill *id id* ...	Non	Aucune	Spécifie un sous–réseau virtuel avec une politique. `fill` signifie utiliser toutes les adresses de ce conteneur avant de passer au suivant. `rotate` signifie sélectionner une adresse du pool suivant de la liste sur chaque requête. `sfill` et `srotate` sont identiques à `fill` et `rotate`, mais une recherche est effectuée pour savoir si le client correspond aux conteneurs, aux fournisseurs ou aux classes du sous–réseau. Si une correspondance permet d'obtenir une adresse, cette adresse est adoptée à partir du conteneur au lieu de suivre la politique indiquée. Il peut y avoir autant d'ID que nécessaire. *id* est soit l'ID de sous–réseau de la définition de sous–réseau, soit le label de cette même définition. Le label est nécessaire si plusieurs sous–réseaux partagent le même ID de sous–réseau.
	virtual sfill *id id* ...			
	virtual rotate *id id* ...			
	virtual srotate *id id* ...			
inorder:	inorder: *id id* ...	Non	Aucune	Spécifie un sous–réseau virtuel avec une politique de remplissage, ce qui signifie utiliser toutes les adresses de ce conteneur avant de passer au conteneur suivant. Il peut y avoir autant d'ID que nécessaire. *id* est soit l'ID de sous–réseau de la définition de sous–réseau, soit le label de cette même définition. Le label est nécessaire si plusieurs sous–réseaux partagent le même ID de sous–réseau.
balance:	balance: *id id* ...	Non	Aucune	Spécifie un sous–réseau virtuel avec une politique de rotation, ce qui signifie utiliser l'adresse suivante du conteneur suivant. Il peut y avoir autant d'ID que nécessaire. *id* est soit l'ID de sous–réseau de la définition de sous–réseau, soit le label de cette même définition. Le label est nécessaire si plusieurs sous–réseaux partagent le même ID de sous–réseau.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
supportBootp	supportBootp true supportBootp 1 supportBootp yes supportBootp false supportBootp 0 supportBootp no	Non	Oui	Indique si le conteneur en cours et tous ceux qui en découlent (jusqu'à mention contraire) doivent accepter les clients BOOTP.
supportUnlisted clients	supportUnlistedclients BOTH supportUnlistedclients DHCP supportUnlistedclients BOOTP supportUnlistedclients NONE supportUnlistedclients true supportUnlistedclients yes supportUnlistedclients 1 supportUnlistedclients false supportUnlistedclients no supportUnlistedclients 0	Non	Both	Indique si le conteneur en cours et tous ceux qui en découlent (jusqu'à mention contraire) doivent accepter les clients non répertoriés. La valeur indique si tous les clients bénéficient d'un accès sans instructions client particulières, si seuls les clients DHCP ont un accès, si seuls les clients BOOTP sont autorisés ou aucun des deux. **Remarque :** Les valeurs true et false ont été conservées par souci de compatibilité avec les versions antérieures mais sont déconseillées. La valeur true est équivalente à BOTH et la valeur false à NONE.
addressrecorddb	addressrecrddb *path*	Non	Aucune	Lorsqu'elle est spécifiée, cette option fonctionne comme le mot–clé **backupfile**. Elle n'est valide qu'au niveau général ou au niveau du conteneur de base de données. **Remarque :** Cette méthode est déconseillée.
backupfile	backupfile *path*	Non	/etc/db_file.crbk	Indique le fichier à utiliser pour les sauvegardes de la base de données. Elle n'est valide qu'au niveau général ou au niveau du conteneur de base de données.
checkpointfile	checkpointfile *path*	Non	/etc/db_file.crbk	Indique le fichier de points de contrôle de la base de données. Le premier fichier de points de contrôle correspond à *path*. Le second est *path*, avec le dernier caractère remplacé par un 2. Le nom du fichier de contrôle ne doit donc pas se terminer à l'origine par un 2. Cette option n'est valable qu'au niveau général ou au niveau du conteneur de base de données.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
clientrecorddb	clientrecorddb *path*	Non	/etc/db_file.crbk	Indique le fichier de sauvegarde de la base de données. Le fichier contient tous les enregistrements client que le serveur DHCP a traités. L'option n'est valide qu'au niveau général ou au niveau du conteneur de base de données.
bootstrapserver	bootstrapserver *IP address*	Non	Aucune	Indique le serveur que les clients doivent utiliser comme point de départ vers les fichiers TFTP à l'issue de la réception de paquets BOOTP ou DHCP. Cette valeur complète le champ **siaddr** du paquet. Elle est valide à tous les niveaux de conteneur.
giaddrfield	giaddrfield *IP address*	Non	Aucune	Définit le champ giaddrfield pour les paquets de réponse. **Remarque :** Cette spécification n'est pas autorisée pour les protocoles BOOTP et DHCP, mais certains clients exigent le champ **giaddr** comme passerelle par défaut pour le réseau. En raison de ce risque de conflit, il est conseillé de n'utiliser giaddrfield qu'au sein d'un conteneur client, bien que l'option fonctionne à tous les niveaux.
pingTime	pingTime *n time_unit*	Non	3 secondes	Indique la durée pendant laquelle la réponse ping doit être attendue avant qu'une adresse ne soit suspendue. L'unité de temps par défaut est de l'ordre des centièmes de seconde. La valeur de l'unité de temps est définie dans la remarque qui précède ce tableau. Elle est valide à tous les niveaux de conteneur. Le paramètre *time_unit* est facultatif.
bootptime	bootptime *n time_unit*	Non	–1, illimité	Indique la durée pendant laquelle louer une adresse à un client BOOTP. La valeur par défaut est –1, ce qui signifie durée illimitée. Les valeurs classiques d'unités de temps sont acceptées. Le paramètre *time unit* est facultatif. Cette option est valide à tous les niveaux de conteneur.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
AllRoutesBroadcast	allroutesbroadcast no allroutesbroadcast false allroutesbroadcast 0 allroutesbroadcast yes allroutesbroadcast true allroutesbroadcast 1	Non	0	Si un réponse de diffusion est requise, indique si cette réponse doit être diffusée sur toutes les routes. Cette option est valide à tous les niveaux de conteneur. Elle est ignorée par les serveurs DHCP AIX car l'adresse MAC réelle du client, y compris les RIF, est stockée pour le paquet en retour. Cette option est valide à tous les niveaux de conteneur.
addressassigned	addressassigned "*string*"	Non	Aucune	Indique une chaîne entre guillemets à exécuter lorsqu'une adresse est attribuée à un client. La chaîne doit comporter deux %s. Le premier %s correspond à l'ID client, sous la forme *type–string*. Le second %s est une adresse IP en format de "dotted quad". Cette option est valide à tous les niveaux de conteneur.
addressreleased	addressreleased "*string*"	Non	Aucune	Indique une chaîne entre guillemets à exécuter lorsqu'une adresse est libérée par un client. La chaîne ne doit comporter qu'un %s, correspondant à l'adresse IP libérée en format de "dotted quad". Cette option est valide à tous les niveaux de conteneur.
appenddomain	appenddomain 0 appenddomain no appenddomain false appenddomain 1 appenddomain yes appenddomain true	Non	Non	Indique s'il convient d'ajouter le nom de domaine défini par l'option 15 au nom d'hôte suggéré par le client lorsque ce dernier ne propose pas de nom de domaine. Cette option est valide à tous les niveaux de conteneur.
canonical	canonical 0 canonical no canonical false canonical 1 canonical yes canonical true	Non	0	Indique que l'ID du client est en format canonique. Cette option n'est valide qu'au niveau du conteneur client.
leaseTimeDefault	leaseTimeDefault *n time_unit*	Non	86400 secondes	Indique la durée du bail par défaut pour les clients. Cette option est valide à tous les niveaux de conteneur. Le paramètre *time_unit* est facultatif.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
proxyarec	proxyarec never proxyarec usedhcpddns proxyarec usedhcpddnsplus proxyarec always proxyarec usedhcpddnsprotected proxyarec usedhcpddnsplusprotected proxyarec alwaysprotected proxyarec standard proxyarec protected	Non	usedhcpddnsplus	Indique les options et méthodes qui doivent être utilisées pour la mise à jour des enregistrements A dans DNS. `never` signifie que l'enregistrement A ne doit jamais être actualisé. `usedhcpddns` signifie utiliser l'option 81 si le client l'a définie. `usedhcpddnsplus` signifie utiliser l'option 81, ou l'option 12 et 15, si spécifié. `always` signifie que l'enregistrement A doit être actualisé pour tous les clients. `XXXXprotected` modifie la commande **nsupdate** pour s'assurer que le client est autorisé. `standard` est synonyme de `always` . `protected` est synonyme de `alwaysprotected` . Cette option est valide à tous les niveaux de conteneur.
releasednsA	releasednsA "*string*"	Non	Aucune	Indique la chaîne d'exécution à utiliser lors de la libération d'une adresse. La chaîne est utilisée pour supprimer l'enregistrement A associé à l'adresse libérée. Cette option est valide à tous les niveaux de conteneur.
releasednsP	releasednsP "*string*"	Non	Aucune	Indique la chaîne d'exécution à utiliser lors de la libération d'une adresse. La chaîne est utilisée pour supprimer l'enregistrement PTR associé à l'adresse libérée. Cette option est valide à tous les niveaux de conteneur.
removedns	removedns "*string*"	Non	Aucune	Indique la chaîne d'exécution à utiliser lors de la libération d'une adresse. La chaîne est utilisée pour supprimer les enregistrements A et PTR associés à l'adresse libérée. Cette option est valide à tous les niveaux de conteneur. **Remarque :** Cette option est déconseillée au profit des mots–clés **releasednsA** et **releasednsP**.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
updatedns	updatedns "*string*"	Non	Aucune	Indique la chaîne d'exécution à utiliser lors de la liaison d'une adresse. La chaîne est utilisée pour mettre à jour les enregistrements A et PTR associés à l'adresse. Cette option est valide à tous les niveaux de conteneur. **Remarque :** Cette option est déconseillée au profit des mots–clés **updatednsA** et **updatednsP**.
updatednsA	updatednsA "*string*"	Non	Aucune	Indique la chaîne d'exécution à utiliser lors de la liaison d'une adresse. La chaîne est utilisée pour mettre à jour l'enregistrement A associé à l'adresse. Cette option est valide à tous les niveaux de conteneur.
updatednsP	updatednsP "*string*"	Non	Aucune	Indique la chaîne d'exécution à utiliser lors de la liaison d'une adresse. La chaîne est utilisée pour mettre à jour l'enregistrement PTR associé à l'adresse. Cette option est valide à tous les niveaux de conteneur.
hostnamepolicy	hostnamepolicy suggested hostnamepolicy resolved hostnamepolicy always_resolved hostnamepolicy defined hostnamepolicy always_defined hostnamepolicy default	Non	default	Spécifie le nom d'hôte à retourner au client. La politique par défaut préfère le nom d'hôte et le nom de domaine explicitement définis par rapport aux noms suggérés. Les autres politiques respectent strictement les consignes (par exemple : `defined` retourne le nom défini ou rien si aucun nom n'est défini dans la configuration). En outre, les politiques utilisant le modificateur `always` demandent au serveur de toujours retourner l'option nom d'hôte même si le client ne l'a pas demandé au moyen de l'option liste des paramètres. A noter que suggérer un nom d'hôte implique également de le demander, et que les noms d'hôte peuvent être suggérés à l'aide de l'option 81 ou des options 12 et 15. Ce mot–clé est valide à tous les niveaux de conteneur.

Mot–clé	Forme	Sous–conteneurs ?	Valeur par défaut	Signification
bootfilepolicy	bootfilepolicy suggested bootfilepolicy merge bootfilepolicy defined bootfilepolicy always	Non	suggested	Définit une préférence pour retourner le nom du fichier de démarrage à un client. `suggested` préfère le nom du fichier de démarrage suggéré par le client à n'importe quel autre nom configuré par le serveur. `merge` ajoute le nom suggéré par le client au répertoire personnel configuré par le serveur. `defined` préfère le nom défini à n'importe quel autre nom suggéré. `always` retourne le nom défini même si le client ne l'a pas demandé à l'aide de l'option liste des paramètres.
stealfromchildren	stealfromchildren true stealfromchildren 1 stealfromchildren yes stealfromchildren false stealfromchildren 0 stealfromchildren no	Non	Non	Indique si le conteneur parent est autorisé à "voler" des adresses dans ses conteneurs enfants lorsqu'il est à court d'adresses. Cela signifie que si vous avez un sous–réseau avec une classe définie à l'aide d'une plage d'adresses, ces adresses sont réservées aux clients qui mentionnent cette classe. Si `stealfromchildren` a la valeur true, les adresses seront récupérées chez un enfant afin de tenter de satisfaire la requête. La valeur par défaut n'autorise pas les vols d'adresses.
homedirectory	homedirectory *path*	Non	Aucune	Indique le répertoire personnel à utiliser dans la section fichier du paquet de réponse. Cette option peut être définie à tous les niveaux de conteneur. La politique bootfile définit comment les éléments spécifiés dans la section fichier du paquet entrant se conjuguent avec les instructions du fichier de démarrage et du répertoire personnel.
bootfile	bootfile *path*	Non	Aucune	Indique le fichier de démarrage à utiliser dans la section fichier du paquet de réponse. Cette option peut être définie à tous les niveaux de conteneur. La politique bootfile définit comment les éléments spécifiés dans la section fichier du paquet entrant se conjuguent avec les instructions du fichier de démarrage et du répertoire personnel.

DHCP et gestion NIM (Network Installation Management)

Le concept d'affectation dynamique d'adresses IP est relativement nouveau. Voici quelques suggestions relatives à l'interaction entre DHCP et NIM.

1. Lorsque vous configurez des objets dans l'environnement NIM, utilisez des noms d'hôte chaque fois que possible : vous pouvez ainsi exploiter un serveur de noms dynamique qui met à jour les adresses IP lorsque le nom d'hôte est converti en adresse IP dans l'environnement NIM.
2. Placez le maître NIM et le serveur DHCP sur le même système. Le serveur DHCP est doté, dans la chaîne DNS de mise à jour, d'une option qui, affectée de la valeur `NIM`, tente de conserver les objets NIM hors des états qui requièrent des adresses IP statiques quand ces adresses changent.
3. Pour les clients NIM, vous devez définir un délai dédié double du temps requis pour installer un client. Cela permet à une adresse IP dédiée de rester valide pendant l'installation. Celle-ci terminée, le client réamorce et DHCP est lancé ou doit être configuré, selon le type de l'installation.
4. Le serveur `dhcpsd` doit être responsable des enregistrements système noms de domaine PTR et "A". Lorsque NIM réinstalle la machine, le fichier contenant le RSA est supprimé et le client ne peut mettre ses enregistrements à jour. C'est pourquoi le serveur doit mettre à jour les enregistrements système. Pour ce faire, modifiez la ligne `updatedns` du fichier /**etc**/**dhcpcd.ini** en :

   ```
   updatedns "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' NONE NONIM"
   ```

   Dans le fichier /**etc**/**dhcpsd.cnf**, changez la ligne `updatedns` en :

   ```
   updatedns "/usr/sbin/dhcpaction '%s' '%s' '%s' '%s' BOTH NIM"
   ```

Remarque : Lorsqu'un objet NIM est placé en état d'attente de l'installation BOS, le serveur `dhcpsd` peut passer des arguments différents de ceux prévus à l'origine. Pour éviter cette situation, réduisez au minimum le délai pendant lequel le client se trouve en état d'attente.

Suivez ces suggestions : les clients dynamiques pourront exploiter l'environnement NIM.

Pour en savoir plus sur l'environnement NIM, reportez-vous au manuel *AIX NIM - Guide de référence*.

Configuration de TCP/IP

Si vous avez installé les logiciels TCP/IP (Transmission Control Protocol/Internet Protocol) et NFS (Network File System), vous pouvez configurer votre système afin de communiquer via un réseau.

Une fois les logiciels TCP/IP et NFS installés, utilisez le raccourci Web-based System Manager, **wsm networks**, ou SMIT, **smit tcpip**, pour configurer le système. L'aide en ligne vous guidera tout au long du processus.

Prérequis

Le logiciel TCP/IP doit être installé. Si vous devez installer TCP/IP, vous devrez installer le logiciel en option TCP/IP Optional Support.

Vous devez disposer des droits d'utilisateur racine pour configurer TCP/IP.

Mise à jour de la liste des hôtes

Un *serveur de noms* est une machine du réseau qui recense les noms et adresses de toutes les machines du réseau. Ces noms sont enregistrés dans la liste des hôtes. Lorsqu'une machine souhaite communiquer avec une autre, elle envoie le nom de cette machine au serveur de noms. Le serveur de noms se réfère à la liste des hôtes et répond en renvoyant l'adresse de la machine demandée. Un serveur de noms offre l'avantage d'une gestion centralisée de la liste des hôtes, qui est accessible depuis n'importe quelle machine du réseau. Ceci se traduit par un gain de temps et d'espace de stockage.

- Si vous faites appel à un serveur de noms pour vos communications réseau, vous n'avez pas à exécuter cette procédure. TCP/IP est déjà configuré.
- Si vous n'utilisez *pas* de serveur de noms pour les communications réseau, vous devez mettre à jour la liste des hôtes afin d'y inclure les noms de tous les systèmes du réseau. A condition de disposer des droits d'utilisateur racine, utilisez le raccourci Web-based System Manager **wsm network** ou le raccourci SMIT **smit hostent**.

Démons TCP/IP

Les démons (ou *serveurs*) sont des process qui fonctionnent en continu, en arrière-plan, pour exécuter des fonctions requises par d'autres process. TCP/IP fournit des démons pour implémenter certaines fonctions sur le système. Leur exécution en arrière-plan n'interrompt pas les autres processus (à moins qu'ils en soient chargés).

Les démons sont appelés par des commandes au niveau de la gestion système, par d'autres démons ou scripts shell. Vous pouvez également les contrôler à l'aide du démon **inetd**, du script shell **rc.tcpip** et du contrôleur SRC (System Resource Controller).

Sous-systèmes et sous-serveurs

Un *sous-système* est un démon ou serveur contrôlé par SRC. Un *sous-serveur* est un démon contrôlé par un sous-système. (Les commandes et noms de démon sont généralement suffixés par un **d**.) Sous–système et sous–serveur sont deux catégories opposées et incompatibles : un démon ne peut relever des deux catégories à la fois. Le seul sous-système TCP/IP qui contrôle d'autres démons est **inetd**. Ainsi, tout sous-serveur TCP/IP est également un sous-serveur **inetd**.

Les démons TCP/IP contrôlés par SRC sont :

Sous-systèmes

gated	Fournit des fonctions de routage de passerelle et prend en charge les protocoles RIP (Routing Information Protocol), RIPng (Routing Information Protocol Next Generation), EGP (Exterior Gateway Protocol), BGP (Border Gateway Protocol) et BGP4+, HELLO, OSPF (Open Shortest Path First), IS–IS (Intermediate System to Intermediate System), ICMP et ICMPv6 (Internet Control Message Protocol /Router Discovery). En outre, **gated** prend également le protocole SNMP (Simple Network Monitoring Protocol) en charge. Le démon **gated** est l'un des deux démons de routage dédiés aux adresses de réseau. Le démon **gated** est préféré au démon **routed** car il admet davantage de protocoles de passerelle.
inetd	Appelle et planifie l'exécution d'autres démons à la réception des demandes de services de démons. Ce démon peut également en lancer d'autres. **inetd** est aussi appelé "super démon".
iptrace	Suivi des paquets au niveau interface pour les protocoles Internet.
named	Fournit la fonction d'appellation au protocole de serveur de noms DOMAIN.
routed	Gère les tables de routage de réseau et prend en charge le protocole RIP (Routing Information Protocol). Le démon **gated** est préféré au démon **routed** car il admet davantage de protocoles de passerelle.
rwhod	Diffuse des messages à l'ensemble des hôtes, toutes les trois minutes, et stocke l'information relative aux utilisateurs connectés et à l'état du réseau. Utilisez **rwhod** avec précaution car il monopolise une part importante des ressources machine.
timed	Fournit la fonction serveur horaire.

Remarque : Les démons **routed** et **gated** relèvent de la catégorie des sous-systèmes TCP/IP. N'exécutez pas la commande **startsrc –g tcpip**, qui lance ces deux démons de routage avec tous les autres sous-systèmes TCP/IP. Ces deux démons lancés ensemble produiraient des résultats imprévisibles.

Les démons TCP/IP contrôlés par le sous-système **inetd** sont :

Sous-serveurs inetd

comsat	Avertit les utilisateurs de l'arrivée d'un courrier.
fingerd	Dresse un compte rendu concernant l'état de tous les utilisateurs connectés et l'état du réseau sur l'hôte distant spécifié. Ce démon utilise le protocole FINGER.
ftpd	Assure le transfert des fichiers pour un processus client en appliquant le protocole FTP (File Transfer Protocol).
rexecd	Assure la fonction de serveur hôte étranger, pour la commande **rexec**.
rlogind	Effectue la connexion à distance pour la commande **rlogin**.
rshd	Effectue la fonction serveur d'exécution des commandes à distance pour les commandes **rcp** et **rsh**.
talkd	Apport de la fonction conversation à la commande **talk.**
syslogd	Lecture et consignation des messages système. Ce démon appartient au groupe de sous-systèmes RAS.
telnetd	Apport de la fonction serveur au protocole TELNET.
tftpd	Assure la fonction serveur pour le protocole TFTP (Trivial File Transfer Protocol).
uucpd	Gère les communications entre BNU et TCP/IP.

Fonction SRC

Le contrôleur de ressources système (SRC) permet, entre autres, de lancer les démons, les arrêter et suivre leurs activités. De plus, SRC permet de grouper des démons en sous-systèmes et sous-serveurs.

Cet outil a été conçu pour aider l'administrateur système à contrôler les démons. Ce contrôle s'effectue au-delà des indicateurs et paramètres disponibles pour chaque commande de démon.

Pour en savoir plus sur SRC, reportez-vous à la section Contrôleur SRC dans *AIX 4.3 System management Concepts: Guide d'administration : système d'exploitation et unités*.

Commandes SRC

Les commandes SRC sont applicables à un seul démon, à un groupe de démons ou à un démon et à ceux qu'il contrôle (sous-système avec sous-serveurs). Par ailleurs, certains démons TCP/IP ne répondent pas à toutes les commandes SRC. Voici la liste des commandes SRC disponibles pour contrôler des démons TCP/IP et leurs exceptions.

startsrc	Démarre tous les sous-systèmes TCP/IP et sous-serveurs **inetd**, sans exception. La commande **startsrc** fonctionne pour tous les sous-systèmes TCP/IP et sous-serveurs **inetd**.
stopsrc	Arrête tous les sous-systèmes TCP/IP et sous-serveurs **inetd**, sans exception. Cette commande s'appelle également **stop normal**. La commande **stop normal** permet aux sous-systèmes de traiter tout le travail en cours et d'y mettre fin en douceur. Pour les sous–serveurs **inetd**, toutes les connexions en attente sont lancées et celles en exécution, terminées. La commande **stop normal** fonctionne pour tous les sous-systèmes TCP/IP et sous-serveurs **inetd**.

stopsrc –f Arrête tous les sous-systèmes TCP/IP et sous-serveurs **inetd**, sans exception. Cette commande s'appelle également **stop force**. **stop force** arrête immédiatement tous les sous-systèmes. Pour les sous-serveurs **inetd**, toutes les connexions en cours ou en attente sont immédiatement terminées.

refresh Rafraîchit les sous-systèmes et sous-serveurs suivants : sous-systèmes **inetd**, **syslogd**, **named**, **dhcpsd** et **gated**.

lssrc Fournit un bref compte rendu de l'état du sous–système spécifié (actif ou non) et des sous–serveurs **inetd** (avec dans ce cas, le nom, l'état et la description du sous–serveur, le nom de la commande et les arguments qui ont permis de le lancer.

lssrc –l Fournit un bref compte rendu d'état accompagné d'informations supplémentaires (état détaillé) sur les sous-systèmes :

- **gated** Etat de la mise au point ou du suivi, protocoles de routage activés, tables de routage, signaux acceptés avec leur fonction.
- **inetd** Etat de la mise au point, liste des sous-serveurs actifs avec état succinct, signaux acceptés avec leurs fonctions.
- **named** Etat de la mise au point, informations sur le fichier **named.conf**.
- **dhcpsd** Etat de la mise au point, toutes les adresses IP contrôlées et leur état actuel.
- **routed** Etat de la mise au point et du suivi, état des informations de routage source, tables de routage.
- **syslogd** Données de configuration de **syslogd**.

La commande **lssrc –l** indique également l'état détaillé des sous-serveurs **inetd** : informations sur l'état et les connexions actives. Certains sous–serveurs fournissent des informations supplémentaires. Il s'agit de :

- **ftpd** Etat de la mise au point et de la journalisation.
- **telnetd** Type d'émulation de terminal.
- **rlogind** Etat de la mise au point.
- **fingerd** Etat de la mise au point et de la journalisation.

Les sous-serveurs **rwhod** et **timed** ne fournissent pas d'état détaillé.

traceson Active la mise au point au niveau socket. Utilisez la commande **trpt** pour mettre la sortie en forme. Cette commande n'est pas prise en charge par les sous-systèmes **timed** et **iptraced**.

tracesoff Désactive la mise au point au niveau socket. Utilisez la commande **trpt** pour mettre la sortie en forme. Cette commande n'est pas prise en charge par les sous-systèmes **timed** et **iptraced**.

Pour des exemples d'utilisation, reportez-vous à la description de la commande qui vous intéresse. Pour en savoir plus sur SRC, reportez-vous à la section Contrôleur SRC dans *AIX 4.3 System management Concepts: Guide d'administration : système d'exploitation et unités*.

Configuration du démon inetd

Pour configurer le démon **inetd** :

1. Définissez les sous-serveurs que le démon doit appeler en ajoutant un sous-serveur **inetd**.
2. Définissez ses caractéristiques de relance, en modifiant les caractéristiques de relance du démon **inetd**.

Configuration des tâches du démon inetd		
Raccourci Web-based System Manager, **wsm network** (application wsm network) OU		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Démarrage du démon **inetd**	**smit mkinetd**	**startsrc –s inetd**
Modification des caractéristiques de relance du démon **inetd**	**smit chinetd** ou **smit lsinetd**	
Arrêt du démon **inetd**	**smit rminetd**	**stopsrc –s inetd**
Liste des sous–serveurs **inetd**	**smit inetdconf**	
Ajout d'un sous-serveur **inetd**[1]	**smit mkinetdconf**	éditez /**etc**/**inetd.conf** puis lancez **refresh –s inetd** ou **kill –1** *inetdPID*[2]
Modification/Affichage des caractéristiques d'un sous–serveur **inetd**	**smit inetdconf**	éditez /**etc**/**inetd.conf** puis lancez **refresh –s inetd** ou **kill –1** *inetdPID*[2]
Suppression d'un sous-serveur **inetd**	**smit rminetd**	éditez /**etc**/**inetd.conf** puis lancez **refresh –s inetd** ou **kill –1** *inetdPID*[2]

Remarques :

1. Ajouter un sous-serveur **inetd** revient à configurer le démon **inetd** pour qu'il puisse appeler le sous-serveur lorsque nécessaire.
2. La commande **refresh** ou **kill** signale au démon **inetd** les modifications apportées à son fichier de configuration.

Services réseau client

Les services réseau client (accessibles via le raccourci Web-based System Manager **wsm network** ou via le raccourci **smit clientnet**) sont les protocoles TCP/IP applicables sous AIX. Chaque protocole ou service est identifié par le numéro de port qu'il utilise sur le réseau, d'où l'expression **port connu**. Par commodité, ces numéros de port peuvent être associés à des noms ou numéros. Par exemple, le protocole de messagerie TCP/IP qui utilise le port 25 est connu sous le nom **smtp**. Si un protocole est déclaré (pas de marque de commentaire) dans le fichier /**etc**/**services**, il peut être utilisé par un hôte.

Par défaut, tous les protocoles TCP/IP sont définis dans ce fichier /**etc**/**services**. Vous n'avez donc pas besoin de configurer ce fichier. Cependant, si vous avez écrit vos propres programmes client/serveur, vous pouvez être amené à les déclarer dans le fichier /**etc**/**services** et à leur réserver un nom et un numéro de port. Si vous décidez d'ajouter un service à /**etc**/**services**, notez que les ports 0 à 1024 sont réservés au système.

Tâches des services réseau client		
Raccourci Web-based System Manager, **wsm network** (application wsm network) OU		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Liste des services disponibles	**smit lsservices**	Affichez /**etc**/**services**
Ajout d'un service	**smit mkservices**	Editez /**etc**/**services**
Modification/affichage des caractéristiques d'un service	**smit chservices**	Editez /**etc**/**services**
Suppression d'un service	**smit rmservices**	Editez /**etc**/**services**

Services réseau serveur

Les services réseau serveur se composent du contrôle de l'accès distant, du démarrage ou de l'arrêt de TCP/IP, et de la gestion du pilote d'unité **pty**, comme indiqué dans le tableau suivant.

Le pilote d'unité **pty** est installé automatiquement avec le système. Par défaut, ce pilote, configuré pour des liaisons symboliques 16 BSD, est disponible dès l'amorçage.

Tâches des services réseau serveur		
Raccourci Web-based System Manager, **wsm network** (application wsm network) OU		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Contrôle d'accès à distance	Reportez–vous à "Exécution de commandes à distance (/etc/host.equiv)", page 3-156 et à "Restrictions d'accès FTP (/etc/ftpusers)", page 3-156.	
Démarrage, redémarrage ou arrêt des sous-systèmes TCP/IP	**smit otherserv**	Reportez-vous à Fonction SRC, page 3-99
Modification/affichage des caractéristiques du pilote d'unité pty	**smit chgpty**	**chdev –l pty0 –P –a num=***X* *X* étant une valeur comprise entre 0 et 64
Désactivation du pilote d'unité pty	**smit pty** puis sélectionnez **Retrait du PTY ; conserver définition**	
Activation du pilote d'unité pty	**smit pty** puis sélectionnez **Configuration du PTY défini**	
Génération d'un compte rendu d'erreur	**smit errpt**	
Suivi de pty	**smit trace**	

Résolution de noms sous TCP/IP

Bien que les adresses Internet 32–bits fournissent un moyen efficace d'identifier la source et la destination des datagrammes à travers un interréseau, les utilisateurs préfèrent utiliser des noms représentatifs et faciles à mémoriser. TCP/IP propose un système d'attribution de noms applicable à des réseaux hiérarchiques ou plats.

Cette section traite des points suivants :

Système d'appellation

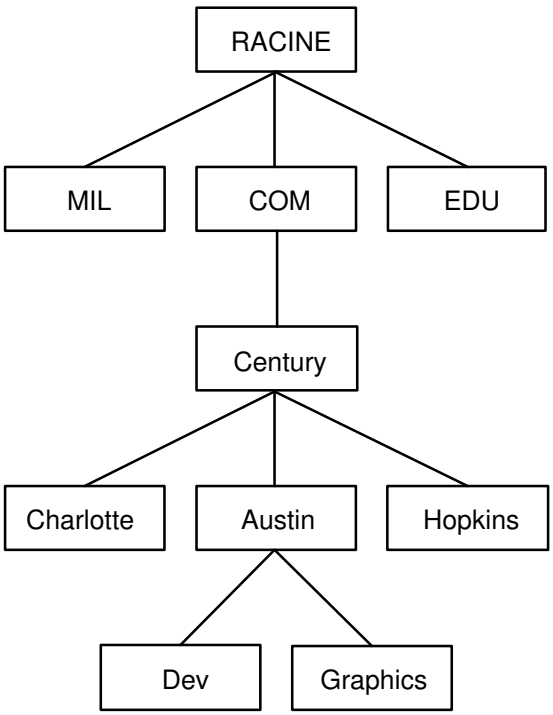
Le système d'appellation des réseaux plats est très simple : les noms attribués aux hôtes sont formés par une chaîne unique de caractères et gérés le plus souvent localement. Chaque machine du réseau plat dispose d'un fichier **/etc/hosts** qui contient, pour chaque hôte du système, l'équivalence entre le nom et l'adresse Internet. Ce fichier s'étoffe avec l'extension du réseau et sa mise à jour représente une tâche de plus en plus lourde. Lorsque des réseaux prennent une grande envergure comme dans le cas d'Internet, leurs systèmes d'appellation sont hiérarchisés. Ces divisions reflètent généralement l'organisation des réseaux. En TCP/IP, le système d'appellation est connu sous le nom de DNS (*domain name system*) et utilise le protocole DOMAIN. Ce protocole DOMAIN est lancé par le démon **named** dans TCP/IP.

Le système d'appellation hiérarchique DNS, comme pour les réseaux plats, attribue aux réseaux et aux hôtes des noms symboliques à la fois représentatifs et faciles à mémoriser. Mais au lieu de tenir un fichier d'équivalence sur chaque machine du réseau, il désigne un ou plusieurs hôtes pour jouer le rôle de *serveurs de noms.* Ces serveurs sont chargés de traduire (résoudre) les noms symboliques des réseaux et des hôtes en adresses Internet interprétables par les machines. Chaque serveur dispose des informations complètes sur la *zone* du domaine dont il a la charge.

Autorité d'appellation

Dans un réseau plat, tous les hôtes sont gérés par une autorité centrale. Cette forme de réseau implique que tous les hôtes aient un nom unique. Transposé à un réseau étendu, ce système représenterait, pour l'autorité centrale, une charge administrative très lourde.

Dans un réseau hiérarchique (organisé en domaines), les hôtes sont gérés par groupes répartis dans une hiérarchie de domaines et de sous-domaines. Ainsi, l'unicité d'un nom d'hôte n'est exigée que dans son domaine local, et l'autorité centrale n'a en charge que le *domaine racine*. Cette structure, qui permet la gestion des sous-domaines en local, décharge l'autorité centrale. Prenons l'exemple du réseau Internet : son domaine racine est divisé en domaines `com` (secteur commercial), `edu` (secteur éducatif), `gov` (secteur public) et `mil` (secteur militaire). A ce niveau, seule l'autorité centrale est habilitée à ajouter de nouveaux domaines. Dans chacun de ces domaines, l'appellation de deuxième niveau est déléguée à un agent désigné. Ainsi, l'agent du domaine COM décide de l'appellation de tous les sous-domaines situés sous `com`. Les appellations de troisième niveau sont confiées à des agents désignés, etc. Dans la figure qui suit, le domaine Century est responsable de l'appellation de ses sous-domaines Austin, Hopkins et Charlotte.



Structure en domaines d'Internet

Le sous-domaine Austin pourrait aussi être divisé en zones comme Dev et Graphics. Dans ce cas, la zone `austin.century.com` couvre toutes les données du domaine `austin.century.com`, excepté celles dépendant de Dev et de Graphics. De même, la zone `dev.century.com` contient uniquement les données confiées à Dev et n'a aucune visibilité sur le contenu de la zone Graphics. La zone `austin.century.com` (par opposition au domaine du même nom) ne contient que les données qui n'ont pas été confiées aux autres zones.

Conventions d'appellation

Dans un système d'appellation hiérarchique, les noms sont formés par une suite de noms sans distinction majuscules/minuscules, séparés par un point et dépourvus d'espaces. Selon le protocole DOMAIN, la longueur du nom de domaine local doit être inférieure à 64 caractères et celle du nom d'hôte, à 32 caractères. Le nom de l'hôte vient en premier, suivi d'un " . " (point), d'une série de noms de domaines locaux et enfin du domaine racine. Au total, le nom complet d'un domaine pour un hôte ne doit pas dépasser 255 caractères (points compris) et se présente sous la forme :

```
hôte.sous-domaine1.[sous-domaine2. . . sous-domaine].domaine_racine
```

Les noms d'hôte étant uniques dans un domaine, vous pouvez utiliser des noms abrégés (relatifs) pour envoyer des messages au sein du même domaine. Par exemple, au lieu d'adresser un message à `smith.eng.lsu.edu`, un hôte du domaine `eng` peut indiquer seulement `smith`. Par ailleurs, chaque hôte peut être assorti de plusieurs alias utilisables par les autres hôtes.

Appellation des hôtes de votre réseau

Les noms d'hôte sont conçus pour simplifier la désignation des ordinateurs d'un réseau. Les administrateurs d'Internet ont constaté que, en matière de nom, il existe de bons et de mauvais choix. Il faut donc éviter certains pièges.

Voici quelques conseils pour vous aider à choisir les noms d'hôte de votre réseau :

- Préférez des noms peu usités tels que `sphinx` ou `eclipse`.
- Utilisez aussi des noms thématiques tels que des couleurs, des éléments `helium` , `argon` , ou `zinc`), des fleurs, des poissons, etc.

- Pensez encore à utiliser de véritables mots (plutôt que des chaînes de caractères aléatoires).

Puisez dans le vocabulaire existant (n'inventez pas de chaînes de caractères). Inversement, pour limiter les oublis ou les confusions (pour l'utilisateur ou la machine), évitez :

- les termes très courants tels que `up`, `down` ou `crash`,
- les noms composés uniquement de chiffres,
- les noms contenant des signes de ponctuation,
- les noms différenciés par des majuscules ou des minuscules (par exemple, `Orange` et `orange`),
- le nom ou les initiales de l'utilisateur principal du système,
- les noms de plus de 8 caractères,
- les orthographes inhabituelles ou volontairement incorrectes (par exemple, `czek`, qui peut être confondu avec "check" ou "tech"),
- les noms de domaine ou assimilables, tel que `yale.edu`.

Serveurs de noms

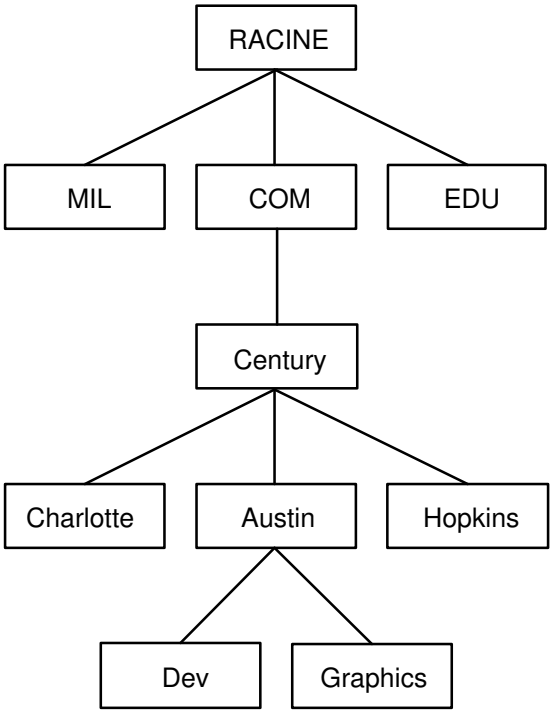
Dans une structure plate, tous les noms doivent être stockés dans le fichier /**etc**/**hosts** de chaque hôte membre du réseau. Ce système se révèle difficile à gérer lorsque le réseau est très étendu.

Dans une structure hiérarchique, les hôtes désignés comme *serveurs de noms* se chargent de résoudre le nom de chaque hôte en une adresse Internet. Ce mécanisme présente deux avantages par rapport à la structure plate : les ressources nécessaires à la résolution des noms ne sont pas mobilisées au niveau de chaque hôte et la tâche de l'administrateur système, alors déchargé de la mise à jour de chaque fichier de résolution des noms, s'en trouve allégée. L'ensemble des noms administrés par un serveur de noms est appelé *zone d'autorité* de ce serveur.

Remarque : La machine qui assure la fonction de résolution des noms pour une zone d'autorité est appelée hôte *serveur de noms* mais, en réalité, c'est le process (démon **named**) contrôlant cette fonction qui est le véritable serveur de noms.

Pour optimiser l'activité du réseau, les serveurs de noms stockent en mémoire *cache* (mémoire temporaire) les équivalences noms-adresses. Ainsi, lorsqu'un client demande au serveur de résoudre un nom, ce dernier consulte d'abord la mémoire cache où se trouvent les équivalences des derniers noms résolus. Ces équivalences sont conservées en mémoire pour une durée limitée (définie dans le paramètre TTL "Time-To-Live" de l'article de ressource), les noms de domaine et d'hôtes pouvant être modifiés. Les autorités d'appellation sont donc en mesure de spécifier la durée pendant laquelle la résolution de noms est réputée fiable.

Un système autonome peut comporter plusieurs serveurs de noms. Ces serveurs de noms suivent généralement une structure hiérarchique qui reflète l'organisation du réseau. Comme le montre la figure Structure en domaines d'Internet, chaque domaine peut bénéficier d'un serveur de noms responsable de tous ses sous-domaines. Les serveurs de noms des sous-domaines communiquent avec le serveur de noms du domaine supérieur (ou serveur de noms *père*) et les serveurs des autres sous-domaines.



Structure en domaines d'Internet

Dans la figure Structure en domaines d'Internet, Austin, Hopkins et Charlotte sont tous des sous-domaines de Century. Si la hiérarchie du réseau est respectée, le serveur de noms Austin communique avec Charlotte et Hopkins ainsi qu'avec le serveur de noms père Century. Austin communique également avec les serveurs de noms chargés de ses sous-domaines.

Il existe plusieurs types de serveur de noms :

serveur de noms maître	Il charge ses données à partir d'un fichier ou d'un disque et peut éventuellement déléguer des fonctions à d'autres serveurs de son domaine.
serveur de noms esclave	Au lancement du système, il reçoit du serveur de noms maître les informations sur une zone d'autorité donnée, et interroge périodiquement ce serveur maître pour la mise à jour des informations. Une fois le délai de rafraîchissement écoulé (valeur de l'article SOA sur le serveur de noms esclave), ou à réception d'une notification émise par le serveur maître, le serveur esclave recharge la base de données à partir du serveur maître si la sienne est devenue obsolète (autrement dit, si sa référence est antérieure à celle de la base du serveur maître). S'il devient nécessaire de forcer un transfert de zones, il suffit de supprimer les bases de données en place sur les serveurs esclaves et de régénérer le démon **named** sur le serveur de noms esclave.
Serveur de noms de tronçon (stub)	Bien que la méthode soit similaire à celle utilisée par le serveur de noms esclave, le serveur de noms de tronçon (stub) reproduit uniquement les données de serveurs de noms de la base de données maître, et non l'ensemble de la base.

Serveur d'indices (hint server)	Ce serveur de noms ne fonctionne que d'après les indices accumulés suite aux requêtes antérieures auprès d'autres serveurs. Le serveur d'indices (hint server) répond aux requêtes en demandant les informations souhaitées auprès des autres serveurs "experts" (serveurs ayant autorité) s'il ne dispose pas dans sa mémoire cache de l'équivalence demandée.
Serveur client ou expéditeur	Envoie les requêtes qu'il ne peut satisfaire localement aux serveurs répertoriés dans une liste prédéfinie. Les serveurs exclusivement expéditeurs (simples transmetteurs d'informations, qui ne sont pas à proprement parler des serveurs) ne dialoguent pas avec les serveurs de noms maîtres pour le domaine racine ou les autres domaines. Les requêtes transitent d'un serveur à l'autre de façon récursive : les serveurs expéditeurs sont contactés l'un après l'autre jusqu'à la fin de la liste. Ce type de configuration est généralement utilisé pour éviter que tous les serveurs d'un site dialoguent avec les autres serveurs Internet, ou pour constituer une mémoire cache étendue dans un certain nombre de serveurs de noms.
Serveur distant	Lance tous les programmes réseau qui font appel au serveur de noms, alors que le process serveur de noms n'est pas exécuté sur l'hôte local. Les requêtes sont prises en charge par un serveur de noms exécuté sur une autre machine du réseau.

Un hôte serveur de noms peut exercer diverses fonctions dans des zones d'autorité différentes. Par exemple, il peut faire fonction de serveur de noms maître dans une zone, et de serveur de noms esclave dans une autre.

Résolution de noms

La procédure d'obtention d'une adresse Internet à partir d'un nom d'hôte, appelée "résolution de noms", est exécutée par la sous-routine **gethostbyname**. Inversement, la traduction d'une adresse Internet en nom d'hôte est appelée "résolution inverse de noms", et est exécutée par la sous-routine **gethostbyaddr**. Ces routines permettent essentiellement d'accéder à une bibliothèque de routines de traduction de noms appelées "routines de résolution".

Les routines de résolution sur les hôtes TCP/IP essaient normalement de résoudre les noms en utilisant les sources suivantes :

1. BIND/DNS (named),
2. NIS (Network Information Services),
3. Fichier /**etc**/**hosts** local.

Lors de l'installation de NIS+, les préférences de recherche sont définies dans le fichier **irs.conf**. Pour plus d'informations, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

Pour résoudre un nom dans un réseau hiérarchique, la routine de résolution émet tout d'abord une requête auprès de la base de données du serveur de noms de domaine, résidant sur l'hôte local (s'il s'agit d'un hôte serveur de noms de domaine) ou sur un hôte étranger. Les serveurs de noms transforment les noms de domaines en adresses Internet. L'ensemble des noms administrés par un serveur de noms est appelé zone d'autorité de ce serveur. Si la routine de résolution utilise un serveur de noms distant, elle a recours au protocole DOMAIN (protocole de noms de domaine) pour les requêtes de mappage. Pour résoudre un nom dans un réseau plat, la routine recherche l'entrée correspondante dans le fichier local /**etc**/**hosts**. Si NIS ou NIS+ est utilisé, le fichier /**etc**/**hosts** du serveur maître est également vérifié.

Par défaut, les routines de résolution essaient de résoudre les noms à l'aide des ressources mentionnées ci–dessus. Le mécanisme BIND/DNS est lancé en premier. Si le fichier **/etc/resolv.conf** n'existe pas ou si le nom est introuvable, une requête est émise auprès de NIS si ce système est en service. NIS ayant autorité sur le fichier **/etc/hosts** local, la recherche peut s'arrêter là. Si le service NIS n'est pas accessible, la recherche s'effectue alors sur le fichier **/etc/hosts** local. Si ce nom reste introuvable, les routines de résolution renvoient le message HOST_NOT_FOUND. Si aucun service n'est accessible, les routines de résolution renvoient le message SERVICE_UNAVAILABLE.

Il est possible de modifier l'ordre de recherche présenté ci–dessus en créant le fichier de configuration **/etc/irs.conf** pour y préciser l'ordre voulu. Ces deux ordres (ordre par défaut et fichier **/etc/irs.conf**) peuvent encore être écrasés par la variable d'environnement **NSORDER**. Si le fichier **/etc/irs.conf** ou la variable **NSORDER** est défini, l'option doit être assortie d'au moins une valeur.

Pour définir l'ordre des hôtes avec le fichier **/etc/irs.conf** :

```
hosts valeur [ continue ]
```

Pour définir l'ordre, chaque méthode doit être indiquée sur une ligne distincte. La *valeur* correspond à une des méthodes indiquées et le mot clé **continue** indique qu'une autre méthode de résolution figure en ligne suivante.

Dans la variable d'environnement **NSORDER** :

```
NSORDER = valeur,valeur,valeur
```

L'ordre est spécifié sur une seule ligne avec des valeurs séparées par une virgule. Les espaces sont admis entre les virgules et le signe égal.

Par exemple, si le réseau local est "plat", seul le fichier **/etc/hosts/** est nécessaire.

Dans cet exemple, le fichier **/etc/irs.conf** contiendrait la ligne suivante :

```
hosts local
```

Autrement, la variable **NSORDER** pourrait être renseignée comme suit :

```
NSORDER=local
```

Si le réseau local est "hiérarchique" et fait appel à un serveur de noms pour la résolution des noms et à un fichier **/etc/hosts** pour une copie de secours, les deux services doivent être spécifiés.

Le fichier **/etc/irs.conf** contient alors les lignes suivantes :

```
hosts dns continue
hosts local
```

Et la variable **NSORDER** est renseignée comme suit :

```
NSORDER=bind,local
```

Remarque : les valeurs doivent être spécifiées en minuscules.

En suivant un ordre de résolution défini ou l'ordre par défaut, l'algorithme de recherche ne passe d'une routine à la suivante que si :

- le service courant n'est pas accessible (il n'est pas actif),
- le service courant ne trouve pas le nom recherché et n'est pas un serveur "expert".

Si le fichier **/etc/resolv.conf** n'existe pas, le mécanisme BIND/DNS est considéré comme non installé, et par là–même non accessible. En cas d'échec des sous–routines **getdomainname** et **yp_bind**, le service NIS est considéré comme non installé et par là–même non accessible. Si le fichier **/etc/hosts** n'a pas pu être ouvert, il est impossible de procéder à une recherche locale et d'accéder au fichier et au service.

Un service est dit *expert* si, de par les informations qu'il contient, il est jugé mieux à même de répondre aux requêtes que les services cités après lui. Les routines de résolution n'essaient pas les services suivants, puisque ces derniers ne peuvent contenir qu'un sous–ensemble des informations du service expert. La résolution des noms s'arrête à la consultation du service expert même s'il n'est pas parvenu à fournir le nom demandé (message HOST_NOT_FOUND renvoyé). En cas d'indisponibilité d'un service expert, le service suivant spécifié est interrogé.

La source "expert" est déclarée par la chaîne "=auth" spécifiée à la suite de son nom. Il est possible de spécifier également tout le mot "authoritative". Par exemple, si la variable **NSORDER** contient :

```
hosts = nis=auth,dns,local
```

Si NIS est actif, la recherche prend fin après consultation de NIS, que le nom ait été trouvé ou non. Sinon, elle est étendue à la source suivante (en l'occurrence, DNS).

Les serveurs de noms TCP/IP ont recours à la mémoire cache pour réduire le coût de recherche de noms d'hôte sur réseaux distants. Ainsi, ils consultent d'abord la mémoire cache où se trouvent les équivalences des derniers noms résolus. Ces équivalences sont conservées en mémoire pour une durée limitée (définie dans le paramètre TTL "Time-To-Live" de l'article de ressource), les noms de domaine et d'hôtes pouvant être modifiés. Les serveurs de noms sont donc en mesure de spécifier la durée pendant laquelle leurs réponses sont réputées fiables.

Risques de conflits de noms d'hôte

En environnement DNS, un nom d'hôte défini soit par la commande **hostname** en ligne de commande, soit par le fichier **rc.net**, doit être le nom officiel de l'hôte tel qu'il est renvoyé par le serveur de noms. Ce nom est généralement le nom complet du domaine de l'hôte sous la forme :

```
hôte.sousdomaine.sousdomaine.domaineracine
```

Remarque : pour les routines de résolution, le domaine par défaut doit être défini. S'il n'est pas défini dans **hostname**, il doit l'être dans **/etc/resolv.conf**.

Si le nom de l'hôte n'est pas configuré en nom complet du domaine, et si le système est configuré avec serveur de noms de domaine associé au programme **sendmail**, le fichier de configuration **/etc/sendmail.cf** doit être modifié conformément à ce nom officiel. Pour que le programme **sendmail** fonctionne correctement, il faut de plus que les macros de nom de domaine soient définies dans cette configuration.

Remarque : pour toutes les fonctions de **sendmail**, le domaine spécifié dans le fichier **/etc/sendmail.cf** prime sur celui défini à la commande **hostname**.

Risques de conflits de noms de domaine

Dans le cas d'un hôte membre d'un réseau DOMAIN mais qui n'est pas un serveur de noms, le nom de domaine local et le serveur de noms de domaine sont spécifiés dans le fichier **/etc/resolv.conf**. Or, dans un hôte serveur de noms de domaine, le domaine local et les autres serveurs de noms sont définis dans des fichiers que le démon **named** lit à son lancement.

Protocole RARP

Le protocole RARP (Reverse Address Resolution Protocol) traduit les adresses matérielles uniques en adresses Internet sur la carte LAN Ethernet (protocole Ethernet seulement). Le protocole Ethernet standard est pris en charge dans les limites suivantes. Le serveur :

- répond uniquement aux requêtes RARP,
- se limite aux entrées permanentes de la table ARP,
- n'utilise pas les entrées dynamiques de la table ARP,
- ne répond pas automatiquement pour lui-même.

L'administrateur système doit créer et tenir à jour manuellement une table des entrées permanentes ARP à l'aide de la commande **arp**. Une entrée de table ARP spécifique doit être ajoutée sur le serveur AIX pour chaque hôte qui sollicite des réponses RARP d'une source "expert".

Résolution locale des noms (/etc/hosts)

Le fichier /**etc**/**hosts** doit être configuré si vous travaillez sur un réseau limité et plat. Cette configuration peut également être utile sur un réseau hiérarchique pour identifier les hôtes inconnus des serveurs de noms.

Vous pouvez configurer votre système en vue de la résolution locale de noms via Web-based System Manager, SMIT ou les commandes. Si c'est à partir de la ligne de commande, veillez à conserver le format du fichier /**etc**/**hosts**, comme indiqué à la section "Hosts File Format for TCP/IP" du manuel *AIX Files Reference*).

Résolution locale des noms		
Raccourci Web-based System Manager, **wsm network** (application wsm network) OU		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Afficher la liste des hôtes	**smit lshostent**	affichez /**etc**/**hosts**
Ajouter un hôte	**smit mkhostent**	éditez /**etc**/**hosts**
Modifier/afficher les caractéristiques d'un hôte	**smit chhostent**	éditez /**etc**/**hosts**
Supprimer un hôte	**smit rmhostent**	éditez /**etc**/**hosts**

Préparation à la résolution DNS (DOMAIN)

Si vous faites partie d'un interréseau étendu, vous devez coordonner vos serveurs de noms et domaines avec leur autorité centrale.

Voici quelques conseils pour configurer le système pour la résolution DNS :

- Procurez-vous un exemplaire du manuel *DNS and BIND in a Nutshell*. (La configuration pour DNS est l'une des tâches les plus ésotériques que l'administrateur de réseau TCP/IP ait à accomplir). Vu l'étendue des possibilités en matière d'architecture de noms de domaines et de configurations de serveurs de noms, cet ouvrage vous sera des plus précieux. Vous trouverez également des informations utiles sur ce type de résolution dans le manuel *TCP/IP Network Administration*. L'interaction entre DNS et NIS est expliquée dans le manuel *Managing NFS and NIS*. Pour plus d'informations sur le NIS+, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.
- Planifiez la configuration.

  Rappelez-vous qu'il est *bien* plus compliqué de changer un nom que de le définir. Avant de configurer vos fichiers, décidez (en accord avec votre organisation) des noms des hôtes, du réseau, de la passerelle et du serveur de noms.
- Définissez des serveurs de noms redondants.

  A défaut, veillez à définir des serveurs de noms esclaves et des serveurs d'indices pour disposer d'un système de secours.
- Pour la sélection des serveurs de noms :
  - choisissez les machines géographiquement les plus proches des systèmes extérieurs ;
  - Vos serveurs de noms doivent être aussi indépendants que possible. Si possible, utilisez des alimentations électriques et des câblages distincts.

  - désignez un autre réseau comme réseau de secours pour votre service de résolution des noms ; faites de même pour les autres réseaux.
- testez les serveurs :
  - testez la résolution des noms normale et inverse,
  - testez le transfert de zone du serveur de noms maître au serveur de noms esclave,
  - testez chaque serveur de noms, après une panne et un réamorçage du système.
- Faites transiter vos requêtes de résolution de noms par des serveurs expéditeurs avant de les envoyer vers des serveurs de noms extérieurs. Cela permet aux serveurs de noms de partager leur mémoire cache et d'améliorer les performances en allégeant la charge des serveurs de noms maîtres.

Configuration des serveurs de noms

Dans un réseau hiérarchisé, certains hôtes sont définis comme *serveurs de noms*. Ces hôtes convertissent les noms en adresses Internet pour d'autres hôtes. Cette fonction est contrôlée par le démon **named**, qui doit par conséquent être actif sur tout hôte serveur de noms.

Avant de procéder à la configuration, déterminez les types de serveur de noms les mieux adaptés à votre réseau. Il existe trois types :

le *serveur de noms maître* : il stocke la base de données contenant les équivalences noms-adresses, charge ses données à partir d'un fichier ou d'un disque et peut éventuellement déléguer des fonctions à d'autres serveurs de son domaine. *serveur de noms esclave* ou *serveur de noms de tronçon (stub)* : ceux–ci reçoivent leurs informations d'un serveur maître au démarrage du système pour une zone d'autorité donnée, puis l'interrogent périodiquement pour les mettre à jour. *serveur d'indices (hint server)* : ce serveur répond aux requêtes de résolution des noms en demandant les informations souhaitées auprès d'autres serveurs experts.

Remarque : les générations antérieures du serveur de noms **named** définissaient le serveur maître comme serveur de noms primaire, le serveur esclave comme serveur de noms secondaire, et le serveur d'indices comme serveur de mémoire cache. Dans cette documentation, toute référence au fichier **named.conf** est spécifique à AIX version 4.3.2 ou ultérieure.

Rappelons qu'un serveur de noms peut exercer des fonctions différentes selon les zones d'autorité. Par exemple, un hôte peut faire fonction de serveur de noms maître dans une zone, et de serveur de noms esclave dans une autre. Si le service NIS ou NIS+ est installé sur votre système, ces services peuvent également vous aider dans la résolution des noms. Pour plus d'informations, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

Plusieurs fichiers sont impliqués dans la configuration des serveurs de noms.

conf Fichier lu au démarrage du démon **named**. Les articles du fichier conf indiquent au démon le type du serveur, ses zones d'autorité (domaines) et l'implantation des données pour la configuration initiale de sa base de données. Son nom par défaut est **/etc/named.conf**. Vous pouvez lui en attribuer un autre en indiquant sur la ligne de commande le nouveau nom complet dès le lancement du démon **named**. Si vous utilisez pour l'amorçage le fichier **/etc/named.conf**, mais que ce dernier n'existe pas, un message est généré dans **syslog** et le démon **named** s'arrête. Toutefois, si un autre fichier conf a été prévu et qu'il n'existe pas, il n'y aura pas de message d'erreur et le démon continuera.

cache Fichier contenant les informations sur la mémoire cache locale : nom et adresse des serveurs de noms bénéficiant de la plus haute ”autorité”. Ce fichier respecte le format des articles de ressource standard (Standard Resource Record Format). Son nom est défini dans le fichier conf.

domain data Il existe trois types de fichiers domain data, également nommés fichiers de données **named**. Le fichier **named** *local* contient les informations de résolution d'adresses en bouclage local. Le fichier de *données* **named** contient les données de résolution d'adresses pour toutes les machines de la zone d'autorité du serveur de noms. Le fichier de *données inversées* **named** contient les informations de résolution inversée d'adresses pour toutes les machines de la zone d'autorité du serveur de noms. Ces trois fichiers respectent le format des articles de ressource standard (Standard Resource Record Format). Leurs noms, défini dans le fichier conf, peut être modifié par l'utilisateur. Par convention, ce nom comporte celui du démon (`named`) avec, en extension, le type de fichier et le nom du domaine. Par exemple, les fichiers du serveur de noms du domaine `abc` peuvent être :

```
named.abc.data

named.abc.rev

named.abc.local
```

En modifiant les fichiers de données **named**, il est conseillé d'incrémenter le numéro de série donné dans l'article SOA pour les serveurs de noms esclaves afin d'effectuer correctement les modifications de zones.

resolv.conf Ce fichier indique par sa présence que l'hôte doit d'abord faire appel à un serveur de noms pour effectuer une résolution. En l'absence de **resolv.conf**, l'hôte fait ensuite appel au fichier /**etc**/**hosts**. Obligatoire sur un serveur de noms, il peut contenir l'adresse de l'hôte local, l'adresse de bouclage (127.0.0.1), ou être vide.

Remarque : pour les routines de résolution, le domaine par défaut doit être défini. S'il n'est pas défini dans /**etc**/**resolv.conf**, il doit l'être dans **hostname**.

Le paramètre TTL (Time-To-Live) est spécifié dans les articles de ressource. A défaut, le délai appliqué est la plus petite valeur définie dans l'article SOA (Start Of Authority) de la zone d'autorité concernée. TTL est utilisé lorsque les données sont stockées en dehors d'une zone (en mémoire cache) pour s'assurer qu'elles n'y sont pas maintenues indéfiniment.

Configuration d'un serveur de noms maître

Pour configurer un serveur de noms maître, utilisez le raccourci Web-based System Manager **wsm network** ou suivez la procédure ci–dessous, qui édite une série de fichiers puis a recours à SMIT ou à la ligne de commande pour démarrer le démon **named**.

1. Editez le fichier /**etc**/**named.conf**. Si le répertoire /**etc** ne contient pas de fichier **named.conf**, copiez-y le fichier-type /**usr**/**samples**/**tcpip**/**named.conf** et éditez-le. Pour en savoir plus et examiner un exemple de fichier de configuration, reportez-vous à la section ”named.conf File Format for TCP/IP” dans le manuel *AIX Files Reference*.

   Fichier lu au démarrage du démon **named**. Ce fichier indique au serveur son type, sa ou ses zones d'autorité et l'implantation des informations initiales qu'il doit aller chercher.

a. Utilisez la clause de configuration *options* pour spécifier le répertoire contenant les fichiers de données **named** (facultatif). Insérez cette clause pour que ces fichiers utilisent les chemins d'accès relatifs à ce répertoire. Par exemple :

```
options {
    directory "/usr/local/domain";
};
```

b. Eventuellement, spécifiez le nom du fichier de zone d'indices. Ce fichier permet de stocker les données en dehors des zones définies. Par exemple :

```
zone "." IN {
    type hint;
    file "/etc/named.ca";
};
```

c. Indiquez le nombre de zones. Pour configurer un serveur en maître d'une zone, spécifiez chaque zone avec son fichier de données de domaine. Voici un exemple de serveur *maître* pour les deux zones d'expéditeur et de recherche inversée :

```
zone "abc.aus.century.com" in {
    type master;
    file "/etc/named.abcdata";
};

zone "201.9.192.in-addr.arpa" in {
    type master;
    file "/etc/named.abcrev";
};
```

d. Définissez le nom du fichier **named** local. Par exemple :

```
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "/etc/named.local";
};
```

2. Editez le fichier /**etc**/**named.ca**. Pour en savoir plus et disposer d'un exemple de fichier cache, reportez-vous à la section "DOMAIN Cache File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   Ce fichier contient l'adresse des serveurs de noms "expert" ou racine *(root)* pour le domaine. Par exemple :

```
; root name servers.
         1          IN    NS    relay.century.com.
relay.century.com.   3600000    IN    A     129.114.1.2
```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

3. Editez le fichier /**etc**/**named.local**. Pour en savoir plus et disposer d'un exemple de fichier de données local, reportez-vous à la section "DOMAIN Local Data File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   a. Spécifiez pour la zone la valeur de SOA (Start Of Authority) et les délais TTL (time-to-live) par défaut. Par exemple :

```
@ IN SOA venus.abc.aus.cntry.com. gail.zeus.abc.aus.cntry.com.
(
                              1.1     ;serial
                              3600    ;refresh
                              600     ;retry
                              3600000 ;expire
                              86400)  ;minimum
```

   b. Spécifiez l'article NS (serveur de noms). Par exemple :

```
IN    NS     venus.abc.aus.century.com.
```

c. Spécifiez l'article PTR (pointeur).

```
1       IN    PTR    localhost.
```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

4. Editez le fichier **/etc/named.data**. Le fichier **/usr/lpp/tcpip/samples/hosts.awk** fournit des instructions pour la création du fichier **/etc/named.data**. Inspirez-vous du fichier-type **/usr/lpp/tcpip/samples/named.data** pour créer **/etc/named.data**. Pour en savoir plus et disposer d'un exemplede fichier de données hôte, reportez-vous à la section "DOMAIN Data File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   a. Indiquez pour la zone la valeur de SOA (Start Of Authority) et les délais TTL (time-to-live). Cet article indique le début de la zone. Il ne peut y avoir qu'un seul article SOA par zone. Par exemple :

```
@    IN    SOA    venus    bob.robert.abc.aus.century.com.
(
                              1.1      ;serial
                              3600     ;refresh
                              600      ;retry
                              3600000  ;expire
                              86400)   ;minimum
```

   b. Précisez les informations de résolution de noms en adresses pour tous les hôtes dans la zone d'autorité du serveur de noms. Par exemple :

```
venus          IN    A          192.9.201.1
venus          IN    A          128.114.100.1
```

   c. Insérez les articles de serveur de noms pour tous les serveurs maîtres de la zone. Par exemple :

```
IN     NS         venus.abc.century.com
IN     NS         kronos.xyz.century.com
```

   d. Insérez d'autres types d'entrée : articles de nom canonique ou d'échangeur de courrier (MX), par exemple.

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

5. Editez le fichier **/etc/named.rev**. Le fichier **/usr/lpp/tcpip/samples/addrs.awk** fournit des instructions sur la création du fichier **/etc/named.rev**. Pour en savoir plus et examiner un exemple de fichier de données hôte inverse, consultez la section "DOMAIN Reverse Data File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   a. Spécifiez pour la zone la valeur de SOA (Start Of Authority) et les délais TTL (time-to-live) par défaut. Cet article indique le début de la zone. Il ne peut y avoir qu'un seul article SOA par zone. Par exemple :

```
@  IN  SOA  venus.abc.aus.century.com.
bob.robert.abc.aus.century.com.
(
                              1.1      ;serial
                              3600     ;refresh
                              600      ;retry
                              3600000  ;expire
                              86400)   ;minimum
```

   b. Précisez les informations de résolution de noms en adresses pour tous les hôtes dans la zone d'autorité du serveur de noms. Par exemple :

```
;ABC.AUS.CENTURY.COM Hosts
1                        IN    PTR   venus.abc.aus.century.com.
2                        IN    PTR   kronos.abc.aus.century.com.
```

c. Insérez d'autres types d'entrée : articles de nom canonique ou de serveur de noms (facultatif).

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

6. Créez un fichier **/etc/resolv.conf** via la commande :

   ```
   touch /etc/resolv.conf
   ```

   Ce fichier indique par sa présence que l'hôte doit d'abord faire appel à un serveur de noms pour effectuer une résolution, et non au fichier **/etc/hosts**. Sa présence est nécessaire sur un serveur de noms et il peut contenir l'adresse locale de l'hôte, l'adresse de bouclage (127.0.0.1) ou être vide.

   Autrement, le fichier **/etc/resolv.conf** peut contenir l'entrée suivante :

   ```
   nameserver 127.0.0.1
   ```

   `127.0.0.1` est l'adresse de bouclage qui, pour l'accès au serveur de noms, dirige l'hôte vers lui-même. Ce fichier **/etc/resolv.conf** peut également comporter une ligne du type :

   ```
   domain NomDomaine
   ```

   Dans l'exemple précédent, *NomDomaine* serait `aus.century.com .`

7. Exécutez l'une des tâches suivantes :

   – Activez le démon **named** :

     ```
     smit stnamed
     ```

     Cette commande initialise le démon à chaque lancement du système. Indiquez quand vous souhaitez lancer le démon **named** : immédiatement, au prochain lancement du système ou les deux.

   – Editez le fichier **/etc/rc.tcpip**. Activez le démon **named** en retirant la marque de commentaire (#) de la ligne suivante :

     ```
     #start /etc/named "$src_running"
     ```

     Cette commande initialise le démon à chaque lancement du système.

8. Si vous ne souhaitez pas initialiser le démon **named** via SMIT, lancez-le pour la session en cours par la commande :

   ```
   startsrc -s named
   ```

Configuration d'un serveur de noms esclave

Pour configurer un serveur de noms esclave, utilisez le raccourci Web-based System Manager **wsm network** ou suivez la procédure ci–dessous, qui édite une série de fichiers puis a recours à SMIT ou à la ligne de commande pour démarrer le démon **named**.

1. Editez le fichier **/etc/named.conf**. Si le répertoire **/etc** ne contient pas de fichier **named.conf**, copiez-y le fichier-type **/usr/samples/tcpip/named.conf** et éditez-le. Pour en savoir plus et examiner un exemple de fichier de configuration, reportez-vous à la section "named.boot File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   Fichier lu au démarrage du démon **named**. Ce fichier indique au serveur son type, sa zone d'autorité et l'implantation des informations initiales qu'il doit aller chercher.

   a. Utilisez la clause de configuration *options* pour spécifier le répertoire contenant les fichiers de données **named** (facultatif). Insérez cette clause pour que ces fichiers utilisent les chemins d'accès relatifs à ce répertoire. Par exemple :

      ```
      options {
          directory "/usr/local/domain";
      };
      ```

   b. Eventuellement, spécifiez le nom du fichier de zone d'indices. Ce fichier permet de stocker les données en dehors des zones définies. Par exemple :

```
zone "." IN {
    type hint;
    file "/etc/named.ca";
};
```

c. Spécifiez les clauses de zone esclave. Chaque strophe comprend le type de zone, avec un nom de fichier facultatif pour une copie de secours des données, et la listes des adresses Internet de serveurs maîtres. Cette liste d'adresses définit les hôtes depuis lesquels la zone sera répliquée. Par exemple :

```
zone "abc.aus.century.com" IN {
    type slave;
    file "/etc/named.abc.bak";
    masters { 192.9.201.1; 192.9.201.2; };
};

zone "xyz.aus.century.com" IN {
    type slave;
    file "/etc/named.xyz.bak";
    masters { 192.9.201.1; 192.9.201.2; };
};
```

d. Insérez les clauses de zone esclave pour fournir les informations de résolution inverse. Par exemple :

```
zone "201.9.192.in-addr.arpa" in {
    type slave;
    file "named.rev.bak";
    masters { 192.9.201.1; 192.9.201.2; };
};

zone "100.114.128.in-addr.arpa" IN {
    type slave;
    file "named.rev.bak";
    masters { 192.9.201.1; 192.9.201.2; };
};
```

e. Pour supporter l'adressage en boucle, indiquez une zone de type *maître* avec comme source le fichier **/etc/named.local**, ainsi que sa zone d'autorité (domaine).

```
zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "/etc/named.local";
};
```

2. Editez le fichier **/etc/named.ca**. Pour en savoir plus et disposer d'un exemple de fichier cache, reportez-vous à la section "DOMAIN Cache File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   Ce fichier contient l'adresse des serveurs de noms "experts" pour le domaine racine (root) du réseau. Par exemple :

```
; root name servers.
         1          IN    NS    relay.century.com.
relay.century.com.   3600000    IN    A     129.114.1.2
```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

3. Editez le fichier **/etc/named.local**. Pour en savoir plus et disposer d'un exemple de fichier de données local, reportez-vous à la section "DOMAIN Local Data File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   a. Spécifiez pour la zone la valeur de SOA (Start Of Authority) et les délais TTL (time-to-live) par défaut. Par exemple :

```
@ IN SOA venus.abc.aus.cntry.com. gail.zeus.abc.aus.cntry.com.
(
                              1.1     ;serial
                              3600    ;refresh
                              600     ;retry
                              3600000 ;expire
                              86400)  ;minimum
```

b. Spécifiez l'article NS (serveur de noms). Par exemple :

```
IN    NS     venus.abc.aus.century.com.
```

c. Spécifiez l'article PTR (pointeur).

```
1      IN    PTR    localhost.
```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

4. Créez un fichier /**etc**/**resolv.conf** via la commande :

```
touch /etc/resolv.conf
```

Ce fichier indique par sa présence que l'hôte doit d'abord faire appel à un serveur de noms pour effectuer une résolution, et non au fichier /**etc**/**hosts**. Vous pouvez insérer des articles pour spécifier le nom, le domaine et l'adresse du serveur de noms.

5. Exécutez l'une des tâches suivantes :

– Activez le démon **named** :

```
smit stnamed
```

Cette commande initialise le démon à chaque lancement du système. Indiquez quand vous souhaitez lancer le démon **named** : immédiatement, au prochain lancement du système ou les deux.

– Editez le fichier /**etc**/**rc.tcpip**. Activez le démon **named** en retirant la marque de commentaire (#) de la ligne suivante :

```
#start /etc/named "$src_running"
```

Cette commande initialise le démon à chaque lancement du système.

6. Si vous ne souhaitez pas initialiser le démon **named** via SMIT, lancez-le pour la session en cours par la commande :

```
startsrc -s named
```

Configuration d'un serveur d'indices

Pour configurer un serveur de noms d'indices ou de mémoire cache, utilisez le raccourci Web-based System Manager **wsm network** ou suivez la procédure ci–dessous, qui édite une série de fichiers puis a recours à SMIT ou à la ligne de commande pour démarrer le démon **named**.

Procédure

Configurez un serveur d'indices comme suit :

1. Editez le fichier /**etc**/**named.conf**. Si le répertoire /**etc** ne contient pas de fichier **named.conf**, copiez-y le fichier-type /**usr**/**samples**/**tcpip**/**named.conf** et éditez-le. Pour en savoir plus et examiner un exemple de fichier de configuration, reportez-vous à la section "named.boot File Format for TCP/IP" dans le manuel *AIX Files Reference*.

– Pour supporter l'adressage en boucle, indiquez une zone de type *maître* avec comme source le fichier /**etc**/**named.local**, ainsi que sa zone d'autorité (domaine). Par exemple :

```
zone ”.” IN {
    type hint;
    file ”/etc/named.ca”;
};
```

2. Editez le fichier /**etc**/**named.ca**. Pour en savoir plus et disposer d’un exemple de fichier cache, reportez-vous à la section ”DOMAIN Cache File Format for TCP/IP” dans le manuel *AIX Files Reference*.

   Ce fichier contient l’adresse des serveurs de noms ”experts” pour le domaine racine (root) du réseau. Par exemple :

```
; root name servers.
         1          IN    NS     relay.century.com.
relay.century.com.   3600000     IN    A      129.114.1.2
```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

3. Editez le fichier /**etc**/**named.local**. Pour en savoir plus et disposer d’un exemple de fichier de données local, reportez-vous à la section ”DOMAIN Local Data File Format for TCP/IP” dans le manuel *AIX Files Reference*.

   a. Spécifiez pour la zone la valeur de SOA (Start Of Authority) et les délais TTL (time-to-live) par défaut. Par exemple :

```
@ IN SOA venus.abc.aus.cntry.com. gail.zeus.abc.aus.cntry.com.
(
                              1.1     ;serial
                              3600    ;refresh
                              600     ;retry
                              3600000 ;expire
                              86400)  ;minimum
```

   b. Spécifiez l’article NS (serveur de noms). Par exemple :

```
IN    NS      venus.abc.aus.century.com.
```

   c. Spécifiez l’article PTR (pointeur).

```
1       IN    PTR    localhost.
```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

4. Créez un fichier /**etc**/**resolv.conf** via la commande :

```
touch /etc/resolv.conf
```

   Ce fichier indique par sa présence que l’hôte doit d’abord faire appel à un serveur de noms pour effectuer une résolution, et non au fichier /**etc**/**hosts**. Vous pouvez insérer des articles pour spécifier le nom, le domaine et l’adresse du serveur de noms.

5. Exécutez l’une des tâches suivantes :

   – Activez le démon **named** :

```
smit stnamed
```

     Cette commande initialise le démon à chaque lancement du système. Indiquez quand vous souhaitez lancer le démon **named** : immédiatement, au prochain lancement du système ou les deux.

   – Editez le fichier /**etc**/**rc.tcpip**. Activez le démon **named** en retirant la marque de commentaire (#) de la ligne suivante :

```
#start /etc/named ”$src_running”
```

     Cette commande initialise le démon à chaque lancement du système.

6. Si vous ne souhaitez pas initialiser le démon **named** via SMIT, lancez-le pour la session en cours par la commande :

```
startsrc –s named
```

Configuration d'un serveur de courrier de domaine

En définissant un serveur de courrier de domaine, vous mettez à la disposition des utilisateurs externes une méthode d'adressage simple leur permettant de correspondre avec votre organisation. Sans cela, l'adresse doit obligatoirement préciser un hôte particulier de votre organisation. Par exemple, `sam@orange.widget.com`, *widget.com* étant le nom de domaine de votre organisation, et *orange* l'hôte utilisé par `sam`. Avec le serveur de courrier de domaine, il suffit à l'utilisateur externe d'indiquer le nom de l'utilisateur et le nom du domaine sans le nom de l'hôte, dans notre exemple, `sam@widget.com`.

Vous pouvez configurer un serveur de courrier via le raccourci Web-based System Manager **wsm network** ou via l'une des procédures suivantes.

Configuration d'un serveur de courrier de domaine

1. Créez un article MX et un article A pour le serveur de courrier (`black.widget.com`) :

```
widget.com           IN    MX     10 black.widget.com
widget.com           IN     A     192.10.143.9
black.widget.com     IN     A     192.10.143.9
```

2. Editez **sendmail.cf** sur le serveur de courrier (`black.widget.com`) pour ajouter l'alias du domaine (classe **w**) :

```
Cw $w $?D$w.$D$. widget.com
```

3. Les clients de la messagerie doivent savoir où adresser leur courrier non local. Editez **sendmail.cf** sur chaque client pour pointer sur le serveur de courrier (macro **S**) :

```
DRblack.widget.com
```

4. A l'aide de l'option **NameServOpt**, configurez le démon **sendmail** de sorte que chacun puisse utiliser les articles MX définis dans le serveur de noms `brown.widget.com`.
5. Ajoutez l'alias des utilisateurs du domaine qui n'ont pas de compte sur le serveur de courrier, en vous aidant du fichier d'alias. Par exemple :

```
sam:sam@orange.widget.com
david:david@green.widget.com
judy:judy@red.widget.com
```

Remarque : les articles MB peuvent remplir la même fonction.

6. La base de données ayant été modifiée, il est conseillé d'incrémenter le numéro de série donné dans l'article SOA.
7. Régénérez la base de données du serveur de noms via la commande **refresh –s named**.
8. Ensuite, lancez successivement les commandes :
   a. **sendmail –bz** pour recompiler le fichier **sendmail.cf** sur le serveur de courrier,
   b. **sendmail –bi** pour recompiler la base d'alias sur le serveur de courrier,
   c. **refresh –s sendmail** pour prendre les modifications en compte.
9. Sur les clients, recompilez (**sendmail**) puis lancez **refresh -s sendmail** pour prendre les modifications en compte.

Il existe d'autres méthodes permettant de configurer un serveur de courrier de domaine. Les procédures qui suivent utilisent les articles MB, MR et MG.

Configuration d'un serveur de courrier de domaine avec des articles MB

1. Définissez un article MB pour chaque utilisateur du domaine. Par exemple :

   ```
   sam IN MB orange.widget.com.
   ```

   dans le fichier **/etc/named.data** de l'hôte `brown.widget.com` . Cette instruction stipule le serveur de courrier (`black.widget.com`) destinataire pour chaque utilisateur du domaine.

2. Configurez le démon **sendmail** sur le serveur de courrier (`black.widget.com`) pour qu'il utilise les articles MB définis sur le serveur de noms (`brown.widget.com`). Ayez recours à l'option **NameServOpt**.

3. La base de données ayant été modifiée, il est conseillé d'incrémenter le numéro de série donné dans l'article SOA.

4. Régénérez la base de données du serveur de noms via la commande **refresh –s named**.

5. Entrez la commande **sendmail –bz** pour recompiler le fichier **sendmail.cf** sur le serveur de courrier, puis la commande **refresh -s sendmail** pour appliquer les modifications.

Définition d'un article MR (Mail Rename)

1. Editez le fichier **/etc/named.data** sur votre serveur de noms de domaine.

2. Ajoutez un article MR pour chaque alias. Par exemple, l'utilisateur `sam` dont l'alias est `sammy` aura pour article MR :

   ```
   sammy IN MR sam
   ```

   Cet article demande que tous les messages adressés à `sammy` soient livrés à `sam`. Il faut prévoir une ligne par article MR.

3. La base de données ayant été modifiée, il est conseillé d'incrémenter le numéro de série donné dans l'article SOA.

4. Régénérez la base de données du serveur de noms via la commande **refresh –s named**.

5. Entrez la commande **sendmail –bz** pour recompiler le fichier **sendmail.cf** sur le serveur de courrier, puis la commande **refresh -s sendmail** pour appliquer les modifications.

Définition d'un article MG (Mail Group)

1. Editez le fichier **/etc/named.data** sur votre serveur de noms de domaine.

2. Ajoutez des articles MG pour chaque groupe courrier. Ces articles fonctionnent comme le fichier **/etc/aliases**, les alias étant tenus à jour sur le serveur de noms. Par exemple :

   ```
   users IN HINFO users-request widget.com
   users IN MG sam
   users IN MG david
   users IN MG judy
   ```

   Ces articles demandent que tous les messages adressés à `users@widget.com` soient livrés à `sam`, `david` et `judy`. Il faut prévoir une ligne par article MG.

Remarque : des articles MB doivent avoir été définis pour `sam`, `david` et `judy`.

3. La base de données ayant été modifiée, il est conseillé d'incrémenter le numéro de série donné dans l'article SOA.

4. Régénérez la base de données du serveur de noms via la commande **refresh –s named**.

5. Entrez la commande **sendmail –bz** pour recompiler le fichier **sendmail.cf** sur le serveur de courrier, puis la commande **refresh -s sendmail** pour appliquer les modifications.

Définition d'articles MX (Mail Exchanger)

1. Editez le fichier /**etc**/**named.data** sur votre serveur de noms de domaine.
2. Ajoutez des articles MX pour chaque machine indirectement connectée à votre réseau et avec laquelle vous souhaitez correspondre. Par exemple, si le courrier adressé aux utilisateurs de `purple.widget.com` doit être transmis à `post.office.widget`, ajoutez un article MX comme suit :

   ```
   purple.widget.com IN MX 0 post.office.widget.
   ```

   Lorsque vous utilisez les articles d'échangeur de courrier (MX), vous devez spécifier le nom de la machine et le nom d'hôte. Il faut prévoir une ligne par article MX. L'utilisation des caractères génériques est admise :

   ```
   *.widget.com IN MX 0 post.office.widget.
   ```

   Ces articles demandent que les messages adressés à un hôte inconnu (sans article MX explicite) du domaine `widget.com` soient expédiés à `post.office.widget`.

Remarque : les caractères génériques dans les articles MX sont incompatibles avec l'utilisation d'Internet.

3. La base de données ayant été modifiée, il est conseillé d'incrémenter le numéro de série donné dans l'article SOA.
4. Régénérez la base de données du serveur de noms via la commande **refresh –s named**.
5. Entrez la commande **sendmail –bz** pour recompiler le fichier **sendmail.cf** sur le serveur de courrier, puis la commande **refresh -s sendmail** pour appliquer les modifications.

Configuration d'un serveur expéditeur

Pour configurer un expéditeur, utilisez le raccourci Web-based System Manager **wsm network** ou suivez la procédure ci–dessous, qui édite une série de fichiers puis a recours à SMIT ou à la ligne de commande pour démarrer le démon **named**.

1. Editez le fichier /**etc**/**named.conf**. Si le répertoire /**etc** ne contient pas de fichier **named.conf**, copiez-y le fichier-type /**usr**/**samples**/**tcpip**/**named.conf** et éditez-le. Pour en savoir plus et examiner un exemple de fichier de configuration, reportez-vous à la section "named.boot File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   – Insérez une ligne "forwarders" dans la strophe d'options du fichier /**etc**/**named.conf** indiquant toutes les adresses IP des serveurs de noms auxquels des requêtes doivent être expédiées. Par exemple :

   ```
   options {
        ...
        forwarders { 192.100.61.1; 129.35.128.222; };
        ...
   };
   ```

   – Spécifiez la zone d'indices. Par exemple :

   ```
   zone "." IN {
       type hint;
       file "/etc/named.ca";
   };
   ```

2. Editez le fichier /**etc**/**named.ca**. Pour en savoir plus et disposer d'un exemple de fichier cache, reportez-vous à la section "DOMAIN Cache File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   Ce fichier contient l'adresse des serveurs de noms "experts" pour le domaine racine (root) du réseau. Par exemple :

```
; root name servers.
          1          IN    NS     relay.century.com.
relay.century.com.    3600000    IN    A      129.114.1.2
```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

3. Editez le fichier /**etc**/**named.local**. Pour en savoir plus et disposer d'un exemple de fichier de données local, reportez-vous à la section "DOMAIN Local Data File Format for TCP/IP" dans le manuel *AIX Files Reference*.

   a. Spécifiez pour la zone la valeur de SOA (Start Of Authority) et les délais TTL (time-to-live) par défaut. Par exemple :

   ```
   @ IN SOA venus.abc.aus.cntry.com. gail.zeus.abc.aus.cntry.com.
   (
                                1.1     ;serial
                                3600    ;refresh
                                600     ;retry
                                3600000 ;expire
                                86400)  ;minimum
   ```

   b. Spécifiez l'article NS (serveur de noms). Par exemple :

   ```
   IN    NS     venus.abc.aus.century.com.
   ```

   c. Spécifiez l'article PTR (pointeur).

   ```
   1       IN    PTR    localhost.
   ```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

4. Créez un fichier /**etc**/**resolv.conf** via la commande :

   ```
   touch /etc/resolv.conf
   ```

   Ce fichier indique par sa présence que l'hôte doit d'abord faire appel à un serveur de noms pour effectuer une résolution, et non au fichier /**etc**/**hosts**.

   Autrement, le fichier /**etc**/**resolv.conf** peut contenir l'entrée suivante :

   ```
   nameserver 127.0.0.1
   ```

   `127.0.0.1` est l'adresse de bouclage qui, pour l'accès au serveur de noms, dirige l'hôte vers lui-même. Ce fichier /**etc**/**resolv.conf** peut également comporter une ligne du type :

   `domain` *`NomDomaine`*

   Dans cet exemple, *NomDomaine* serait `austin.century.com .`

5. Exécutez l'une des tâches suivantes :

   – Activez le démon **named** :

   ```
   smit stnamed
   ```

   Cette commande initialise le démon à chaque lancement du système. Indiquez quand vous souhaitez lancer le démon **named** : immédiatement, au prochain lancement du système ou les deux.

   – Editez le fichier /**etc**/**rc.tcpip**. Activez le démon **named** en retirant la marque de commentaire (#) de la ligne suivante :

   ```
   #start /etc/named "$src_running"
   ```

   Cette commande initialise le démon à chaque lancement du système.

6. Si vous ne souhaitez pas initialiser le démon named via SMIT, lancez-le pour la session en cours par la commande :

   ```
   startsrc -s named
   ```

Configuration de serveur exclusivement expéditeur

Pour configurer un serveur de noms exclusivement expéditeur, utilisez le raccourci Web-based System Manager **wsm network** ou suivez la procédure ci–dessous, qui édite une série de fichiers puis a recours à SMIT ou à la ligne de commande pour démarrer le démon **named**.

Remarque : : vous pouvez obtenir une configuration similaire sans exécuter de serveur de noms exclusivement expéditeur. il suffit de créer un fichier /**etc**/**resolv.conf** en insérant des lignes de serveur de noms qui pointent vers les serveurs expéditeurs souhaités.

1. Editez le fichier /**etc**/**named.conf**. Si le répertoire /**etc** ne contient pas de fichier **named.conf**, copiez-y le fichier-type /**usr**/**samples**/**tcpip**/**named.conf** et éditez-le. Pour en savoir plus et examiner un exemple de fichier de configuration, reportez-vous à la section ”named.boot File Format for TCP/IP” dans le manuel *AIX Files Reference*.
   – Insérez les lignes ”forwarders” et ”forward only” dans la strophe d’options du fichier /**etc**/**named.conf** indiquant toutes les adresses IP des serveurs de noms auxquels des requêtes doivent être expédiées. Par exemple :

```
options {
    ...
    forwarders { 192.100.61.1; 129.35.128.222; };
    forward only;
    ...
};
```

2. Editez le fichier /**etc**/**named.ca**. Pour en savoir plus et disposer d’un exemple de fichier cache, reportez-vous à la section ”DOMAIN Cache File Format for TCP/IP” dans le manuel *AIX Files Reference*. Ce fichier contient l’adresse des serveurs ”experts” pour le domaine racine (root) du réseau. Par exemple :

```
; root name servers.
         1          IN    NS    relay.century.com.
relay.century.com.   3600000    IN    A     129.114.1.2
```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

3. Editez le fichier /**etc**/**named.local**. Pour en savoir plus et disposer d’un exemple de fichier de données local, reportez-vous à la section ”DOMAIN Local Data File Format for TCP/IP” dans le manuel *AIX Files Reference*.
   a. Spécifiez pour la zone la valeur de SOA (Start Of Authority) et les délais TTL (time-to-live) par défaut. Par exemple :

```
@ IN SOA venus.abc.aus.cntry.com. gail.zeus.abc.aus.cntry.com.
(
                              1.1     ;serial
                              3600    ;refresh
                              600     ;retry
                              3600000 ;expire
                              86400)  ;minimum
```

   b. Spécifiez l’article NS (serveur de noms). Par exemple :

```
IN    NS     venus.abc.aus.century.com.
```

   c. Spécifiez l’article PTR (pointeur).

```
1      IN    PTR    localhost.
```

Remarque : toutes les lignes de ce fichier doivent respecter le format des articles de ressource standard (Standard Resource Record Format).

4. Créez un fichier **/etc/resolv.conf** via la commande :

   ```
   touch /etc/resolv.conf
   ```

   Ce fichier indique par sa présence que l'hôte doit d'abord faire appel à un serveur de noms pour effectuer une résolution, et non au fichier **/etc/hosts**.

   Autrement, le fichier **/etc/resolv.conf** peut contenir l'entrée suivante :

   ```
   nameserver 127.0.0.1
   ```

   `127.0.0.1` est l'adresse de bouclage qui, pour l'accès au serveur de noms, dirige l'hôte vers lui-même. Ce fichier **/etc/resolv.conf** peut également comporter une ligne du type :

   ```
   domain NomDomaine
   ```

   Dans cet exemple, *NomDomaine* serait `austin.century.com .`

5. Exécutez l'une des tâches suivantes :

   – Activez le démon **named** :

   ```
   smit stnamed
   ```

   Cette commande initialise le démon à chaque lancement du système. Indiquez quand vous souhaitez lancer le démon **named** : immédiatement, au prochain lancement du système ou les deux.

   – Editez le fichier **/etc/rc.tcpip**. Activez le démon **named** en retirant la marque de commentaire (#) de la ligne suivante :

   ```
   #start /etc/named "$src_running"
   ```

   Cette commande initialise le démon à chaque lancement du système.

6. Si vous ne souhaitez pas initialiser le démon **named** via SMIT, lancez-le pour la session en cours par la commande :

   ```
   startsrc -s named
   ```

Configuration d'un hôte avec serveur de noms

Vous pouvez configurer un hôte pour un serveur de noms via le raccourci Web-based System Manager **wsm network** ou via l'une des procédures suivantes.

1. Créez un fichier **/etc/resolv.conf**.
2. Si l'hôte est appelé à utiliser plusieurs serveurs de noms, ajoutez ceux-ci à la liste.
3. En supposant que le serveur de noms est opérationnel, vous pouvez tester sa communication avec l'hôte via la commande suivante :

   ```
   host hostname
   ```

   Indiquez un nom d'hôte que le serveur doit résoudre. Si le processus aboutit, vous obtenez un résultat du type :

   ```
   brown.abc.aus.century.com is 129.35.145.95
   ```

D'autres tâches de configuration sont présentées dans le tableau suivant.

Configuration d'un hôte avec serveur de noms		
Raccourci Web-based System Manager, **wsm network** (application wsm network) OU		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Créer un fichier **/etc/resolv.conf**.	**smit stnamerslv2**	créez et éditez **/etc/resolv.conf**[1]

Configuration d'un hôte avec serveur de noms		
Afficher la liste des serveurs utilisés par un hôte	**smit lsnamerslv**	affichez /**etc**/**resolv.conf**
Ajouter un serveur de noms	**smit mknamerslv**	éditez /**etc**/**resolv.conf** [2]
Supprimer un serveur de noms	**smit rmnamerslv**	éditez /**etc**/**resolv.conf**
Activer/Réactiver la résolution DNS	**smit stnamerslv**	
Désactiver la résolution DNS	**smit spnamerslv**	
Modifier/Afficher le domaine	**smit mkdomain**	éditez /**etc**/**resolv.conf**
Supprimer un domaine	**smit rmdomain**	éditez /**etc**/**resolv.conf**

Remarques :

1. Sur la première ligne du fichier /**etc**/**resolv.conf**, entrez le mot `domain` puis le nom complet du domaine auquel appartient l'hôte. Par exemple :

   ```
   domain abc.aus.century.com
   ```

2. Sur une ligne vierge après la ligne introduite par `domain`, entrez `nameserver` suivi d'au moins un espace et de l'adresse Internet (en notation décimale à points) du serveur de noms à ajouter (il doit desservir le domaine indiqué dans l'instruction `domain`). Vous pouvez insérer jusqu'à 16 entrées de serveur de noms. Par exemple, votre fichier /**etc**/**resolv.conf** peut contenir les entrées :

   ```
   nameserver 192.9.201.1
   nameserver 192.9.201.2
   ```

   Le système interroge les serveurs dans l'ordre de leur spécification.

Configuration de zones dynamiques sur le serveur de noms DNS

La commande **named** autorise les mises à jour dynamiques. La base de données nommée et les fichiers de configuration doivent être configurés pour permettre aux machines clientes d'émettre des mises à jour. Une zone peut être dynamique ou statique. La zone par défaut est statique.

Pour rendre une zone dynamique, il faut ajouter le mot clé **allow–update** à la strophe correspondante du fichier /**etc**/**named.conf** file. Ce mot clé précise la liste de correspondances d'adresses Internet définissant les hôtes autorisés à soumettre des mises à jour. Pour en savoir plus et examiner un exemple de fichier de configuration, reportez-vous à la section "named.boot File Format for TCP/IP" dans le manuel *AIX Files Reference*. Dans l'exemple ci–dessous, la mise à jour de la zone dynamique est autorisée à tous les hôtes :

```
zone "aoot.austin.ibm.com" IN {
    type master;
    file "named.data";
    allow-update { any; };
};
```

Sur une zone dynamique, trois modes de sécurité peuvent être définis :

Non sécurisé	N'importe qui peut, à tout moment, mettre à jour les informations de la zone. **Avertissement :** il est déconseillé d'opter pour ce mode. Des données risquent d'être perdues ou interceptées, et l'utilisateur frustré. Il convient au minimum de limiter la mise à jour d'une zone non sécurisée ("unsecured") à des adresses Internet spécifiques.
Contrôlé	Autorise la création d'informations et le remplacement de données existantes. C'est sans doute le mode le plus adapté à un environnement de transition sécurisé. Ce mode requiert également que les données entrantes soient horodatées et munies d'une signature à clé.
Pré–securisé	Impose que les mises à jour remplacent les informations existantes par des informations similaires. Ce mode requiert également que les données entrantes soient horodatées et munies d'une signature à clé.

Par défaut, une zone dynamique se trouve en mode non sécurisé. Pour changer de mode, ajoutez "controlled" ou "presecured" à la suite du mot-clé **update–security**, dans la strophe du fichier /**etc**/**named.conf**, pour informer la commande **named** du niveau de sécurité à appliquer. Par exemple :

```
zone "aoot.austin.ibm.com" IN {
    type master;
    file "named.boot";
    allow-update { any; };
    update-security controlled;
};
```

Une fois le mode sélectionné, les fichiers de données doivent être amenés au niveau de sécurité choisi. En mode non sécurisé, les fichiers de données sont utilisés tels quels. En mode contrôlé ou pré–sécurisé, vous devez créer un ensemble de paires de clés entre noms de serveur maîtres et hôtes pour chaque nom de la zone. Utilisez pour cela la commande **nsupdate** avec l'option **–g**. Cette commande génère la paire de clés, une privée et une publique. Ces clés sont nécessaires pour authentifier les mises à jour. Après avoir créé toutes les clés pour la liste de noms de zones, il faut les ajouter au fichier de données. Le format de clé (KEY) est le suivant :

Index ttl Classe Type IndicClé Protocole Algorithme DonnéesClé

où :

Index	Nom référençant les données de la zone.
ttl	ttl ("time to live") des données. Ce champ est facultatif.
Classe	Classe des données : dépend de la zone, mais généralement IN.
Type	Type de l'enregistrement. Dans ce cas, le type est KEY.
IndicClé	Informations sur la clé. En général, l'enregistrement de clé pour un hôte est sous la forme 0x0000. Le code 0x0100 définit l'enregistrement de clé associé au nom de zone.
Protocole	Protocole à utiliser. Pour le moment, il n'y en a qu'un, `0`.
Algorithme	Algorithme de la clé. Pour le moment, il n'y en a qu'un, `1`. Cette méthode est celle de l'authentification privé/public.
DonnéesClé	Clé exprimée en base 64. La commande **nsupdate** génère les deux clés (publique et privée) en base 64. Dans le fichier de sortie, la clé publique apparaît en dernier.

Exemple

Pour garantir la sécurité d'un nom d'hôte dans une zone dynamique, il faut ajouter au fichier de zone une ligne du type ci–dessous pour la zone contenant ce nom :

```
bears     4660     IN     KEY     0x0000     0     1     AQOtg......
```

Dans cet exemple, `bears` est doté d'un enregistrement KEY défini : toute personne souhaitant mettre à jour `bears` doit signer sa mise à jour avec la clé privée correspondant à la clé publique enregistrée dans la base de données. Pour que la commande **nsupdate** agisse, cette clé privée doit figurer dans un fichier de clé chez le client (fichier /**etc**/**keyfile** par défaut). Son format est le suivant :

NomHôte NomMaître base64 clé

Une entrée similaire KEY doit se trouver dans la section de définition de la zone. **La clé de zone est obligatoire en mode pré–sécurisé ou contrôlé : sans clé, le mode est considéré non sécurisé.** L'exemple `bears` précédent montre comment procéder, mais l'utilisation de clé privée revient à l'administrateur qui utilise la commande **nsupdate** en mode administrateur.

Pour générer une paire de clés avec la commande **nsupdate**, entrez :

nsupdate –g –h *NomZone* **–p** *NomServeur* **–k** *FichierAdmin*

Une clé est générée pour la zone. Placez la dernière clé de la paire au début de la section relative à la zone, comme suit :

```
IN     KEY     0x0100  0  1  Key
```

La zone est prête à être chargée. L'administrateur doit utiliser la clé zone pour appliquer les mises à jour et effectuer des opérations de maintenance sur la zone.

Routage TCP/IP

Cette section traite des points suivants :

Une *route* indique l'itinéraire des paquets à travers le réseau Internet. Elle ne définit pas le parcours complet, mais seulement le segment entre un hôte et une passerelle vers la destination (ou une autre passerelle). Il existe trois types de route :

route hôte	Passerelle capable d'envoyer les paquets vers un hôte ou une passerelle d'un autre réseau.
route réseau	Passerelle capable d'envoyer les paquets vers n'importe quel hôte d'un réseau spécifique.
route par défaut	Passerelle utilisable lorsqu'aucune route hôte ou réseau n'est définie.

Les routes (32 au maximum) sont définies dans la *table de routage* du noyau. Chaque définition donne des informations sur les réseaux accessibles à partir de l'hôte local, les passerelles et le nombre de bonds (distance) requis pour les atteindre. A réception d'un datagramme, la passerelle recherche dans la table de routage l'étape suivante du parcours.

Routage statique ou dynamique

TCP/IP propose deux types de routage : *statique* ou *dynamique*. Avec le routage statique, la table de routage est gérée manuellement à l'aide d'une **commande** de routage. Le routage statique est conseillé lorsqu'un réseau communique avec un ou plusieurs réseaux. Toutefois, si ce type de routage est pratique lorsque la communication se limite à deux ou trois réseaux, il devient fastidieux sur une plus grande échelle, avec la multiplication du nombre de passerelles.

Avec le routage dynamique, ce sont les démons qui mettent à jour la table de routage automatiquement. Les démons de routage reçoivent en permanence les informations émises par d'autres démons de routage, et mettent systématiquement à jour la table de routage en conséquence.

TCP/IP propose deux démons de routage dynamique : **routed** et **gated**. Le démon **gated** gère les protocoles RIP (Routing Information Protocol), RIPng (Routing Information Protocol Next Generation), EGP (Exterior Gateway Protocol), BGP (Border Gateway Protocol) et BGP4+, HELLO (Defense Communications Network Local–Network Protocol), OSPF (Open Shortest Path First), IS–IS (Intermediate System to Intermediate System), ainsi que ICMP et ICMPv6 (Internet Control Message Protocol) / Router Discovery simultanément. Le démon **gated** prend également le protocole SNMP (Simple Network Monitoring Protocol) en charge. Le démon **routed** n'admet que le protocole RIP.

Les démons de routage peuvent fonctionner en mode *passif* ou *actif* (selon l'option définie à leur lancement). En mode actif, ils diffusent périodiquement des informations de routage sur leur réseau local aux passerelles et aux hôtes, et en reçoivent d'eux. En mode passif, ils se limitent à recevoir les informations et ne tiennent pas à jour les passerelles distantes.

Ces deux types de routage sont applicables aux passerelles mais aussi à d'autres hôtes d'un réseau. Les travaux de routage statique fonctionnent de la même façon pour les

passerelles que pour les autres hôtes. Les démons de routage dynamique, toutefois, doivent être exécutés en mode passif (quiet) sur les hôtes qui ne sont pas des passerelles.

Passerelles

Les passerelles sont des types de routeur *: un routeur* interconnecte des réseaux et assure la fonction de routage. Certains routeurs opèrent le routage au niveau de l'interface de réseau ou de la couche physique.

Les passerelles, quant à elles, assurent le routage au niveau de la couche réseau : elles reçoivent les datagrammes IP des autres passerelles, les transmettent aux hôtes du réseau local et acheminent les datagrammes IP d'un réseau à l'autre. Par exemple, une passerelle reliant deux réseaux en anneau à jeton est équipée de deux cartes de réseau en anneau à jeton dotée chacune de sa propre interface de réseau en anneau à jeton. Pour la transmission des informations, la passerelle reçoit les datagrammes via une interface de réseau et les envoie par l'autre. Les passerelles contrôlent périodiquement leurs connexions réseau à partir de messages d'état sur les interfaces.

Pour l'aiguillage des paquets, les passerelles se fondent sur le réseau de destination et non sur l'hôte de destination. Ainsi, elles n'ont pas à garder trace des diverses destinations hôte possibles d'un paquet. Au lieu de cela, elles acheminent les paquets en fonction du réseau de l'hôte de destination. C'est le réseau de destination qui se charge ensuite d'envoyer les paquets à l'hôte de destination. Généralement, une passerelle ne requiert qu'une capacité limitée de stockage disque (éventuellement) et de mémoire centrale.

La distance à parcourir entre l'hôte émetteur et l'hôte destinataire dépend du n à traverser (*nombre de passerelles* à traverser). 0 si la passerelle est rattachée au réseau, 1 si le réseau est accessible via une passerelle, etc. La distance d'un message s'exprime généralement en nombre de passerelles, ou *nombre de bonds* (ou distance *métrique*).

Passerelles intérieures et extérieures

Les passerelles intérieures font partie du même système autonome. Elles communiquent entre elles à l'aide des protocoles RIP (Routing Information Protocol), RIPng (Routing Information Protocol Next Generation), Intermediate System to Intermediate System, OSPF (Open Shortest Path First protocol) ou du protocole HELLO. Les passerelles extérieures appartiennent à des systèmes autonomes distincts. Elles utilisent les protocoles EGP (Exterior Gateway Protocol), BGP (Border Gateway Protocol) ou BGP4+.

Prenons l'exemple de deux systèmes autonomes. Le premier correspond à tous les réseaux administrés par la société Widget. Le second correspond à tous les réseaux administrés par la société Gadget. La société Widget possède une machine pomme, qui est la passerelle de Widget pour Internet. La société Gadget possède une machine orange, qui est la passerelle de Gadget pour Internet. Les deux sociétés possèdent plusieurs réseaux distincts en interne. Les passerelles reliant les réseaux internes sont des passerelles intérieures. Mais les passerelles pomme et orange sont extérieures.

Chaque passerelle extérieure ne communique pas avec toutes les autres passerelles extérieures. En fait, la passerelle extérieure acquiert un ensemble de passerelles limitrophes (les autres passerelles extérieures) avec lesquelles elle communique. Ces passerelles limitrophes ne sont pas définies par une proximité géographique, mais plutôt par les communications qui s'établissent entre elles. Les passerelles limitrophes, à leur tour, possèdent d'autres passerelles limitrophes extérieures. Ainsi, les tables de routage des passerelles extérieures sont mises à jour et les informations de routage sont diffusées vers l'ensemble des passerelles extérieures.

Les informations de routage sont expédiées avec les coordonnées (R,D), R étant le réseau cible et D la distance à parcourir (et donc le coût correspondant) pour l'atteindre. Chaque passerelle indique les réseaux qui lui sont accessibles et le coût de leur accès. La passerelle réceptrice détermine les chemins les plus courts et les indique aux passerelles limitrophes. Ainsi, chaque passerelle extérieure reçoit en continu des informations (et met alors à jour ses tables de routage) qu'elle retransmet aux passerelles limitrophes.

Protocoles de passerelle

Toute passerelle, interne ou externe, communique avec les autres via des protocoles. Voici une présentation succincte des protocoles de passerelle TCP/IP courants :

Protocole HELLO
Le protocole HELLO est utilisé par les passerelles intérieures pour communiquer entre elles. HELLO est chargé de calculer le chemin d'accès le plus court (en durée) aux autres réseaux.

RIP (Routing Information Protocol)
Le protocole RIP est également utilisé par les passerelles intérieures pour communiquer entre elles. Comme le protocole HELLO, RIP calcule le chemin d'accès le plus court aux autres réseaux. A la différence de HELLO cependant, RIP calcule la distance en nombre de sauts, et non en durée. Comme le démon **gated** enregistre toutes les distances métriques en interne en tant que durée, il convertit les nombres de sauts calculés par RIP en durée.

Routing Information Protocol Next Generation
RIPng est le protocole RIP étendu qui permet de gérer IPv6.

OSPF (Open Shortest Path First)
Le protocole OPSF est utilisé par les passerelles intérieures pour communiquer entre elles. Ce protocole de communication est plus approprié que RIP pour les réseaux complexes comprenant plusieurs routeurs. Il fournit un routage multi–itinéraire au même coût.

EGP (Exterior Gateway Protocol)
Les passerelles extérieures utilisent ce protocole pour communiquer entre elles. Le protocole EGP ne calcule par le plus court chemin vers les autres réseaux. Il indique simplement si un réseau particulier est accessible ou non.

BGP (Border Gateway Protocol)
Les passerelles extérieures utilisent ce protocole pour communiquer entre elles. Ce protocole permet l'échange d'informations d'accessibilité entre des systèmes autonomes, mais il fournit davantage de fonctions que le protocole EGP. BGP utilise les attributs de chemin pour fournir des informations supplémentaires sur chaque route afin de sélectionner la plus appropriée.

Border Gateway Protocol 4+
BGP4+ est le protocole BGP version 4, qui gère IPv6 et propose d'autres fonctions étendues par rapport aux versions précédentes.

IS–IS (Intermediate System to Intermediate System)
Les passerelles intérieures utilisent le protocole IS–IS pour communiquer entre elles. Ce protocole de communication permet de router des paquets IP et ISO/CLNP et, comme OSPF, il utilise un algorithme de détection du chemin le plus court pour déterminer les routes les plus rapides.

Planification des passerelles

Avant de configurer les passerelles de votre réseau, vous devez :

1. déterminer le nombre de passerelles nécessaires,
2. décider du type de routage.

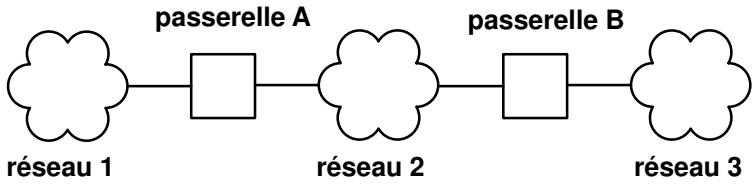
Nombre de passerelles

Le nombre de passerelles nécessaires dépend :

- du nombre de réseaux à connecter,
- du type de connexion des réseaux,

- du niveau d'activité des réseaux connectés.

Par exemple, si les utilisateurs des réseau 1, réseau 2 et réseau 3 doivent tous communiquer ensembles (comme le montre la figure **Exemple de configuration de passerelle**). Pour relier le réseau 1 directement au réseau 2, vous devez utiliser une première passerelle (passerelle A). Pour relier le réseau 2 directement au réseau 3, vous devez utiliser une autre passerelle (passerelle B). Supposons maintenant que les routes appropriées sont déterminées et que tous les utilisateurs des trois réseaux parviennent à communiquer.



Exemple de configuration de passerelle

Cependant, si le réseau 2 est très occupé, les communications entre le réseau 1 et le réseau 3 peuvent s'en trouver ralenties. De plus, si la communication entre ces deux réseaux est la plus importante, il peut être utile de les connecter directement. Pour ce faire, vous devez ajouter deux passerelles supplémentaires, une sur le réseau 1 (passerelle C), l'autre sur le réseau 3 (passerelle D), reliées par une connexion directe. Cette solution n'est peut–être pas suffisante, une passerelle pouvant raccorder plus de deux réseaux.

Un moyen plus efficace peut consister à connecter directement la passerelle A à la passerelle B et au réseau 2, ce qui suppose d'équiper A et B d'une seconde carte réseau. En règle générale, le nombre de connexions réseau assuré par une passerelle est limité au nombre de cartes réseau qu'elle peut prendre en charge.

Type de routage

Si votre réseau est limité et sa configuration relativement fixe, le routage statique est une solution satisfaisante. En revanche, si votre réseau est étendu et sa configuration très variable, il est préférable d'opter pour un routage dynamique. Une solution intermédiaire peut également être envisagée en panachant les routages statique et dynamique. Par exemple, il est possible de définir statiquement certaines routes et d'autoriser la mise à jour d'autres routes par les démons. Les routes statiques créées ne sont ni notifiées aux autres passerelles ni mises à jour par les démons de routage.

Routage dynamique

Déterminez le démon de routage à utiliser en fonction du type de passerelle nécessaire et des protocoles qu'elle peut prendre en charge. S'il s'agit d'une passerelle intérieure et qu'elle ne requiert que le protocole RIP, optez pour le démon **routed**. Sinon, utilisez **gated**.

Remarque : Si les démons **gated** et **routed** sont exécutés sur le même hôte simultanément, des résultats imprévisibles peuvent survenir.

Configuration d'une passerelle

Pour définir une machine comme passerelle, suivez la procédure ci-dessous. Dans un souci de clarté, on suppose que la passerelle doit être connectée à deux réseaux et qu'elle a déjà fait l'objet d'une configuration minimale (reportez-vous à "Configuration TCP/IP minimale", page 3-97) sur un des deux réseaux.

1. Installez et configurez la deuxième carte de réseau, si ce n'est déjà fait. (consultez les sections "Installation d'une carte réseau", page 3-39, "Configuration d'une carte réseau en anneau à jeton haute performance", page 3-39 et "Configuration d'une carte Ethernet haute performance", page 3-39.)

2. Choisissez une adresse IP pour la seconde interface de réseau et configurez l'interface comme indiqué à "Configuration d'une interface de réseau", page 3-55.
3. Ajoutez une route d'accès au second réseau.
4. Pour utiliser une machine AIX comme routeur interréseau sur les réseaux TCP/IP, entrez :

   ```
   no -o ipforwarding=1
   ```

5. La passerelle peut désormais accéder aux deux réseaux directement raccordés.
   a. Pour que le routage statique serve à communiquer avec des hôtes et réseaux en dehors de ces deux réseaux, ajoutez les routes nécessaires.
   b. Pour le routage dynamique, procédez comme indiqué à "Configuration du démon routed", page 3-133 ou "Configuration du démon gated", page 3-133. Si votre interréseau doit rejoindre le réseau Internet, suivez les instructions de la section "Obtention d'un numéro de système autonome", page 3-136.

Configuration d'une passerelle		
Raccourci Web-based System Manager, **wsm network** (application wsm network) OU		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Afficher le tableau de routage	**smit lsroute**	**netstat –rn**[1]
Ajouter une route statique	**smit mkroute**	**route ajoutée** *destination passerelle*[2]
Supprimer une route statique	**smit rmroute**	**route supprimée** *destination passerelle*[2]
Vider la table de routage	**smit fshrttbl**	**route flush**

Remarques :

1. La table est divisée en colonnes, où sont répertoriés l'adresse de destination, l'adresse de passerelle, les indicateurs, le nombre de bonds et l'interface de réseau. Pour la description de ces colonnes, reportez-vous à la commande **netstat** dans le manuel *AIX Commands Reference*. En cas d'échec de livraison de trames, si les tables de routage sont correctes, un ou plusieurs des événements ci-dessous sont probablement en cause :
   – réseau défaillant,
   – passerelle ou hôte distant défaillant,
   – passerelle ou hôte distant en panne, ou non disponible pour réceptionner des trames,
   – hôte distant ne disposant pas de route retour au réseau source.
2. *destination* représente l'adresse ou le nom symbolique de l'hôte ou réseau de destination et *passerelle*, l'adresse ou le nom symbolique de la passerelle. (Une route implicite a 0 comme valeur de destination.)

Sécurité des routes

Les routes peuvent être sécurisées en limitant leur accès à certains utilisateurs. Les restrictions d'accès sont basées sur les ID de groupe primaire et auxiliaire des utilisateurs. Avec la commande **route**, vous pouvez établir une liste de 32 ID groupe maximum et les autoriser ou non à utiliser une route. Si la liste contient des groupes autorisés, n'importe quel utilisateur de n'importe quel groupe a accès à la route. Si au contraire, la liste est

formée de groupes non autorisés, seuls les utilisateurs n'appartenant pas aux groupes de la liste ont accès à la route. L'utilisateur racine a accès à toutes les routes.

En outre, les groupes peuvent être associés à une interface via la commande **ifconfig**. Dans ce cas, tout paquet à expédier peut utiliser n'importe quelle route dont l'accès est autorisé aux groupes associés à son interface en entrée.

Si plusieurs routes ont la même destination, les réceptions de réacheminement ICMP pour cette destination sont ignorés et la recherche de MTU d'accès n'est pas effectuée sur ces routes.

Suppression manuelle de routes dynamiques

Si le démon **routed** est actif, *aucune route supprimée manuellement n'est* remplacée par les informations RIP entrantes (du fait des contrôles d'E/S). Si vous utilisez le démon **gated** sans l'indicateur –n, la route supprimée manuellement *est* remplacée par celle fournie par les informations RIP entrantes.

Configuration du démon routed

Pour configurer le démon **routed** :

1. Supprimez la marque de commentaire (#) et modifiez la clause routed du script shell **/etc/rc.tcpip** : le démon **routed** sera automatiquement activé au lancement du système.
   - Indiquez le mode d'exécution souhaité : actif (indicateur **–s**) ou passif (indicateur**–q**).
   - Activez éventuellement le suivi des paquets (indicateur **–t**). Vous pouvez également le faire pendant l'exécution du démon **routed**, via la commande **kill**. Cette commande communique au démon un signal **SIGUSR1**. Ce signal peut également servir à incrémenter le niveau de suivi sur quatre niveaux. Vous pouvez également désactiver le suivi de paquet pendant l'exécution du démon **routed,** via la commande **kill** : cette commande communique au démon un signal **SIGUSR2**. Pour en savoir plus, reportez-vous au démon **routed** et à la commande **kill**.
   - Activez éventuellement la mise au point (indicateur **–d**). Précisez alors également le fichier journal dans lequel consigner les informations de mise au point (ou indiquez que vous souhaitez les diriger vers l'écran de la console).
   - Indiquez si vous exécutez le démon **routed** sur une passerelle (indicateur **–g**).

   Remarque : Un hôte non passerelle peut exécuter **routed**, mais en mode passif uniquement.
2. Identifiez tous les réseaux connus en les répertoriant dans le fichier **/etc/network.** Pour plus de détails, reportez-vous à la section "Networks File Format for TCP/IP" dans le manuel *AIX Files Reference*. Un exemple du fichier **networks** est proposé dans le répertoire **/usr/samples/tcpip**.
3. Définissez dans le fichier **/etc/gateways** les routes d'accès à toutes les passerelles connues qui ne sont pas directement connectées à votre réseau. Reportez-vous à la section "Gateways File Format for TCP/IP" dans le manuel *AIX Files Reference* pour des exemples détaillés d'entrées de fichier **/etc/gateways.** Un exemple du fichier **gateways** est proposé dans le répertoire **/usr/samples/tcpip**.

   Attention : N'exécutez pas le démon **routed** et le démon **gated** sur la même machine. Des résultats imprévisibles pourraient survenir.

Configuration du démon gated

Procédez comme suit :

1. Déterminez les protocoles de passerelle appropriés pour votre système. Vous pouvez utiliser les protocoles de routage EGP, BGP, RIP, RIPng, HELLO, OSPF, ICMP/Router Discovery ou IS–IS. Vous pouvez également prévoir le protocole SNMP, qui permet

d'afficher et de modifier à partir d'un hôte distant les informations de gestion d'un élément de réseau.

Remarque : Utilisez les protocoles EGP, BGP ou BGP4+ pour notifier les adresses des réseaux d'un système autonome aux passerelles des autres systèmes autonomes. Si vous faites partie du réseau Internet, EGP, BGP, or BGP4+ doivent être appliqués pour notifier le système de passerelles noyau de l'accessibilité du réseau. Utilisez les protocoles de routage interne pour communiquer les informations d'accessibilité à l'intérieur d'un système autonome.

2. Identifiez tous les réseaux connus en les répertoriant dans le fichier /**etc**/**network.** Pour plus de détails, reportez-vous à la section "Networks File Format for TCP/IP" dans le manuel *AIX Files Reference*. Un exemple du fichier **networks** est proposé dans le répertoire /**usr**/**samples**/**tcpip**.
3. Modifiez le fichier /**etc**/**gated.conf** pour intégrer la configuration souhaitée pour le démon **gated**.
   a. Indiquez le niveau de suivi souhaité. S'il doit débuter avant l'analyse du fichier **gated.conf**, spécifiez l'indicateur **–t** pour activer le suivi au lancement du démon. Pour plus de détails, reportez-vous à la section "gated Daemon" dans le manuel *AIX Commands Reference*.
   b. Indiquez les protocoles de routage souhaités. Vous devez spécifier une instruction par protocole. Supprimez la marque de commentaire (#) et modifiez les instructions correspondant aux protocoles à utiliser.
      – Avec EGP :
        – Insérez la clause `autonomoussystem`. Demandez un numéro de système autonome à Internet si vous êtes sur Internet, sinon, attribuez vous-même ce numéro en fonction des numéros sur votre réseau.
        – Positionnez la clause EGP sur `yes`.
        – Insérez une clause `group` pour chaque système autonome.
        – Insérez une clause `neighbor` pour chaque passerelle limitrophe dans ce système autonome. Par exemple :

```
autonomoussystem 283 ;

egp yes {
         group maxup 1 {
              neighbor nogendefault 192.9.201.1 ;
              neighbor nogendefault 192.9.201.2 ;
        } ;
        group {
              neighbor 192,10.201.1 ;
              neighbor 192,10.201.2 ;
        } ;
} ;
```

      – Avec RIP ou HELLO :
        – Positionnez l'instruction RIP ou HELLO sur `yes`.
        – Dans l'instruction RIP ou HELLO, spécifiez `quiet` pour que la passerelle se contente de recevoir des informations de routage, mais n'en diffuse pas. Sinon, spécifiez `supplier` pour qu'elle puisse recevoir et diffuser ces informations.
        – Spécifiez `pointopoint` pour que la passerelle ne diffuse les informations qu'aux passerelles source figurant dans l'instruction `sourcegateways`. Sinon, n'indiquez rien. Si vous incluez la valeur `pointopoint` , vous

devez spécifier un nom de passerelle ou une adresse Internet (en notation décimale à points) dans la clause `sourcegateways`. Par exemple :

```
# Notification à des passerelles spécifiques

rip/hello pointopoint {
          sourcegateways
                101.25.32.1
                101.25.32.2 ;
} ;

# Broadcast to all

rip/hello supplier {
         interface en0 noripout ;
         trustedgateways
                101.25.33.1
                101.25.33.2 ;
} ;
```

Ces deux premiers exemples peuvent être activés simultanément dans le fichier **gated.conf**.

```
# Diffusion à aucun utilisateur

rip/hello quiet {
         interface tr0 noripin ;
} ;
```

- Avec BGP :
  - Insérez la clause `autonomoussystem`. Demandez un numéro de système autonome à Internet si vous êtes sur Internet, sinon, attribuez vous-même ce numéro en fonction des numéros sur votre réseau.
  - Positionnez la clause BGP sur `yes`.
  - Insérez une clause `peer` pour chaque passerelle limitrophe dans ce système autonome. Par exemple :

```
# Exécuter toutes les opérations BGP

bgp yes {
        peer 192.9.201.1 ;
} ;
```

- Avec SNMP :
  - Positionnez la clause SNMP sur `yes`.

```
snmp yes;
```

Configuration du démon gated pour l'exécution de IPv6

Pour configurer le démon **gated** pour l'exécution avec IPv6 (Internet Protocol version 6), vérifiez d'abord que votre système est configuré pour IPv6 et le routage IPv6 :

1. Exécutez **autoconf6** pour configurer automatiquement vos interfaces pour IPv6.
2. Configurez les adresses locales de chaque interface IPv6 sur laquelle vous voulez utiliser le routage IPv6, via la commande :

   `ifconfig` *`interface`* `inet6 fec0:`*`n`*`::`*`address`*`/64 alias`

   où

   interface est le nom de l'interface, comme `tr0` ou `en0` .

   n est un nombre décimal quelconque, par exemple `11`

address est la portion de l'interface IPv6 qui suit les deux colonnes, par exemple, avec l'adresse IPv6 `fe80::204:acff:fe86:298d` , l'entrée *d'adresse* serait `204:acff:fe86:298d` .

Remarque : La commande **netstat –i** permet d'afficher votre adresse IPv6 pour chaque interface configurée.

Ainsi, si l'anneau à jeton `tr0` est associé à l'adresse IPv6 `fe80::204:acff:fe86:298d` , entrez la commande :

```
ifconfig tr0 inet6 fec0:13::204:acff:fe86:298d/64 alias
```

3. Pour activer le réacheminement IPv6, utilisez la commande :

```
no –o ip6forwarding=1
```

4. Pour lancer **ndpd–router**, utilisez la commande :

```
ndpd–router –g
```

Affichez **ndpd–router** pour déterminer les indicateurs à utiliser dans votre configuration réseau.

Si vous lancez **ndpd–router**, votre système pourra être utilisé comme routeur pour le protocole Neighbor Discovery Protocol. Les routeurs Neighbor Discovery Protocol communiquent les informations de routage aux hôtes Neighbor Discovery afin qu'ils acheminent les paquets IPv6.

Tout hôte du réseau devant appartenir au réseau IPv6 doit exécuter **ndpd–host**. Les hôtes du réseau qui exécutent **ndpd–host** se reconnaîtront comme appartenant à un réseau IPv6 et utiliseront par conséquent le protocole Neighbor Discovery Protocol. Ce protocole leur permet de déterminer et de contrôler les adresses de communication, non seulement pour autoriser le routage limitrophe, mais aussi pour rechercher les routeurs limitrophes afin de réacheminer les paquets.

Pour plus d'informations, reportez–vous aux sections **ndpd–router**, **ndpd–host**, ou consultez RFC 1970, *Neighbor Discovery*.

Ensuite, configurez le démon gated :

1. Déterminez les protocoles de passerelle IPv6 appropriés pour votre système. Vous pouvez utiliser les protocoles de routage IPv6 BGP4+ (Border Gateway Protocol étendu pour IPv6) et RIPng (Routing Information Protocol Next Generation).
2. Modifiez le fichier /**etc**/**gated.conf** pour intégrer la configuration souhaitée pour le démon **gated**.

   Remarque : AIX versions 4.3.2 et ultérieures exécutent **gated** version 3.5.9. La syntaxe du fichier **gated.conf** est légèrement modifiée par rapport aux versions précédentes. Pour connaître la syntaxe appropriée, reportez–vous à la documentation **gated.conf** ou utilisez le fichier exemple disponible dans le répertoire /**usr**/**sample**/**tcpip**.

   Pour configurer BGP4+ ou RIPng, utilisez les adresses IPv6 dont la syntaxe spécifie une adresse IP.

Remarque : Par défaut, le protocole RIPng envoie des paquets à plusieurs destinataires.

Dès que le fichier /**etc**/**gated.conf** a été modifié, le démon **gated** peut être lancé.

Obtention d'un numéro de système autonome

Si vous utilisez EGP ou BGP, il est recommandé de solliciter auprès du NIC un *numéro de système autonome* officiel pour votre passerelle. Coordonnées : INFO@INTERNIC.NET ou 1-800-444-4345 (USA).

Recherche de MTU d'accès

Pour deux hôtes communiquant via un chemin d'accès à des réseaux multiples, les paquets transmis sont fragmentés si leur taille dépasse celle de la plus petite MTU d'un réseau quelconque du chemin d'accès. La fragmentation étant susceptible de réduire les performances du réseau, il suffit, pour l'éviter, de transmettre des paquets de taille inférieure ou égale à celle de la plus petite MTU du chemin d'accès du réseau : vous faites alors appel à la MTU d'accès.

Sous AIX, un algorithme de recherche de MTU d'accès est pris en charge tel que défini dans le RFC 1191. Pour l'activer pour les applications TCP et UDP, modifiez les options **tcp_pmtu_discover** et **udp_pmtu_discover** de la commande **no**. Quand elle est activée pour TCP, la recherche de MTU d'accès impose automatiquement aux paquets transmis par les applications TCP une taille ne dépassant pas la MTU d'accès. Les applications UDP déterminent elles-mêmes la taille de leurs paquets transmis : aussi doivent-elles être configurées pour utiliser l'information de MTU d'accès via l'option socket **IP_FINDPMTU**, même si l'option **udp_pmtu_discover no** est activée. Les options **tcp_pmtu_discover** et **udp_pmtu_discover** sont désactivées par défaut.

Une fois la MTU d'accès trouvée pour une route de réseau, une route hôte distincte est "clonée" pour le chemin d'accès. Vous pouvez afficher les routes hôte "clonées" et la valeur MTU d'accès pour la route avec la commande **netstat –r**. L'accumulation des routes "clonées" peut être évitée en permettant l'expiration et la suppression des routes inutilisées. L'option **route_expire** de la commande **no** contrôle l'expiration des routes ; elle est désactivée par défaut.

Les routes pouvant être modifiées dynamiquement, les valeurs MTU d'accès peuvent également changer dans le temps. La diminution de ces valeurs étant susceptible de provoquer la fragmentation de paquets, ces valeurs sont analysées régulièrement (toutes les 10 minutes par défaut). Vous pouvez modifier la fréquence d'analyse avec l'option **pmtu_default_age** de la commande **no**.

L'augmentation des valeurs MTU d'accès peut accroître les performances du réseau. Les valeurs trouvées sont donc analysées régulièrement pour y rechercher une augmentation (toutes les 30 minutes par défaut). Vous pouvez modifier la fréquence d'analyse avec l'option **pmtu_rediscover_interval** de la commande **no**.

Si tous les routeurs du chemin d'accès au réseau n'admettent pas le RFC 1191, déterminer la valeur MTU d'accès exacte peut s'avérer impossible. Dans ce cas, la commande **mmtu** permet d'entériner ou non les valeurs testées.

Remarque :

1. Sur les routes en double et sur celles définies avec **group routing**, la recherche de MTU d'accès n'est pas possible.
2. Avec la recherche de MTU d'accès activée, l'option **arpqsize** de la commande **no** a sa valeur minimale définie à 5. Si, par la suite, la recherche de MTU d'accès est désactivée, cette valeur n'est pas diminuée.

Protocole SLIP

Configuration de SLIP pour modem

Pour configurer un protocole SLIP entre deux systèmes communiquant via un modem, vous pouvez utiliser le raccourci Web-based System Manager **wsm network** ou la procédure suivante, qui fait appel à SMIT et à la ligne de commande. Les deux hôtes sont appelés bronze et gold.

1. Connectez physiquement les modems à bronze et gold.
2. Pour créer un tty sur bronze via SMIT :
   a. Entrez :

   ```
   smit maktty
   ```

   b. Sélectionnez **rs232** comme type de tty.
   c. Sélectionnez un port série disponible, par exemple **sa0** (port série système 1).
   d. Sélectionnez dans la liste un numéro de port pour le tty.
   e. Définissez le débit (en bauds) de votre modem.
   f. Désactivez l'option Activation de la connexion.
   g. Quittez SMIT.
3. Créez un tty sur gold.

   Suivez la même procédure que pour bronze (étape 2), excepté pour l'option Activation de la connexion, qui doit être activée (**enable**).

   Dans la suite de la procédure, le numéro tty de bronze et de gold est supposé être tty1.
4. Testez la connexion physique avec ATE.
   a. Côté bronze, entrez :

   ```
   ate
   ```

   b. Dans le MENU PRINCIPAL (ETAT NON CONNECTE), sélectionnez **Alter**. Indiquez, en bauds, le débit de votre modem (Rate), et tty1 comme unité (Device).
   c. Dans le MENU PRINCIPAL (ETAT NON CONNECTE), sélectionnez **Connect**. Lorsque vous y êtes invité par ATE, composez le numéro d'appel de gold et appuyez sur Entrée.
   d. A ce stade, vous devez recevoir une invite de connexion pour gold.
   e. Enfin, à partir de l'écran connecté, déconnectez-vous de gold, appuyez sur **Ctrl–v** (pour appeler le MENU PRINCIPAL (ETAT CONNECTE), entrez **t** pour mettre fin à la connexion, puis **q** pour quitter ATE.

   Remarque : Si vous ne recevez pas d'invite de connexion, revenez à l'étape 1 et vérifiez la configuration. Ne poursuivez qu'une fois la connexion établie avec gold.

   La configuration de tty pour ATE est légèrement différente de celle pour SLIP. Pour cette raison, vous devez apporter les modifications suivantes :

   a. Côté bronze, entrez :

   ```
   smit chgtty
   ```

   b. Côté gold, entrez :

   ```
   smit chgtty-pdisable tty1
   ```

   Sélectionnez **tty1**, puis **Modification/affichage d'un programme TTY**. Désactivez l'option Activation de la connexion puis quittez SMIT.

5. Insérez la ligne suivante dans le fichier /**usr**/**lib**/**uucp**/**Devices** de bronze et de gold :

   ```
   Direct tty1 - 9600 direct
   ```

   ou remplacez `9600` par tout autre débit de modem.

6. Créez une interface de réseau SLIP sur bronze.

   a. Entrez :

   ```
   smit mkinet1sl
   ```

   b. Pour le port TTY de l'interface de réseau SLIP, sélectionnez **tty1**.

   c. Spécifiez une *adresse Internet* , par exemple 130.130.130.1.

   d. Spécifiez une adresse de *destination* (de gold), par exemple 130.130.130.2.

   e. Spécifiez le débit (en *bauds*) de votre modem.

   f. Spécifiez la *chaîne de numérotation*, par exemple :

      – "" AT OK ATDT555-1234 CONNECT ""

      – Cette commande signifie : utiliser `tty1` à `9 600` bauds. Envoyez AT au modem. Le modem doit répondre OK. Composez le numéro d'appel `555-1234` . Le modem doit répondre CONNECTE. Les espaces avant et après les doubles guillemets sont obligatoires.

   g. Quittez SMIT.

7. Créez une interface de réseau SLIP sur gold.

   Suivez la même procédure que pour bronze (étape 5), mais en inversant les adresses Internet et de destination.

8. Ajoutez les deux lignes ci-dessous dans le fichier /**etc**/**hosts** de bronze et de gold :

   ```
   130.130.130.1   bronze
   130.130.130.2   gold
   ```

   Le nom attribué doit être unique. Autrement dit, si le nom `bronze` est déjà attribué à l'interface de réseau en anneau à jeton de l'hôte bronze, choisissez-en un autre pour l'interface SLIP, tel que `bronze_slip`.

   Remarque : Le script `/usr/sbin/slipcall.` fournit une interface simplifiée pour la commande **slattach**.

9. Testez la connexion SLIP.

   a. Côté bronze, entrez :

   ```
   ping gold
   ```

   b. Côté gold, entrez :

   ```
   ping bronze
   ```

   Si les deux tests aboutissent, la connexion SLIP peut être utilisée. Sinon, revenez à l'étape 5 et vérifiez la configuration sur bronze et sur gold.

Configuration de SLIP pour câble de modem nul

Pour configurer un protocole SLIP entre deux systèmes communiquant via un câble de modem nul, vous pouvez utiliser le raccourci Web-based System Manager **wsm network** ou la procédure suivante, qui fait appel à SMIT et à la ligne de commande. Les deux hôtes sont appelés bronze et gold.

1. Reliez physiquement bronze et gold par un câble de modem nul. Les câbles suivants vous sont nécessaires. (Ils sont répertoriés dans l'ordre de leur connexion, du bronze au gold.)
   a. Câble B (référence 00G0943, par exemple). Câble de raccordement port série : livrés avec chaque système (sauf pour certains modèles qui ne le requièrent pas).
   b. Câble D (référence 6323741, code 2936 par exemple). Câble asynchrone EIA-232/V.24.
   c. Câble E (référence 59F2861, code 2937 par exemple). Interposeur imprimante/terminal EIA-232 (câble de modem nul).
   d. Carte échangeur (prises des deux côtés).
2. Créez un tty sur bronze.
   a. Entrez :

   ```
   smit maktty
   ```

   b. Sélectionnez **rs232** comme type de tty.
   c. Sélectionnez un port série disponible, par exemple **sa0** (port série système 1).
   d. Sélectionnez dans la liste un numéro de port pour le tty.
   e. Fixez le débit, en bauds, à19200 (vous le passerez ultérieurement à 38400).
   f. Désactivez l'option Activation de la connexion puis quittez SMIT.
3. Créez un tty sur gold.

   Suivez la même procédure que pour bronze (étape 2), excepté pour l'option Activation de la connexion, qui doit être activée (**enable**).

   Remarque : Dans la suite de la procédure, le numéro tty de bronze et de gold est supposé être tty1.
4. Testez la connexion physique avec ATE.
   a. Côté bronze, entrez :

   ```
   ate
   ```

   b. Dans le MENU PRINCIPAL (ETAT NON CONNECTE), sélectionnez **Alter**. Indiquez 19200 comme débit (Rate) et tty1 comme unité (Device).
   c. Dans le MENU PRINCIPAL (ETAT NON CONNECTE), sélectionnez **Connect**. Lorsque vous y êtes invité par ATE, à composer un numéro de téléphone, appuyez sur Entrée. Le message suivant doit s'afficher :

   ```
   ate: 0828-010 La commande Connect a établi une connexion via le
   port tty1
   ```

   d. Appuyez sur Entrée. Vous devez recevoir une invite de connexion pour gold. Connectez-vous.
   e. Enfin, à partir de l'écran connecté, déconnectez-vous de gold, appuyez sur **Ctrl–v** (pour appeler le MENU PRINCIPAL (ETAT CONNECTE), entrez **t** pour mettre fin à la connexion, puis **q** pour quitter ATE.

   Remarque : Si vous ne recevez pas d'invite de connexion, revenez à l'étape 1 et vérifiez la configuration. Ne poursuivez qu'une fois la connexion établie avec gold.

La configuration de tty pour ATE est légèrement différente de celle pour SLIP. Pour cette raison, vous devez apporter les modifications suivantes :

a. Côté bronze, entrez :

```
smit chgtty
```

Sélectionnez **tty1**. Fixez le débit en bauds à 38400 puis quittez SMIT.

b. Côté gold, entrez :

```
pdisable tty1
```

c. Côté gold, entrez :

```
smit chgtty
```

Sélectionnez **tty1**. Désactivez l'option Activation de la connexion, fixez le débit (en bauds) à 38400, puis quittez SMIT.

5. Insérez la ligne suivante dans le fichier /**usr**/**lib**/**uucp**/**Devices** de bronze et de gold :

```
Direct tty1 - 38400 direct
```

6. Créez une interface de réseau SLIP sur **bronze**.

a. Entrez :

```
smit mkinet1sl
```

b. Pour le port TTY de l'interface de réseau SLIP, sélectionnez **tty1**.

c. Spécifiez l'adresse Internet, par exemple 130.130.130.1.

d. Spécifiez l'adresse de destination (de gold), par exemple 130.130.130.2, puis appuyez sur Entrée.

7. Créez une interface de réseau SLIP sur gold.

Suivez la même procédure que pour bronze (étape 5), mais en inversant les adresses Internet et de destination.

8. Ajoutez les deux lignes ci-dessous dans le fichier /**etc**/**hosts** de bronze et de gold :

```
130.130.130.1   bronze
130.130.130.2   gold
```

Le nom attribué doit être unique. Autrement dit, si le nom `bronze` est déjà attribué à l'interface de réseau en anneau à jeton de l'hôte bronze, choisissez-en un autre pour l'interface SLIP, tel que `bronze_slip`.

9. Lancez SLIP sur bronze et gold.

Entrez :

```
slattach tty1
```

10. Testez la connexion SLIP.

a. Côté bronze, entrez :

```
ping gold
```

b. Côté gold, entrez :

```
ping bronze
```

Si les deux tests aboutissent, la connexion SLIP peut être utilisée. Sinon, revenez à l'étape 5 et vérifiez la configuration sur bronze et sur gold.

Désactivation d'une connexion SLIP

Pour désactiver une connexion SLIP :

1. Entrez :

   ```
   ps -ef | grep slatt
   ```

   Relevez le numéro des process associés à la commande **slattach**.

2. Pour chaque numéro de process, entrez :

   ```
   kill numéro_process
   ```

   N'utilisez pas l'indicateur **–9** de la commande **kill**.

   Si l'indicateur **–9** est malencontreusement associé à la commande **slattach**, un verrou slip est susceptible d'être resté dans /etc/locks. Supprimez-le pour le nettoyage post-**slattach**.

Suppression d'un TTY

Pour retirer un tty, vous disposez du raccourci Web-based System Manager **wsm network** ou du raccourci SMIT **smit rminet**.

Protocole asynchrone point-à-point (PPP)

Le sous–système asynchrone PPP (Point–to–Point Protocol) offre une alternative à SLIP, en proposant une méthode standard pour le transport des datagrammes multiprotocoles au travers de supports point–à–point. PPP se compose de trois couches principales :

1. Une méthode d'encapsulage des datagrammes multiprotocoles. AIX PPP prend en charge les protocoles de couche réseau TCP/IP.
2. Un protocole LCP (Link Control Protocol) qui établit, configure et teste la connexion de liaison de données. AIX PPP l'implémente via des extensions de noyau.
3. Une famille de protocoles NCP (Network Control Protocols) pour établir et configurer différents protocoles de couche réseau. AIX PPP prend en charge le protocole IPCP (Internet Protocol Control Protocol) pour négocier une connexion TCP/IP.

AIX PPP prend en charge les RFC (Request for Comments) suivants :

- RFC 1661, "The Point-to-Point Protocol, LCP."
- RFC 1332, "The PPP Internet Protocol Control Protocol (IPCP)."
- RFC 1662, "PPP in HDLC-like Framing."
- RFC 1334, "PPP Authentication Protocols."
- RFC 1990, "PPP Multilink"

AIX PPP différencie client et serveur. Un système AIX peut être à la fois client et serveur : la distinction n'a pour but que de simplifier la configuration. Les serveurs PPP tentent d'affecter un pool d'adresses IP parmi les connexions en cours d'établissement. Il existe une corrélation entre les unités de support : AIX PPP la rompt. Toutes les connexions PPP serveur sont affectées sur la base du "premier disponible", ceci pour faciliter la séparation entre PPP et le support. Le processus de raccordement doit demander à être lié au type de liaison adéquat.

Processus utilisateur

Le protocole asynchrone PPP sur AIX utilise trois niveaux de processus utilisateur :

1. Un démon de contrôle (**pppcontrold**) exécuté par la racine sous le contrôleur SRC (System Resource Controller) (**startsrc -s pppcontrold**). Ce démon assure le chargement et la configuration de toutes les extensions de noyau associées au sous-système. Il reste actif aussi longtemps que PPP est requis par le système d'exploitation.
2. Un processus de liaison (**pppattachd**) qui associe un flot TTY à une instance du protocole de contrôle de liaison NPC (Network Control Protocol), et un protocole datagramme. Il existe une instance de **pppattachd** pour chaque connexion PPP active dans le système. Tout utilisateur du processus de liaison doit appartenir au groupe **uucp** et comporter /**usr**/**sbin** dans sa variable d'environnement **PATH**.
3. Un processus de numérotation (**pppdial**) qui établit une connexion sortante. Le numéroteur est conçu pour être exécuté avec **pppattachd** comme programme connecteur. Son objet est d'interagir au travers de l'unité asynchrone avant la négociation PPP. Cette interaction est définie de la même façon que le format du dialogue chat UUCP. Le numéroteur aide à établir une connexion avec un système distant. L'établissement effectif de la session est hors de la portée de PPP.

Configuration du protocole asynchrone PPP

Vous pouvez configurer le protocole asynchrone PPP à l'aide de Web-based System Manager ou de SMIT. Toutes les opérations de configuration sont indiquées dans le tableau ci-après. Ces opérations sont accessibles à l'utilisateur racine.

Pour la configuration initiale de votre système, vous aurez à :

- Ajouter une configuration de liaison
- ajouter une interface de serveur (si vous définissez la machine en tant que serveur PPP),
- ajouter une interface de demande (si vous souhaitez que la machine accepte les connexions à la demande),
- manipuler les utilisateurs/mots de passe PAP ou CHAP(si vous désirez que la machine gère l'authentification PPP),
- lancer PPP pour prendre les modifications en compte (ou arrêter puis relancer PPP si ce protocole est actif).

Configuration du protocole PPP asynchrone	
Raccourci Web-based System Manager, (application wsm network) OU	**wsm network**
Tâche	*Raccourci SMIT*
Création d'une configuration de contrôle de liaison	**smit ppplcp**
Ajouter une configuration de liaison	**smit addlcp**
Modifier/afficher une configuration de liaison	**smit chglcp**
Supprimer une configuration de liaison[1]	**smit rmlcp**
Créer des interfaces IP PPP	**smit pppip**
Ajouter une interface serveur	**smit addpppserver**
Modifier/afficher une interface serveur	**smit listserver**
Supprimer une interface serveur[1]	**smit rmlistserver**
Ajouter une interface de demande	**smit addpppdemand**
Modifier/afficher une interface de demande	**smit listdemand**
Supprimer une interface de demande[1]	**smit rmlistdemand**
Manipuler les utilisateurs/mots de passe PAP	**smit ppppap**
Ajouter un utilisateur PAP	**smit addpapuser**
Modifier/afficher un utilisateur PAP	**smit listpapuser**
Supprimer un utilisateur PAP	**smit rmpapuser**
Manipuler les utilisateurs/mots de passe CHAP	**smit pppchap**
Ajouter un utilisateur CHAP	**smit addchapuser**
Modifier/afficher un utilisateur CHAP	**smit listchapuser**
Supprimer un utilisateur CHAP	**smit rmchapuser**
Lancer PPP[2]	**smit startppp**
Arrêter PPP[3]	**smit stopppp**

Remarques :

1. Sélectionner cette opération fait disparaître les informations existantes.
2. Lancer le protocole PPP est également possible avec la commande **startsrc –s pppcontrold**. En outre, via l'interface SMIT, vous pouvez demander que ce protocole soit lancé à l'amorçage du système.
3. Arrêter le protocole PPP est aussi possible avec la commande **stopsrc –s pppcontrold**. Par ailleurs, via SMIT, vous pouvez demander que ce protocole ne soit pas démarré à l'amorçage du système.

Protocoles PPP et SNMP

L'interaction de PPP avec le démon TCP/IP SNMP permet d'obtenir les informations relatives à la configuration de la couche de liaison PPP, et celles concernant les interfaces LCP (Link Control Protocol). Dans la mesure où la configuration de TCP/IP SNMP et du logiciel de gestion de SNMP est correcte, PPP SNMP peut :

- rechercher les informations sur la configuration de la liaison PPP (Maximum Receive Unit size, Asynchronous Character Mapping, etc.)
- définir les informations de configuration de la liaison PPP ;
- rechercher les informations relatives à l'interface LCP pour les liaisons LCP actives ;
- passer l'état des liaisons LCP actives à "down" en définissant l'objet **ifAdminStatus** approprié dans la base MIB (Management Information Base).

Tous les objets définis dans le RFC 1471 pour la MIB PPP ne sont pas pris en charge. Seul le tableau **pppLink** s'applique au sous-sytème AIX PPP : les parties **pppLqr** et **pppTests** ne sont donc pas prises en charge. La partie **pppLink** est prise en charge, excepté les objets suivants :

- L'objet **pppLinkConfigMagicNumber** est accessible seulement en lecture. Dans AIX PPP, la négociation de numéros magiques est toujours exécutée et ne peut être désactivée.
- L'objet **pppLinkConfigFcsSize** est accessible seulement en lecture. AIX PPP n'accepte que la taille 16 pour FCS.

Activation de PPP SNMP

SNMP pour PPP est désactivé par défaut. Vous pouvez activer PPP SNMP via le raccourci Web-based System Manager **wsm network** ou via la procédure suivante. Cette procédure est accessible à l'utilisateur racine.

Remarque : La configuration de liaison PPP est supposée définie avant d'entamer cette procédure. Sinon, exécutez la procédure décrite à la section "Configuration du protocole asynchrone PPP", page 3-144.

1. Lancez l'interface SMIT et affichez l'écran Change/Show a Link Configuration avec la commande :

   ```
   smit chglcp
   ```

2. Basculez sur yes le champ Enable PPP SNMP subagent.
3. Validez vos modifications et quittez SMIT.

PPP SNMP sera activé au prochain redémarrage du protocole PPP.

- Si PPP est en cours d'utilisation :
  a. Arrêtez-le avec le raccourci **smit stopppp** (voir le tableau à la sectionConfiguration du protocole asynchrone PPP, page 3-144).
  b. Vérifiez régulièrement où en est l'arrêt complet du sous-système, via la commande :

     ```
     lssrc -s pppcontrold
     ```

     Le temps que prend l'arrêt complet dépend du nombre de liaisons défini dans la configuration PPP. L'état `inoperative` renvoyé par la commande ci-dessus signifie que le sous-système est complètement arrêté.
  c. Démarrez-le avec le raccourci **smit startppp** (voir le tableau à la section Configuration du protocole asynchrone PPP, page 3-144).
- Si PPP n'est pas en cours d'utilisation, lancez-le via le raccourci **smit startppp** (voir le tableau à la section Configuration du protocole asynchrone PPP, page 3-144).

Normes QoS (Qualité du service) TCP/IP

Les normes QoS (Quality of Service) sont une famille de normes Internet qui offrent un mode de traitement préférentiel de certains types de trafic IP. Ces normes peuvent réduire les délais d'attente variables et la congestion ayant pour effet de limiter les performances du réseau. AIX offre une prise en charge des normes QoS au niveau de l'hôte afin de répartir le trafic vers l'extérieur en classes de service distinctes. Ces normes permettent également d'indiquer et de faire des réservations de ressources telles que l'exigent les applications des clients.

Les normes QoS peuvent être utilisées par un organisme pour déployer et mettre en place des politiques de gestion du réseau régissant l'utilisation de la largeur de bande du réseau. Avec les normes QoS, un hôte AIX peut procéder aux opérations suivantes :

- Réguler le volume d'un certain type de trafic au sein du réseau ;
- Marquer des paquets sélectionnés en fonction d'un certain type de politique afin que les routeurs puissent par la suite fournir le service demandé ;
- Prendre en charge des services, tels que le service virtuel de lignes spécialisées avec une prise en charge appropriée des normes QoS le long de la route ;
- Participer aux requêtes de réservation de ressources des destinataires et annoncer les sessions expéditrices disponibles pour ces requêtes.

La prise en charge des normes QoS par AIX offre les fonctions suivantes :

- Services différenciés tels que définis dans la norme RFC 2474
- Politique de gestion du trafic
- Marquage des paquets à l'intérieur et hors du profil
- Conception du trafic
- Mesure
- Services intégrés pour applications client et serveur tels que définis dans la norme RFC 1633
- Signalisation RSVP (RFC 2205)
- Service garanti (RFC 2212)
- Service de contrôle de charge (RFC 2211)
- Mise en réseau conformément à la politique en vigueur
- Bibliothèque RAPI partagée destinée aux applications

Le sous–système de normes QoS pour AIX se compose de quatre éléments :

Extension du noyau QoS (/usr/lib/drivers/qos)
L'extension du noyau QoS réside dans le répertoire **/usr/lib/drivers/qos** ; elle est chargée et déchargée à l'aide des méthodes de configuration **cfgqos** et **ucfgqos**. Cette extension de noyau permet la prise en charge QoS sur l'hôte AIX.

Agent de politique (/usr/sbin/policyd)
L'agent de politique est un démon de niveau utilisateur qui réside dans **/usr/sbin/policyd**. Il prend en charge la gestion de la politique et sert d'interface avec l'extension du noyau QoS afin d'installer, de modifier et de supprimer les règles de politique. Les règles de politique peuvent être définies dans le fichier de configuration local (**/etc/policyd.conf**) ou récupérées dans le serveur de réseau central à l'aide de LDAP ou de ces deux méthodes réunies.

Agent RSVP (/usr/sbin/rsvpd)
L'agent RSVP est un démon de niveau utilisateur qui réside dans **/usr/sbin/rsvpd**. Il met en œuvre la sémantique de protocole de signalisation RSVP.

Bibliothèque partagée RAPI (/usr/lib/librapi.a)
Les applications peuvent utiliser la RSVP API (RAPI) pour une meilleure qualité de service telle que définie par le modèle QoS Internet de services intégrés (Integrated Services Internet QoS model). Cette bibliothèque dialogue avec l'agent RSVP local afin de diffuser la requête QoS le long du chemin emprunté par le flux de données à l'aide du protocole RSVP. Cette API est une norme ouverte.

Remarque : la prise en charge de QoS pour AIX est basée sur un ensemble de normes Internet en constante évolution et des ébauches de normes en cours d'élaboration par l'Engineering Task Force (IETF) ainsi que ses divers groupes de travail. Les efforts de normalisation au sein de l'IETF permettront d'améliorer la cohérence et la définition de cette technologie. Il est également à noter que la QoS est une nouvelle technologie Internet récemment déployée au sein de ce réseau. Elle présente de nombreux avantages à tous les stades de son déploiement. Toutefois, les services bout en bout ne peuvent être offerts qu'avec une prise en charge totale de la technologie QoS.

Modèles QoS

Les modèles QoS pour Internet sont des normes ouvertes définies par l'IETF. Deux de ces modèles sont en cours de normalisation au sein de l'IETF: *Services intégrés* et *Services différenciés*. Ceux–ci renforcent le modèle traditionnel de service optimisé décrit dans la norme RFC 1812.

Services intégrés

Le service IS (Services intégrés) est un modèle dynamique de réservation des ressources pour Internet, tel que décrit dans la norme RFC 1633. Les hôtes utilisent un protocole de signalisation appelé Resource ReSerVation Protocol (RSVP) pour demander au réseau, de manière dynamique, une qualité de service spécifique. Les paramètres QoS sont acheminés dans ces messages RSVP et chaque nœud de réseau le long du chemin installe ces paramètres afin de disposer de la qualité de service requise. Ces paramètres QoS décrivent l'un des deux services actuellement définis, à savoir le service garanti et le service de contrôle de charge. L'IS se caractérise par le fait que cette signalisation porte sur chaque flux de trafic et que les réservations s'appliquent à chaque bond sur le chemin. Bien que ce modèle soit tout à fait à même de répondre à l'évolution constante des applications, il persiste encore certains problèmes en termes d'évolutivité qui empêchent son déploiement sur des réseaux au sein desquels des routeurs uniques gèrent plusieurs flux simultanés.

Services différenciés

Le service DS (Services différenciés) résout les problèmes d'évolutivité par flux et par bond par le biais d'un mécanisme simple de classification des paquets. Plutôt qu'une approche de signalisation dynamique, le service DS privilégie l'utilisation de bits dans l'octet TOS (type de service) IP afin de répartir les paquets en classes. Ce modèle de bit particulier dans l'octet TOS IP est appelé point de code DS. Il est utilisé par les routeurs pour définir la qualité de service fournie au niveau de ce bond en particulier, se rapprochant par là–même de leur mode d'acheminement IP par le biais de la consultation des tables de routage. Le traitement d'un paquet avec un point de code DS particulier s'appelle le PHB (per–hop behavior). Il est géré indépendamment à chaque nœud de réseau. La concaténation de ces différents PHB indépendants offre un service bout en bout.

Les services différenciés (DS) sont en cours de normalisation par un groupe de travail IETF, qui a défini trois PHB : le PHB avec acheminement expéditif (EF : abréviation de Expedited Forwarding), le groupe PHB avec acheminement assuré (AF : abréviation de Assured Forwarding) et le PHB par défaut (DE : abréviation de par défaut). Le EF PHB peut être utilisé pour la mise en œuvre d'un service bout en bout, telle qu'une ligne spécialisée (VLL) offrant un délai d'attente et un taux d'instabilité faibles ainsi que des pertes réduites. L'AF est une famille de PHB, appelé groupe de PHB. Il est utilisé pour classer des paquets en fonction des différents niveaux de priorité. Le niveau de priorité attribué à un paquet détermine son importance relative au sein de la classe AF. Par ce biais, il est possible de bénéficier du service dit *Olympique*, à savoir bronze, argent et or. Le DE PHB est le modèle traditionnel de service optimisé tel que normalisé par la RFC 1812.

Normes prises en charge et ébauches de normes

Les ébauches de normes Internet et les RFC suivants traitent des normes sur lesquelles s'appuie la mise en œuvre des modèles QoS AIX.

RFC 2474	Définition du champ Services différenciés (champ DS) dans les en–têtes IP versions 4 et 6
RFC 2475	Architecture des services différenciés
RFC 1633	Présentation des services intégrés au sein de l'architecture Internet
RFC 2205	Protocole de réservation des ressources (RSVP)
RFC 2210	Utilisation du RSVP avec les services intégrés IETF
RFC 2211	Spécification du service d'éléments réseau avec contrôle de charge
RFC 2212	Spécification de la qualité de service garantie
RFC 2215	Paramètres de définition généraux des éléments réseau des services intégrés
draft–ietf–diffserv–framework–01.txt, octobre 1998	Cadre des services différenciés
draft–ietf–diffserv–rsvp–01.txt, novembre 1998	Cadre d'utilisation du RSVP avec des réseaux DIFF–serv
draft–ietf–diffserv–phb–ef–01.txt	Groupe PHB d'acheminement expéditif
draft–ietf–diffserv–af–04.txt	Groupe PHB d'acheminement assuré
draft–rajan–policy–qosscheme–00.txt, octobre 1998	Schéma des services différenciés et intégrés au sein des réseaux
draft–ietf–rap–framework–01.txt, novembre 1998	Cadre pour contrôle d'admission [25] basé sur des règles de politique
draft–ietf–rap–rsvp–ext–01.txt, novembre 1998	Extensions RSVP pour contrôle de politique

Remarque : la QoS est une nouvelle technologie Internet récemment déployée au sein de ce réseau. Elle présente de nombreux avantages à tous les stades de son déploiement. Toutefois, les services bout en bout ne peuvent être offerts qu'avec une prise en charge totale de la technologie QoS.

Installation de QoS

QoS for AIX est livré avec **bos.net.tcp.server**. L'installation de ces fichiers est indispensable pour utiliser QoS. Pour utiliser la bibliothèque RAPI partagée, installez aussi **bos.adt.include**.

Configuration de QoS

Arrêt et démarrage du sous–système QoS AIX

QoS peut être lancé ou arrêté avec le raccourci SMIT (**smit qos**) ou les commandes **mkqos** et **rmqos**.

Pour désactiver dès à présent le sous–système QoS et lors du prochain redémarrage du système, procédez comme suit :

```
/usr/sbin/rmqos –B
```

Pour activer le sous–système QoS pour la période en cours seulement, procédez comme suit :

```
/usr/sbin/mkqos –N
```

Reportez–vous à la description des commandes **mkqos** et **rmqos** pour le lancement et le retrait des indicateurs de commande.

Les démons **policyd** et **rsvpd** sont configurés par les fichiers de configuration /**etc**/**policyd.conf** et /**etc**/**rsvpd.conf**. Ces fichiers *doivent* être édités afin de personnaliser le sous–système QoS en fonction de l'environnement local. QoS ne fonctionne pas correctement avec les configurations type fournies.

Configuration de l'agent RSVP

L'agent RSVP est nécessaire si l'hôte doit prendre en charge le protocole du même nom. Utilisez le fichier de configuration /**etc**/**rsvpd.conf** pour configurer l'agent RSVP. La syntaxe de ce fichier est précisée dans le fichier de configuration type installé dans /**etc**/**rsvpd.conf**.

Configuration type

```
interface 1.2.3.1
interface 1.2.3.2 disabled
interface 1.2.3.3 disabled
interface 1.2.3.4
    {
      trafficControl
    }
rsvp 1.2.3.1
    {
      maxFlows 64
    }
rsvp 1.2.3.4
    {
      maxFlows 100
    }
```

L'exemple ci–dessus illustre une possibilité de configuration RSVP au sein de laquelle l'hôte AIX a 4 interfaces (virtuelles ou physiques) représentées par les 4 adresses IP : `1.2.3.1`, `1.2.3.2`, `1.2.3.3`, et `1.2.3.4`.

L'interface `1.2.3.1` a été activée pour le RSVP. Toutefois, la fonction de contrôle du trafic n'a pas été spécifiée et les messages RESV RSVP entrants n'entraînent pas la réservation des ressources au sein du sous–système TCP AIX. Cette interface peut prendre en charge un maximum de 64 sessions RSVP simultanées.

Les interfaces `1.2.3.2` et `1.2.3.3` ont été désactivées. L'agent RSVP ne peut pas utiliser cette interface pour transmettre ni recevoir des messages RSVP.

L'interface `1.2.3.4` a été activée pour le RSVP. En outre, elle peut procéder à des réservations de ressources au sein du sous–système TCP AIX en réponse à un message RESV RSVP. Cette interface peut prendre en charge jusqu'à 100 sessions RSVP.

Toutes les autres interfaces existantes sur l'hôte mais non reprises de manière explicite dans /**etc**/**rsvpd.conf** sont désactivées.

Configuration de l'agent de politique

L'agent de politique est un composant indispensable du sous–système QoS AIX. Utilisez le fichier /**etc**/**policyd.conf** pour configurer l'agent de politique. La syntaxe de ce fichier est précisée dans le fichier de configuration type installé dans /**etc**/**policyd.conf**.

Configurations type

Dans l'exemple suivant, une catégorie de service de qualité est créée et utilisée dans la règle de politique tcptraffic. Cette catégorie de service a une vitesse de transmission maximum de 110 000 Kbps, une profondeur de compartiment à jeton de 10 000 bits et une valeur TOS IP sortante de 11100000 en système binaire. La règle de politique tcptraffic offre ce service de qualité à l'ensemble du trafic. L'adresse IP source est fournie par `1.2.3.6`, l'adresse de destination par `1.2.3.3` et le port de destination par des valeurs situées entre 0 et 1024. Cette règle ne s'applique que de 8 heures à 11 heures (heure locale).

Les instructions suivantes définissent une catégorie de services par défaut et l'utilisent pour réduire le trafic UDP provenant des interfaces `1.2.3.1` à `1.2.3.4` vers les adresses IP `1.2.3.6` à `1.2.3.10`, port 8000.

```
ServiceCategories  premium
    {
       PolicyScope     DataTraffic
       MaxRate         110000
       MaxTokenBucket  10000
       OutgoingTOS     11100000
    }

ServicePolicyRules   tcptraffic
    {
       PolicyScope    DataTraffic
       Direction      Outgoing
       Permission     Allowed
       ProtocolNumber 6  # tcp
       TimeOfDayRange          8:00-23:00
       SourceAddressRange      1.2.3.6-1.2.3.6
       DestinationAddressRange 1.2.3.3-1.2.3.3
       DestinationPortRange    0-1024
       ServiceReference        premium
    }
```

La configuration type ci–après peut être utilisée pour télécharger des règles à partir d'un serveur LDAP à l'aide du nom de sous–arborescence spécifique,

```
ou=NetworkPolicies,o=myhost.mydomain.com,c=us
```

afin de consulter les politiques sur l'hôte du serveur LDAP.

```
ReadFromDirectory
{
  LDAP_Server   1.2.3.27
  Base          ou=NetworkPolicies,o=myhost.mydomain.com,c=us
}
```

Identification des problèmes au niveau du QoS

La commande **qosstat** peut être utilisée pour afficher des informations d'état relatives aux politiques actives installées dans le sous–système QoS. Ces informations peuvent vous être utiles afin de détecter la présence d'un problème lors du débogage de la configuration QoS. Utilisez **qosstat** pour produire le rapport suivant.

```
Action:
  Token bucket rate (B/sec): 10240
  Token bucket depth (B): 1024
  Peak rate (B/sec): 10240
  Min policied unit (B): 20
  Max packet size (B): 1452
  Type: IS-CL
  Flags: 0x00001001 (POLICE,SHAPE)

  Statistics:
    Compliant packets: 1423 (440538 bytes)

  Conditions:
    Source address       Dest address          Protocol
    192.168.127.39:8000  192.168.256.29:35049  tcp (1connection)

Action:
  Token bucket rate (B/sec): 10240
  Token bucket depth (B): 1024
  Peak rate (B/sec): 10240
  Outgoing TOS (compliant): 0xc0
  Outgoing TOS (non-compliant): 0x00
  Flags: 0x00001011 (POLICE,MARK)
  Type: DS

  Statistics:
    Compliant packets: 335172 (20721355 bytes)
    Non-compliant packets: 5629 (187719 bytes)

  Conditions:
    Source address        Dest address       Protocol
    192.168.127.39:80     *:*                tcp (1 connection)
    192.168.127.40:80     *:*                tcp (5 connections)
```

Référence QoS

Commandes

- **qosstat**
- **mkqos**
- **rmqos**

Méthodes

- **cfgqos**
- **ucfgqos**

Sécurité TCP/IP

En fonction des contraintes du domaine, l'administrateur système doit assurer un certain niveau de protection (par exemple, pour répondre à la politique de sécurité de son entreprise). Ou encore, l'accès à certains systèmes publics doit être étroitement contrôlé. Ces niveaux de sécurité peuvent s'appliquer au réseau, au système d'exploitation, au logiciel d'application et aux programmes développés par l'administrateur.

Cette section décrit le dispositif de sécurité fourni avec TCP/IP, en mode standard et sécurisé, et développe certaines notions de sécurité propres à l'environnement réseau.

Cette section traite des points suivants :

Système de protection du système d'exploitation

La plupart des fonctions de protection proposées pour TCP/IP sont calquées sur celles du système d'exploitation. En voici les grandes lignes.

Contrôle d'accès

Le dispositif de sécurité appliqué au réseau prolonge celui du système d'exploitation :

- Authentification de l'utilisateur
- Authentification de la connexion
- Protection des échanges de données

L'authentification de l'utilisateur s'opère au niveau de l'hôte distant via un mot de passe et un nom d'utilisateur (identiques à ceux déclinés par l'utilisateur lors de la connexion au système local). Les commandes TCP/IP sécurisées, telles que **ftp**, **rexec** et **telnet**, subissent les mêmes contraintes et contrôles que celles du systèmes d'exploitation.

L'authentification de connexion vise à contrôler l'identité et l'adresse IP de l'hôte distant. Ainsi, tout risque d'usurpation d'identité par un hôte distant est évité.

La protection des échanges permet d'importer/exporter des données à un niveau de sécurité spécifique, entre des cartes réseau dotées de droits et de protections identiques. Il peut s'agir de données confidentielles sur cartes avec niveau de protection maximal, par exemple.

Audit

L'audit de réseau réalisé via le sous–système **audit** qui s'applique aux routines de réseau noyau et aux programmes d'application, consigne toutes les actions touchant à la sécurité.

L'audit s'applique aux événement suivants :

Evénements au niveau noyau

- Changement de configuration
- Changement d'ID hôte
- Changement de route
- Connexion

- Création d'une prise (socket)
- Exportation d'objets
- Importation d'objets

Evénements au niveau application

- Accès au réseau
- Changement de configuration
- Changement d'ID hôte
- Changement de route statique
- Configuration du courrier
- Connexion
- Exportation de données
- Importation de données
- Consignation de courrier dans un fichier

Toute création et suppression d'objets subit un audit de la part du système d'exploitation. Les enregistrements d'audit au niveau application interrompent et relancent l'audit pour éviter toute redondance avec l'audit du noyau.

Base NTCB

La base NBTB (Network Trusted Computing Base) est un module logiciel et matériel dédié à la protection du réseau. Les dispositifs matériels sont fournis par les cartes réseau utilisées avec TCP/IP. Le logiciel étant constitué exclusivement de processus sécurisés et des fichiers associés.

Chemin d'accès sécurisé, shell sécurisé et clé SAK

Le système d'exploitation prévoit un *chemin d'accès sécurisé* pour empêcher tout programme non autorisé de lire des données à partir d'un terminal utilisateur. Ce chemin est utilisé pour les communications confidentielles avec le système (par exemple, pour la modification de mots de passe ou l'entrée en communication). Un *shell sécurisé* (**tsh**) est également proposé, qui n'exécute que les programmes sécurisés, testés et contrôlés comme tels. TCP/IP prend tous ces dispositifs en charge, de même que la clé SAK (*Secure Attention Key*) dont le rôle est de mettre en place l'environnement pour une communication sécurisée entre vous et le système. La clé SAK locale est accessible dès l'utilisation de TCP/IP. Par ailleurs, la commande **telnet** donne accès à une clé SAK distante.

La clé SAK locale offre les mêmes fonctions sous **telnet** et sous d'autres programmes d'application du système : elle met fin au processus **telnet** et à tout autre processus associé au terminal exécutant **telnet**. Toutefois, sous **telnet**, vous pouvez envoyer une demande de chemin d'accès sécurisé au système distant via la commande **telnet send sak** (en mode commande **telnet**). Vous pouvez définir une seule clé pour l'émission d'une requête SAK à l'aide de la commande **telnet set sak**.

Système de protection de TCP/IP

Certains composants du système de protection sont spécifiques de TCP/IP. Ce sont des commandes TCP/IP et des processus sécurisés TCP/IP, qui renforcent, pour TCP/IP, le système de sécurité du système d'exploitation.

Protection des commandes TCP/IP

Certaines commandes TCP/IP ont pour but de fournir un environnement sécurisé durant l'exploitation. Il s'agit de **ftp**, **rexec** et **telnet**. La fonction **ftp** concerne les transferts de

données. La commande **rexec** s'applique à l'exécution des commandes sur un hôte étranger. La commande **telnet** (TELNET) a trait à la connexion sur un hôte étranger.

Ces commandes n'offrent une sécurité que lors de leur exécution. C'est–à–dire qu'elles ne définissent pas d'environnement sécurisé pour l'exécution d'autres commandes. Pour protéger votre système lors de l'exécution d'autres opérations, faites appel à la commande **securetcpip**. Cette commande permet de protéger le système en désactivant les applications et démons non sécurisés et en autorisant la protection du protocole de réseau en couches IP.

Les commandes **ftp**, **rexec**, **securetcpip** et **telnet** fournissent les garanties suivantes :

securetcpip **securetcpip** active le système de protection de TCP/IP. L'accès aux commandes non sécurisé est supprimé du système à l'émission de cette commande. Les commandes suivantes sont supprimées par l'exécution de la commande **securetcpip** :

- **rlogin** et **rlogind**
- **rcp**, **rsh** et **rshd**
- **tftp** et **tftpd**
- **trpt**

securetcpip permet de hisser le système du niveau de sécurité standard au niveau de sécurité maximal. Dès lors, vous n'aurez à réexécuter **securetcpip** que si vous réinstallez TCP/IP.

ftp **ftp** Fournit un environnement sécurisé pour le transfert de fichiers. Lorsqu'un utilisateur appelle la commande **ftp** vers un hôte étranger, il est invité à fournir un ID de connexion (un ID de connexion par défaut, l'ID de connexion courant de l'utilisateur sur l'hôte local, est proposé) et un mot de passe pour l'hôte distant.

Le processus de connexion automatique recherche, dans le fichier **$HOME/.netrc** de l'utilisateur local, l'ID et le mot de passe à soumettre à l'hôte étranger. Pour plus de sécurité, les droits d'accès au fichier **$HOME/.netrc** doivent être fixés à 600 (lecture et écriture réservées au propriétaire). A défaut, la connexion automatique échoue.

> **Remarque :** Le fichier **.netrc** impose de stocker les mots de passe dans un fichier non chiffré. C'est pourquoi la connexion automatique par **ftp** n'est pas disponible si le système est configuré avec **securetcpip**. Pour la réactiver, supprimez la commande **ftp** de la strophe `tcpip:` du fichier **/etc/security/config**.

Le transfert de fichiers via **ftp** suppose deux connexions TCP/IP : une pour le protocole et une pour le transfert des données. La connexion au protocole, principale, est une connexion fiable car établie sur des ports de communication fiables. La connexion secondaire, dédiée au transfert des données proprement dit, doit être établie sur les mêmes hôtes local et distant que la première (condition vérifiée sur chacun des hôtes). Faute de quoi, la commande **ftp** émet un message d'erreur indiquant que la connexion n'a pas été authentifiée, puis s'arrête. Ce contrôle vise à éviter qu'un hôte tiers n'intercepte des données qui ne lui sont pas destinées.

rexec La commande **rexec** s'applique à l'exécution des commandes sur un hôte étranger. L'utilisateur est invité à décliner son ID de connexion et son mot de passe.

Avec le dispositif de connexion automatique, la commande **rexec** recherche, dans le fichier **$HOME/.netrc** de l'utilisateur local, l'ID et le mot de passe à soumettre à l'hôte étranger. Pour plus de sécurité, les droits d'accès au fichier **$HOME/.netrc** doivent être fixés à 600 (lecture et écriture réservées au propriétaire). A défaut, la connexion automatique échoue.

> **Remarque :** Le fichier **.netrc** impose de stocker les mots de passe dans un fichier non chiffré. C'est pourquoi la connexion automatique par **rexec** n'est pas disponible si le système est exploité en mode sécurisé. Pour la réactiver, supprimez l'entrée **rexec** de la strophe `tcpip:` du fichier **/etc/security/config**.

telnet ou **tn** **telnet** (TELNET) fournit un environnement sécurisé à la connexion sur un hôte étranger. L'utilisateur est invité à décliner son ID de connexion et son mot de passe. Le terminal de l'utilisateur est considéré comme directement connecté à l'hôte : l'accès au terminal est contrôlé par des bits d'autorisation. Les autres utilisateurs (groupe et autres) n'ont pas accès en lecture au terminal, mais ils peuvent y écrire des messages si le propriétaire les y autorise. La commande **telnet** donne également accès au shell sécurisé du système distant via la clé SAK (Secure Attention Key). Cette clé, qui peut être définie par la commande **telnet**, doit être différente de celle utilisée pour appeler le chemin d'accès sécurisé local.

Exécution de commandes à distance (/etc/hosts.equiv)

Les utilisateurs répertoriés dans le fichier **/etc/hosts.equiv** peuvent exécuter certaines commandes sur votre système sans fournir de mot de passe.

Opérations relatives aux hôtes distants autorisés à exécuter des commandes		
Raccourci Web-based System Manager, (application wsm network) OU	**wsm network**	
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Afficher la liste	**smit lshostsequiv**	affichez **/etc/hosts.equiv**
Ajouter un hôte	**smit mkhostsequiv**	*éditez **/etc/hosts.equiv**
Supprimer un hôte	**smit rmhostsequiv**	*éditez **/etc/hosts.equiv**

Pour en savoir plus sur les procédures relatives aux fichiers signalées par un astérisque (*), reportez-vous à "hosts.equiv File Format for TCP/IP" dans le manuel *AIX Files Reference*.

Restrictions d'accès FTP (/etc/ftpusers)

Les utilisateurs répertoriés dans le fichier **/etc/ftpusers** sont protégés contre l'accès FTP à distance. Par exemple, supposons que l'utilisateur bob est connecté à un système distant et qu'il connaît le mot de passe de l'utilisateur carl sur votre système. Si carl figure dans le fichier **/etc/ftpusers**, bob ne pourra pas transférer des fichiers via FTP de ou vers le compte de carl, bien qu'il connaisse son mot de passe.

Opérations relatives aux utilisateurs protégés		
Raccourci Web-based System Manager, **wsm network** (application wsm network) OU		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Afficher la liste	**smit lsftpusers**	affichez /**etc**/**ftpusers**
Ajouter un utilisateur	**smit mkftpusers**	*éditez /**etc**/**ftpusers**
Supprimer un utilisateur	**smit rmftpusers**	*éditez /**etc**/**ftpusers**

Pour en savoir plus sur les procédures relatives aux fichiers signalées par un astérisque (*), reportez-vous à ”ftpusers File Format for TCP/IP” dans le manuel *AIX Files Reference*.

Processus sécurisés

Un processus (ou programme) sécurisé est un script shell, un démon ou un programme conforme aux normes de sécurité établies et révisées par des organismes agréés (aux USA, le ministère de la défense), qui certifient également certains programmes sécurisés.

A ces programmes sont associés différents niveaux de sécurité : A1, B1, B2, B3, C1, C2 et D (A1 étant le niveau maximal), satisfaisant chacun à des critères spécifiques. Par exemple, le niveau C2 intègre les aspects suivants :

intégrité des programmes	Le processus accomplit de façon sûre toutes ses fonctions, ni plus, ni moins.
modularité	Le code source du processus est fractionné en modules qui ne sont pas directement impliqués ou accessibles par d’autres modules.
principe du moindre privilège	Les activités utilisateur se déroulent toujours au niveau le plus faible : un utilisateur habilité à lire un fichier ne peut le modifier par inadvertance.
réutilisation d’objet limitée	Un utilisateur ne peut pas, par exemple, utiliser accidentellement une section de mémoire qui porte un indicateur d’écrasement mais n’a pas encore été vidée et peut contenir des informations importantes.

TCP/IP contient de nombreux démons sécurisés et non sécurisés. Les démons sécurisés sont certifiés conformes aux normes de sécurité.

On trouve parmi les démons sécurisés :

- **ftpd**
- **rexecd**
- **telnetd**

On trouve parmi les démons non sécurisés :

- **rshd**
- **rlogind**
- **tftpd**

Un système n’est sécurisé que s’il est exploité en association avec une base informatique sécurisée. Autrement dit, chaque hôte doit correspondre à une machine sécurisée et, sur un réseau, tous les serveurs de fichiers, passerelles et autres hôtes doivent être sécurisés.

Base NTCB

Le réseau intègre des mécanismes matériels et logiciels pour mettre en oeuvre les dispositifs de sécurité. Cette section définit les différents composants de la base NTCB (Network Trusted Computing Base) en relation avec TCP/IP. Les dispositifs matériels sont fournis par les cartes réseau utilisées avec TCP/IP.

Ces cartes sont programmées pour contrôler les données entrantes : elles ne peuvent recevoir que les données destinées au système local, et ne peuvent diffuser que celles recevables par tous les systèmes.

Le module logiciel de NTCB est constitué exclusivement de programmes sécurisés. Les programmes et fichiers associés sont répertoriés ci-dessous (par répertoires) :

Répertoire /etc				
Nom	**Propriétaire**	**Groupe**	**Mode**	**Droits d'accès**
gated.conf	root	system	0664	rw–rw–r—
gateways	root	system	0664	rw–rw–r—
hosts	root	system	0664	rw–rw–r—
hosts.equiv	root	system	0664	rw–rw–r—
inetd.conf	root	system	0644	rw–r—r—
named.conf	root	system	0644	rw–r—r—
named.data	root	system	0664	rw–rw–r—
networks	root	system	0664	rw–rw–r—
protocols	root	system	0644	rw–r—r—
rc.tcpip	root	system	0774	rwxrwxr—
resolv.conf	root	system	0644	rw–rw–r—
services	root	system	0644	rw–r—r—
3270.keys	root	system	0664	rw–rw–r—
3270keys.rt	root	system	0664	rw–rw–r—

Répertoire /usr/bin				
Nom	**Propriétaire**	**Groupe**	**Mode**	**Droits d'accès**
host	root	system	4555	r–sr–xr–x
hostid	bin	bin	0555	r–xr–xr–x
hostname	bin	bin	0555	r–xr–xr–x
finger	root	system	0755	rwxr–xr–x
ftp	root	system	4555	r–sr–xr–x
netstat	root	bin	4555	r–sr–xr–x
rexec	root	bin	4555	r–sr–xr–x
ruptime	root	system	4555	r–sr–xr–x
rwho	root	system	4555	r–sr–xr–x
talk	bin	bin	0555	r–xr–xr–x
telnet	root	system	4555	r–sr–xr–x

Répertoire /usr/sbin				
Nom	**Propriétaire**	**Groupe**	**Mode**	**Droits d'accès**
arp	root	system	4555	r–sr–xr–x
fingerd	root	system	0554	r–xr–xr––
ftpd	root	system	4554	r–sr–xr––
gated	root	system	4554	r–sr–xr––
ifconfig	bin	bin	0555	r–xr–xr–x
inetd	root	system	4554	r–sr–xr––
named	root	system	4554	r–sr–x––
ping	root	system	4555	r–sr–xr–x
rexecd	root	system	4554	r–sr–xr––
route	root	system	4554	r–sr–xr––
routed	root	system	0554	r–xr–x–––
rwhod	root	system	4554	r–sr–xr––
securetcpip	root	system	0554	r–xr–xr––
setclock	root	system	4555	r–sr–xr–x
syslogd	root	system	0554	r–xr–xr––
talkd	root	system	4554	r–sr–xr––
telnetd	root	system	4554	r–sr–xr––

Répertoire /usr/ucb				
Nom	**Propriétaire**	**Groupe**	**Mode**	**Droits d'accès**
tn	root	system	4555	r–sr–xr–x

Répertoire /var/spool/rwho				
Nom	**Propriétaire**	**Groupe**	**Mode**	**Droits d'accès**
rwho (répertoire)	root	system	0755	drwxr–xr–x

Protection des données

Le dispositif de sécurité sous TCP/IP ne chiffre pas les données transmises par le réseau. Il est donc recommandé de prendre des mesures pour prévenir tout risque de défaillance du système de sécurité pouvant révéler des mots de passe ou des informations confidentielles.

L'utilisation de ce produit dans un environnement relevant du ministère de la défense (Department of Defense - DOD - aux Etats-Unis) requiert la conformité aux normes de sécurité DOD 5200.5 et NCSD-11.

Identification des incidents TCP/IP

Cette section traite du diagnostic des incidents courants en environnement TCP/IP.

La commande **netstat** est très utile pour localiser un incident. Une fois la zone en cause isolée, vous disposez d'outils plus précis : commandes **netstat -i** et **netstat -v** pour déterminer si l'incident se situe au niveau d'une interface matérielle, puis programmes de diagnostics pour mieux cerner les causes de l'incident. Ou bien, si la commande **netstat -s** a détecté des erreurs de protocole, vous pouvez utiliser la commande **trpt** ou **iptrace.**

Cette section traite des points suivants :

Incidents de communication

Si vous ne parvenez pas à communiquer avec un hôte de votre réseau :

- Essayez de contacter l'hôte à l'aide de la commande **ping**. Lancez la commande **ping** sur l'hôte local pour vérifier que l'interface locale reliée au réseau est opérationnelle et active.
- Tentez de résoudre le nom de l'hôte avec la commande **host**. Si vous n'y parvenez pas, vous avez un problème de résolution de noms. Reportez-vous à "Incidents de résolution de noms", page 3-160.

Si le nom est résolu et que l'hôte à contacter se trouve sur un autre réseau, il s'agit peut-être de difficultés de routage : reportez-vous à "Incidents de routage", page 3-162.

- Sur un réseau en anneau à jeton, vérifiez si l'hôte cible réside sur un autre anneau. Dans l'affirmative, il est probable que le champ `allcast` soit mal renseigné. Pour accéder au menu des interfaces de réseau, vous pouvez utiliser le raccourci Web-based System Manager **wsm network** ou SMIT **smit chinet**. Spécifiez ensuite **no** dans le champ Confine Broadcast to Local Ring to du menu SMIT pour réseau en anneau à jeton.
- Si un grand nombre de paquets ARP transitent sur le réseau, vérifiez que votre masque de sous–réseau est correctement défini, faute de quoi vous vous trouvez en présence d'un conflit de diffusion pouvant affecter les performances de votre système.

Incidents de résolution de noms

Les routines de résolution exécutées sur des hôtes TCP/IP tentent de résoudre les noms en en faisant appel successivement et dans cet ordre :

1. au serveur de noms DOMAIN (**named**),
2. NIS (Network Information Services),
3. au fichier /**etc**/**hosts** local.

Lors de l'installation de NIS+, les préférences de recherche sont définies dans le fichier **irs.conf**. Pour plus d'informations, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

Hôte client

En cas d'échec de résolution d'un nom d'hôte avec le fichier /**etc**/**hosts** (réseau plat), vérifiez que ce fichier contient le nom d'hôte et l'adresse IP correcte.

En cas d'échec de résolution d'un nom d'hôte avec un serveur de noms :

1. Vérifiez que le fichier **resolv.conf** contient le nom du domaine et l'adresse Internet d'un serveur de noms.
2. Vérifiez que le serveur de noms local est opérationnel en émettant la commande **ping** avec l'adresse IP du serveur (relevée dans le fichier **resolv.conf** local).
3. Si le serveur de noms est opérationnel, vérifiez que le démon **named** sur votre serveur de noms local est actif en émettant la commande **lssrc –s named** sur le serveur de noms.
4. Si vous exécutez **syslogd**, recherchez les éventuels messages d'erreur journalisés. (la sortie des messages est définie dans le fichier /**etc**/**syslog.conf**).

Si ces opérations ne permettent pas d'identifier l'incident, examinez l'hôte serveur de noms.

Hôte serveur de noms

En cas d'échec de résolution d'un nom d'hôte :

1. Vérifiez que le démon **named** est actif :

   ```
   lssrc -s named
   ```

2. Vérifiez que l'adresse de l'hôte cible existe dans la base de données du serveur de noms et qu'elle est correcte. Envoyez un signal SIGINT au démon **named** pour placer un cliché de la base de données et de la mémoire cache dans le fichier /**var**/**tmp**/**named_dump.db**. Vérifiez que l'adresse que vous tentez de résoudre s'y trouve et est correcte.

   Ajoutez ou corrigez les informations de résolution nom-adresse dans le fichier de données hôte **named** du serveur de noms maître du domaine. Puis, exécutez la commande SRC ci-dessous pour relire les fichiers de données :

   ```
   refresh -s named
   ```

3. Vérifiez que les demandes de résolution de noms ont été traitées. Pour ce faire, lancez le démon **named** à partir de la ligne de commande et spécifiez le niveau de mise au point (de 1 à 9) sachant que plus le niveau est élevé, plus le mécanisme de mise au point consigne d'informations.

   ```
   startsrc -s named -a "-d DebugLevel"
   ```

4. Recherchez d'éventuelles erreurs de configuration dans les fichiers de données **named**. Pour en savoir plus, reportez-vous à "Configuration des serveurs de noms", page 3-111, et aux sections "DOMAIN Data File Format," "DOMAIN Reverse Data File Format," "DOMAIN Cache File Format," et "DOMAIN Local Data File Format" dans le manuel *AIX Files Reference*.

Remarque : le plus souvent, les erreurs proviennent d'une mauvaise utilisation du point (.) et de l'arrobas (@) dans les fichiers de données DOMAIN.

Si des utilisateurs externes ne peuvent accéder à vos domaines :

- Vérifiez que tous vos serveurs de noms non maîtres (esclave, cache) sont définis avec les mêmes délais TTL dans les fichiers de données DOMAIN.

Si vos serveurs sont continuellement sollicités par des routines de résolution externes :

- Assurez-vous que vos serveurs diffusent des fichiers de données DOMAIN avec des délais TTL suffisants : si la valeur TTL est nulle ou négligeable, le délai accordé aux données transférées s'écoule très rapidement. Pour y remédier, prévoyez au moins une semaine comme valeur minimum dans vos enregistrements SOA.

Incidents de routage

Si vous ne parvenez pas à accéder à un hôte de destination, contrôlez les points suivants :

- Si vous recevez le message `Network Unreachable` vérifiez la route vers l'hôte passerelle, en lançant la commande **netstat –r** qui affiche les tables de routage noyau.
- Si vous recevez le message `No route to host`, vérifiez que l'interface de réseau local est opérationnelle en lançant la commande **ifconfig** nom_interface. Le résultat doit indiquer "up". Lancez la commande **ping** pour tenter d'atteindre un autre hôte du réseau.
- Si vous recevez le message `Connection timed out` :
  - Vérifiez que la passerelle locale est opérationnelle à l'aide de la commande **ping** assortie du nom ou de l'adresse Internet de la passerelle.
  - Vérifiez qu'une route vers l'hôte passerelle a été correctement définie. Lancez la commande **netstat -r** pour afficher la liste des tables de routage noyau.
  - Vérifiez que l'hôte qui vous intéresse dispose d'une entrée de table de routage renvoyant à votre machine.
- En routage statique, vérifiez qu'une route vers la passerelle et l'hôte cible a été définie : Lancez la commande **netstat -r** pour afficher la liste des tables de routage noyau.

Remarque : L'hôte qui vous intéresse doit disposer d'une entrée de table de routage renvoyant à votre machine.

- En routage dynamique, vérifiez, à l'aide de la commande **netstat –r,** que la passerelle est répertoriée dans les tables de routage noyau et qu'elle est correcte.
- Si l'hôte passerelle utilise le protocole RIP avec le démon **routed**, vérifiez qu'une route statique d'accès à l'hôte cible est définie dans le fichier **/etc/gateways.**

Remarque : Cette opération n'est requise que si le démon de routage ne parvient pas à identifier la route vers l'hôte distant en interrogeant les autres passerelles.

- Si l'hôte passerelle utilise RIP avec le démon **gated**, vérifiez qu'une route statique d'accès à l'hôte cible est définie dans le fichier **gated.conf**.
- En routage dynamique avec le démon **routed** :
  - Si **routed** ne parvient pas à identifier la route par le biais de demandes (par exemple, si l'hôte cible n'exécute pas le protocole RIP), vérifiez qu'une route d'accès à l'hôte cible est définie dans le fichier **/etc/gateways**.
  - Vérifiez que les passerelles chargées d'expédier les paquets à l'hôte sont opérationnelles et exécutent RIP. Sinon, vous devez définir une route statique.
  - Exécutez le démon **routed** avec l'option de mise au point pour journaliser les anomalies (réception de paquets erronés par exemple). Appelez le démon à partir de la ligne de commande, comme suit :

```
startsrc –s routed –a "–d"
```

  - Exécutez le démon **routed** avec l'indicateur **–t** pour envoyer tous les paquets entrants et sortants vers la sortie standard. Exécuté dans ce mode, **routed** reste sous le contrôle du terminal qui l'a lancé. Et il peut être arrêté depuis ce terminal.
- En routage dynamique avec le démon **gated** :
  - Vérifiez que le fichier **/etc/gated.conf** est correctement configuré et que vous exécutez les protocoles adéquats.
  - Vérifiez que les passerelles sur les réseaux source et cible utilisent le même protocole.
  - Vérifiez que la machine que vous tentez de contacter dispose d'une route retour vers votre machine hôte.

  - Vérifiez que les noms de passerelle des fichiers **gated.conf** et /**etc**/**networks** correspondent.

- Si vous utilisez le protocole RIP ou HELLO et que les routes d'accès ne peuvent pas être identifiées par des demandes de routage, vérifiez qu'une route d'accès à l'hôte cible est définie dans le fichier **gated.conf**. Il est conseillé de définir des routes statiques si :
  - L'hôte de destination n'exécute pas le même protocole que l'hôte source et ne peut donc pas échanger d'informations de routage.
  - L'accès à l'hôte doit se faire par une passerelle distante (c'est-à-dire sur un autre système autonome que l'hôte source). Le protocole RIP peut être utilisé uniquement entre des hôtes d'un même système autonome.

Autres possibilités

Si aucune des solutions proposées n'aboutit, vous pouvez activer le suivi du démon de routage (**routed** ou **gated**). Exécutez la commande SRC **traceson** à partir de la ligne de commande ou envoyez un signal au démon pour spécifier différents niveaux de suivi. Pour en savoir plus, reportez-vous au démon **gated** ou **routed.**

Incidents SRC

- Si les modifications apportées au fichier /**etc**/**inetd.conf** ne sont pas prises en compte :

  Mettez à jour le démon **inetd** via la commande **refresh –s inetd** ou **kill –1** *InetdPID*.

- Si **startsrc –s** [*sous_système*] renvoie le message :

  ```
  0513-00  The System Resource Controller is not active.
  ```

  Le sous-système SRC (System Resource Controller) n'a pas été activé. Lancez la commande **srcmstr &** pour lancer SRC, puis à nouveau la commande **startsrc**.

  Vous pouvez tenter de lancer le démon à partir de la ligne de commande sans SCR.

- Si **refresh –s** [*sous_système*] ou **lssrc –ls** [*sous_système*] renvoie le message :

  ```
  [subsystem name] does not support this option.
  ```

  Le sous-système ne prend pas en charge l'option SRC émise. Consultez la documentation relative au sous-système.

- Si le message ci-dessous s'affiche :

  ```
  SRC was not found, continuing without SRC support.
  ```

  Un démon a été appelé directement à partir de la ligne de commande et non via la commande **startsrc**. Ceci ne constitue pas un incident. Toutefois les commandes SRC (telles que **stopsrc** et **refresh)** ne peuvent pas être utilisées pour manipuler un sous-système appelé directement.

Incidents liés à telnet ou rlogin

Voici quelques indications sur les incidents liés aux commandes **telnet** et **rlogin**.

Distortion de l'écran

Si vous rencontrez des problèmes de distorsion d'écran dans des applications plein écran :

1. Vérifiez la variable d'environnement **TERM**, via la commande :

   ```
   env
   ```

   OU

   ```
   echo $TERM
   ```

2. Vérifiez que la valeur de **TERM** concorde avec le type d'écran de terminal utilisé.

Mise au point par telnet

Les sous-commandes **telnet** qui peuvent vous aider à résoudre des incidents sont :

display	Affiche les valeurs définies et les valeurs de commutation.
toggle	Affiche toutes les données réseau en hexadécimal.
toggle options	Change l'affichage des options internes du process **telnet.**

Programmes utilisant la bibliothèque curses étendue

Certains problèmes peuvent apparaître au niveau des touches de fonction et des touches fléchées si vous utilisez les commandes **rlogin** et **telnet** avec des programmes faisant appel à la bibliothèque curses étendue. En effet, ces touches génèrent des séquences d'échappement, qui peuvent être dissociées si le temps imparti ne suffit pas à la séquence complète. Après un certain délai, la bibliothèque curses décide si Echap doit être interprété seul ou comme le début d'une séquence d'échappement multi-octets générée par d'autres touches (touches fléchées, touches de fonction ou touche Action).

Si, dans le temps imparti, la touche Echap n'est suivie d'aucune donnée valide, curses l'interprète comme la touche Echap seule et fractionne la séquence de touches. Le délai associé aux commandes **rlogin** et **telnet** dépend du réseau : c'est en fonction de sa vitesse que les touches de fonction et les touches fléchées fonctionnent normalement ou non. Pour résoudre efficacement le problème, attribuez une valeur élevée (entre 1000 et 1500) à la variable d'environnement **ESCDELAY**.

Incidents de configuration

Une fois la carte installée, les interfaces de réseau sont automatiquement configurées au premier lancement du système. Il reste toutefois certaines valeurs initiales à définir pour TCP/IP, telles que le nom d'hôte, l'adresse Internet, etc. Pour cela, vous avez à votre disposition le raccourci Web-based System Manager **wsm network** ou l'interface SMIT :

- Servez-vous du raccourci **smit mktcpip** pour définir les valeurs initiales pour le nom d'hôte, l'adresse Internet et le masque de sous–réseau.
- Cette commande **smit mktcpip** permet également de spécifier un serveur pour la résolution de noms. Cependant, **smit mktcpip** ne configure qu'une seule interface de réseau.
- Pour définir d'autres attributs de réseau, utilisez le raccourci **smit chinet**.

Si vous souhaitez mettre en place des routes statiques pour que l'hôte puisse acheminer des informations de transmission (par exemple, une route d'accès à la passerelle locale), définissez–les de façon permanente dans la base de configuration, avec le raccourci Web-based System Manager **wsm network**, ou SMIT **smit mkroute**.

Si vous rencontrez d'autres difficultés, reportez-vous à "Configuration d'une liste de contrôle du réseau TCP/IP", page 3-4.

Incidents courants sur les interfaces de réseau

Une fois la carte installée, les interfaces de réseau sont automatiquement configurées au premier lancement du système. Il reste toutefois certaines valeurs initiales à définir pour TCP/IP. Par exemple, il est possible de définir le nom d'hôte et l'adresse Internet à l'aide du raccourci Web-based System Manager **wsm network**, ou SMIT **smit mktcpip**.

Si vous passez par SMIT, ayez recours au raccourci **smit mktcpip** pour définir ces valeurs de façon permanente dans la base de configuration. Pour les modifier dans le système actif, utilisez les raccourcis **smit chinet** et **smit hostname**. Le raccourci **smit mktcpip** permet une configuration minimale de TCP/IP. Pour ajouter des cartes, passez par le menu Further Configuration, accessible via le raccourci **smit tcpip**.

Si, malgré la validité des valeurs définies, vous avez toujours des difficultés à recevoir et envoyer des données :

- Vérifiez que votre carte réseau dispose d'une interface de réseau en exécutant la commande **netstat –i**. La sortie doit mentionner une interface, par exemple **tr0**, dans la colonne `Name` . Dans le cas contraire, créez une interface de réseau via Web-based System Managerou via la commande **smit mkinet**.
- Vérifiez que l'adresse IP de l'interface est correcte, en exécutant **netstat –i**. La sortie doit afficher l'adresse IP dans la colonne Network. Si l'adresse est incorrecte, modifiez-la via Web-based System Manager ou via la commande **smit chinet**.
- Consultez le journal des erreurs, en lançant la commande **errpt,** pour vérifier qu'aucun incident de carte n'a été détecté.
- Vérifiez que la carte est fiable en exécutant les programmes de diagnostics.

Si le problème n'est toujours pas identifié, reportez-vous aux sections "Incident sur une interface de réseau SLIP", page 3-165,"Incidents sur une interface de réseau Ethernet", page 3-165 ou "Incidents sur une carte de réseau en anneau à jeton", page 3-166.

Incidents sur une interface de réseau SLIP

En général, la méthode la plus efficace pour résoudre ce type d'incident consiste à vérifier pas à pas la configuration de votre système. Vous pouvez également :

- Vérifiez que le process **slattach** s'exécute sur le port tty approprié, via la commande **ps –ef**. Si ce n'est pas le cas, lancez la commande **slattach**. Pour la syntaxe à utiliser, reportez-vous à "Configuration de SLIP pour modem", page 3-138, ou "Configuration de SLIP pour câble de modem nul", page 3-140.
- Vérifiez les adresses point-à-point spécifiées via la commande **smit chinet**.

  Sélectionnez l'interface SLIP. Vérifiez l'adresse Internet et l'adresse de destination.

Si le modem ne fonctionne pas correctement :

- Vérifiez son installation. Reportez-vous au manuel opérateur du modem.
- Vérifiez que les contrôles de flux que le modem peut effectuer sont désactivés.

Si le tty ne fonctionne pas correctement, vérifiez le débit (en bauds) correspondant ainsi que les caractéristiques du modem, dans la base de données de configuration, via la commande **smit tty**.

Incidents sur l'interface de réseau Ethernet

Si une interface réseau est initialisée, les adresses définies et la carte installée correcte :

- Vérifiez qu'un connecteur en T est directement branché sur l'émetteur-récepteur (intégré ou non).
- Assurez–vous que vous utilisez un câble Ethernet (50 OHM).
- Assurez–vous que vous utilisez des terminaisons Ethernet (50 OHM).

- Les cartes Ethernet peuvent fonctionner avec un émetteur-récepteur interne ou externe. Un cavalier, installé sur la carte, définit le type d'émetteur-récepteur utilisé. Vérifiez la position de ce cavalier (reportez-vous à la documentation de la carte).
- Vérifiez le type de connecteur utilisé (BNC pour câble fin et DIX pour câble épais). Si vous changez le type de connecteur, utilisez le raccourci Web-based System Manager **wsm devices** ou SMIT **smit chgenet**, pour définir le champ Application des modifications à la base de données seulement. Ce champ doit être coché (avec Web-based System Manager) ou défini à **yes** (avec SMIT). Réamorcez ensuite la machine pour appliquer la nouvelle configuration. (Reportez-vous à "Configuration et gestion des cartes", page 3-39.)

Incidents liés à une interface de réseau en anneau à jeton

Si vous ne parvenez pas communiquer avec certaines machines, alors que l'interface de réseau est initialisée, les adresses convenablement définies et la carte installée correcte :

- Vérifiez si les machines en cause se trouvent sur un autre anneau. Si tel est le cas, utilisez le raccourci Web-based System Manager **wsm devices** ou SMIT **smit chinet**, pour cocher le champ Limitation diffusion sur RL en anneau à jeton. Ce champ *ne doit pas* être coché (avec Web-based System Manager) ou doit être défini à **no** (avec SMIT).
- Vérifiez que la carte de réseau en anneau à jeton est configurée pour fonctionner à la bonne vitesse d'anneau. Si ce n'est pas le cas, modifiez l'attribut de vitesse de l'anneau avec l'application Web-based System Manager wsm network ou avec SMIT (voir "Configuration et gestion de cartes", page 3-39). Dès la relance de TCP/IP, la vitesse d'anneau de la carte de réseau en anneau à jeton sera identique à celle du réseau.

Incidents avec un pont anneau à jeton/Ethernet

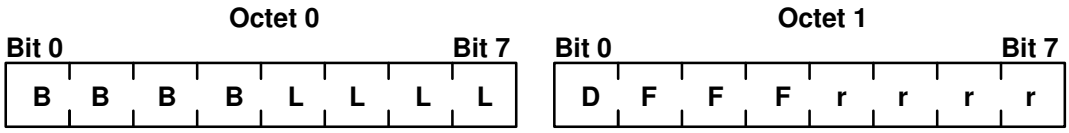
Si la communication entre un réseau en anneau à jeton et un réseau Ethernet reliés par un pont est défaillante alors que le pont fonctionne normalement, il est probable que la carte Ethernet rejette des paquets. Ce rejet a lieu lorsque le nombre de paquets entrants (en-têtes compris) est supérieur à la valeur MTU (Maximum Transmission Unit) de la carte. Par exemple, un paquet de 1500 octets envoyé par une carte en anneau à jeton via un pont, totalise 1508 octets, avec un en-tête LLC de 8 octets. Si la valeur MTU de la carte Ethernet est fixée à 1500, le paquet est rejeté.

Vérifiez les valeurs MTU (Maximum Transmission Unit) des deux cartes de réseau. Pour autoriser l'adjonction, par la carte en anneau à jeton, d'en-têtes LLC de 8 octets aux paquets sortants, la valeur MTU de cette carte doit être inférieure d'au moins 8 octets à celle de la carte Ethernet. Par exemple, pour qu'une carte en anneau à jeton puisse communiquer avec une carte Ethernet avec une MTU de 1500 octets, sa MTU doit être fixée à 1492.

Incidents sur un pont reliant deux réseaux en anneau à jeton

Lorsque la communication transite par un pont, la valeur MTU par défaut (de 1500 octets) doit être ramenée à 8 octets en-dessous de la valeur maximum I-frame déclarée par le pont dans le champ de contrôle de routage.

Pour retrouver la valeur du contrôle de routage, exécutez le démon **iptrace** qui permet d'examiner les paquets entrants. Les bits 1, 2 et 3 de l'octet 1 constituent les bits de trames maximales (Largest Frame Bit). Ils déterminent le maximum d'informations transmissibles entre deux stations de communication sur une route spécifique. Pour le format du champ de contrôle de routage, consultez la figure ci-dessous :



Champs de contrôle de routage (RC)

Les valeurs possibles des bits de trames maximales sont :

000	516 octets maximum dans le champ d'information.
001	1500 octets maximum dans le champ d'information.
010	2052 octets maximum dans le champ d'information.
011	4472 octets maximum dans le champ d'information.
100	8144 octets maximum dans le champ d'information.
101	Réservé.
110	Réservé.
111	Utilisé dans les trames de diffusion générale (toute route).

Par exemple, si la valeur de "maximum I-frame" est 2052 dans le champ de contrôle de routage, celle de MTU doit être fixée à 2044 (pour les interfaces anneau à jeton seulement).

Remarque : lorsque vous utilisez **iptrace**, le fichier de sortie *ne doit pas* résider sur un système de fichiers NFS.

Incidents de livraison de paquets

Communication avec un hôte distant

Si vous ne parvenez pas à établir la communication avec un hôte distant :

- Lancez la commande **ping** sur l'hôte local pour vérifier que l'interface locale reliée au réseau est opérationnelle et active.
- Appliquez la commande **ping** successivement aux hôtes et passerelles par lesquelles l'information transite, pour localiser la défaillance.

Si vous constatez des pertes de paquet ou des retards de livraison :

- Lancez la commande **trpt** pour effectuer un suivi des paquets au niveau socket.
- Lancez la commande **iptrace** pour effectuer le suivi de toutes les couches de protocole.

Si vous ne parvenez pas à établir la communication entre un réseau en anneau à jeton et un réseau Ethernet reliés par un pont qui fonctionne normalement :

- Vérifiez les valeurs MTU (Maximum Transmission Unit) des deux cartes de réseau. Elles doivent être compatibles pour autoriser la communication. En effet, si la taille du paquet entrant (en-têtes compris) est supérieure à la valeur MTU (Maximum Transmission Unit) de la carte, la machine rejette le paquet. Par exemple, un paquet de 1500 octets envoyé via un pont récupère un en-tête LLC de 8 octets pour atteindre une taille de 1508 octets. Si la valeur MTU de la machine réceptrice est fixée à 1500, le paquet est rejeté.

Réponses snmpd

Si **snmpd** ne répond pas et qu'aucun message d'erreur n'est transmis, il est probable que la taille du paquet est trop grande pour le gestionnaire de paquets UDP noyau. Dans ce cas, augmentez la valeur des variables du noyau **udp_sendspace** et **udp_recvspace** :

```
no -o udp_sendspace=64000
no -o udp_recvspace=64000
```

La taille maximale d'un paquet UDP est 64 ko : une demande de plus de 64 ko est rejetée. Pour éviter ce type d'incident, le paquet doit être fractionné.

Incidents au niveau du protocole DHCP

Si vous ne pouvez pas obtenir une adresse IP ou d'autres paramètres de configuration :

- Vérifiez que vous avez spécifié une interface à configurer : via l'application Web-based System Manager wsm network, en éditant le fichier /**etc**/**dhcpcd.ini** ou en utilisant le raccourci SMIT **smit dhcp**.
- Vérifiez qu'il existe un serveur sur le réseau local ou un agent relais configuré pour acheminer vos requêtes hors du réseau local.
- Vérifiez que le programme **dhcpcd** est actif. Dans la négative, lancez-le via la commande **startsrc –s dhcpcd**.

Informations de référence TCP/IP

Les thèmes relatifs au protocole TCP/IP abordés dans cette section sont les suivants :

Liste des commandes TCP/IP

chnamsv	Modification sur un hôte de la configuration du service de noms TCP/IP.
chprtsv	Modification de la configuration d'un service d'impression sur une machine client ou serveur.
hostent	Manipulation directe des entrées d'équivalence d'adresse dans la base de données de configuration du système.
ifconfig	Configuration/affichage des paramètres d'interface d'un réseau TCP/IP.
mknamsv	Configuration sur un hôte du service de noms TCP/IP pour un client.
mkprtsv	Configuration sur un hôte d'un service d'impression TCP/IP.
mktcpip	Définition des valeurs requises pour le lancement de TCP/IP sur un hôte.
no	Configuration des options de réseau.
rmnamsv	Déconfiguration sur un hôte du service de noms TCP/IP.
rmprtsv	Déconfiguration de la configuration d'un service d'impression sur une machine client ou serveur.
slattach	Raccordement des lignes série comme interfaces de réseau.
arp	Affichage/modification des tables de traduction d'adresse Internet en adresse matérielle, utilisées par ARP (Address Resolution Protocol).
gettable	Récupération à partir d'un hôte des tables d'hôte au format NIC.
hostid	Définition ou affichage de l'identificateur de l'hôte local courant.
hostname	Définition ou affichage du nom du système hôte courant.
htable	Conversion des fichiers hôtes au format utilisé par les routines de bibliothèque de réseau.
ipreport	Génération d'un rapport de suivi de paquet à partir du fichier spécifié.
iptrace	Suivi des paquets au niveau interface pour les protocoles Internet.
lsnamsv	Affichage des informations du service de noms stockées dans la base de données.
lsprtsv	Affichage des informations du service d'impression stockées dans la base de données.
mkhosts	Génération du fichier de tables hôte.
namerslv	Manipulation directe des entrées de serveur de noms de domaine pour les routines de résolution dans la base de données de configuration.

netstat	Affichage de l'état du réseau.
route	Manipulation directe des tables de routage.
ruser	Manipulation directe des entrées de trois bases de données système distinctes contrôlant l'accès des hôtes étrangers aux programmes locaux.
ruptime	Affichage de l'état de chaque hôte d'un réseau.
securetcpip	Activation de la fonction de sécurité réseau.
setclock	Définition de la date et de l'heure d'un hôte sur un réseau.
timedc	Informations sur le démon **timed**.
trpt	Suivi des prises TCP (Transmission Control Protocol).

Liste des démons TCP/IP

fingerd	Affichage des informations sur un utilisateur distant.
ftpd	Fonction serveur pour le protocole FTP (File Transfer Protocol) d'Internet.
gatedn	Apport des fonctions de routage de passerelles aux protocoles RIP (Routing Information Protocol), HELLO, EGP (Exterior Gateway Protocol), BGP (Border Gateway Protocol) et SNMP (Simple Network Management Protocol).
inetd	Gestion du service Internet pour un réseau.
named	Apport de la fonction serveur au protocole DOMAIN.
rexecd	Apport de la fonction serveur à la commande **rexec.**
rlogind	Apport de la fonction serveur à la commande **rlogin.**
routed	Gestion des tables de routage de réseau.
rshd	Apport de la fonction serveur pour l'exécution de commandes à distance.
rwhod	Apport de la fonction serveur aux commandes **rwho** et **ruptime.**
syslogd	Lecture et consignation des messages système.
talkd	Apport de la fonction serveur à la commande **talk.**
telnetd	Apport de la fonction serveur au protocole TELNET.
tftpd	Assure la fonction serveur pour le protocole TFTP (Trivial File Transfer Protocol).
timedn	Appel au démon **timeserver** au lancement du système.

Raccourcis SMIT pour TCP/IP

Vous trouverez dans le récapitulatif des raccourcis du manuel *AIX 4.3 Guide d'administration : système d'exploitation et unités* les raccourcis correspondant aux tâches de gestion système TCP/IP.

Liste des méthodes

Les méthodes d'unité sont des programmes associés à une unité qui exécutent des opérations de base de configuration d'unité. Pour en savoir plus sur les méthodes TCP/IP, reportez-vous à la section "List of TCP/IP Programming References" dans *AIX Communications Programming Concepts*.

Liste des fichiers TCP/IP

/etc/rc.bsdnet

Pour des informations sur les fichiers TCP/IP et les formats de fichier, reportez-vous à la section ”List of TCP/IP Programming References”dans *AIX Communications Programming Concepts*.

Liste des RFC

Pour connaître la liste des RFC (Request for Comments) pris en charge par AIX, reportez-vous à la section ”List of TCP/IP Programming References” dans *AIX Communications Programming Concepts*.

- RFC 1359 ”Connecting to the Internet: What connecting institutions should anticipate.”
- RFC 1325 ”FYI on questions and answers: Answers to commonly asked ’new Internet user’ questions”
- RFC 1244 ”Site Security Handbook”
- RFC 1178 ”Choosing a Name for Your Computer”
- RFC 1173 ”Responsibilities of host and network managers: A summary of the ’oral tradition’ of the Internet”

Accès aux RFC

Nombre de RFC sont accessibles en ligne. Vous pouvez en obtenir une copie papier auprès de SRI, indépendamment ou par abonnement. Pour en savoir plus, écrivez à nisc@nisc.sri.com ou appelez le 1–415–859–6387.

Les exemplaires en ligne sont accessibles via FTP à partir de ftp.nisc.sri.com, sous la forme rfc/rfc*nnnn*.txt ou rfc/rfc*nnnn*.ps (*nnnn* représentant le numéro RFC sans zéros à gauche). De plus, vous pouvez faire une demande de RFC par courrier électronique à partir du serveur de courrier automatisé de SRI, en envoyant un message à mail-server@nisc.sri.com. Dans le corps du message, indiquez le RFC qui vous intéresse, par exemple, `send rfc`*`nnnn`* où *nnnn* est le numéro du RFC. Pour les RFC PostScript, spécifiez l’extension, par exemple, `send rfc`*`nnnn`*`.ps`. Vous pouvez formuler plusieurs demandes dans un seul message, sous réserve de les spécifier sur des lignes distinctes. L’index des RFC peut être obtenu par la commande `send rfc-index`.

API à chargement dynamique

AIX prend en charge la résolution de noms à partir de cinq mappes différentes :

- serveur de noms de domaine (DNS),
- serveur d'informations réseau (NIS),
- NIS+,
- méthodes locales de résolution de noms et
- API définies par l'utilisateur et chargées de manière dynamique.

Avec l'interface de programmation d'application (API) à chargement dynamique, vous pouvez charger vos modules et disposer de routines venant s'ajouter aux mappes fournies par AIX. L'API à chargement dynamique vous permet de créer ce type d'interface dans l'une des cinq classes de mappes : hôtes, services, protocoles, réseaux et netgroup. Vous pouvez créer vos propres modules utilisateur contenant des API pour tout ou partie de ces classes de mappes. Les sections suivantes définissent les prototypes et les noms de fonctions d'une API pour chacune de ces cinq classes. Reportez–vous à la section Configuration d'une API dynamique pour plus d'informations sur la configuration d'une API à chargement dynamique avec AIX.

Noms de fonctions et prototypes

AIX prend en charge cinq classes de mappes pour des modules pouvant être chargés par l'utilisateur : hôtes, services, protocoles, réseaux et netgroup. Afin d'instancier chaque accesseur de mappe, AIX exige que le module fourni par l'utilisateur se serve expressément des noms de fonction et des prototypes de fonction AIX définis pour chaque classe de mappe.

Type de mappes de services

Les éléments qui suivent représentent le prototype requis pour une classe de mappes de services définie par l'utilisateur :

```
void *sv_pvtinit();
void sv_close(void *private);
struct servent * sv_byname(void *private, const char *name, const char
*proto);
struct servent * sv_byport(void *private, int port, const char *proto);
struct servent * sv_next(void *private);
void sv_rewind(void *private);
void sv_minimize(void *private);
```

La fonction *sv_pvtinit* est indispensable bien qu'elle se limite au renvoi d'un NULL si la routine d'appel n'exige pas de données privées.

Les fonctions autres que *sv_pvtinit* sont facultatives. L'utilisateur peut faire l'impasse sur tout ou partie de ces fonctions facultatives.

Type de mappes de protocoles

Les éléments qui suivent représentent le prototype requis pour une classe de mappes de protocoles définie par l'utilisateur :

```
void * pr_pvtinit();
void pr_close(void *private);
struct protoent * pr_byname(void *private, const char *name);
struct protoent * pr_bynumber(void *private, int num);
struct protoent * pr_next(void *private);
void pr_rewind(void *private);
void pr_minimize(void *private);
```

La fonction *pr_pvtinit* est indispensable bien qu'elle se limite au renvoi d'un NULL si la routine d'appel n'exige pas de données privées.

Les fonctions autres que *pr_pvtinit* sont facultatives. L'utilisateur peut faire l'impasse sur tout ou partie de ces fonctions facultatives.

Type de mappes d'hôtes

Les éléments qui suivent représentent le prototype requis pour une classe de mappes d'hôtes définie par l'utilisateur :

```
void * ho_pvtinit();
void ho_close(void *private);
struct hostent * ho_byname(void *private, const char *name);
struct hostent * ho_byname2(void *private, const char *name, int af);
struct hostent * ho_byaddr(void *private, const void *addr, size_t len, int
af);
struct hostent * ho_next(void *private);
void ho_rewind(void *private);
void ho_minimize(void *private);
```

La fonction *ho_pvtinit* est indispensable bien qu'elle se limite au renvoi d'un NULL si la routine d'appel n'exige pas de données privées.

Les fonctions autres que *ho_pvtinit* sont facultatives. L'utilisateur peut faire l'impasse sur tout ou partie de ces fonctions facultatives.

Type de mappes réseau

Les éléments qui suivent représentent le prototype requis pour une classe de mappes réseau définie par l'utilisateur :

```
void * nw_pvtinit();
void nw_close(void *private);
struct nwent * nw_byname(void *private, const char *name, int addrtype);
struct nwent * nw_byaddr(void *private, void *net, int length, int
addrtype);
struct nwent * nw_next(void *private);
void nw_rewind(void *private);
void nw_minimize(void *private);
```

La fonction *nw_pvtinit* est indispensable bien qu'elle se limite au renvoi d'un NULL si la routine d'appel n'exige pas de données privées.

Les fonctions autres que *nw_pvtinit* sont facultatives. L'utilisateur peut faire l'impasse sur tout ou partie de ces fonctions facultatives.

Structure de données

AIX fournit la structure de données requise pour la mise en place de la classe de mappes réseau qui l'utilise pour communiquer avec le système d'exploitation.

```
  struct nwent {
        char *name;       /* official name of net */
        char **n_aliases; /* alias list */
        int n_addrtype;   /* net address type */
        void *n_addr;     /* network address */
        int n_length;     /* address length, in bits */
   };
```

Type de mappes Netgroup

Les éléments qui suivent représentent le prototype requis pour une classe de mappes netgroup définie par l'utilisateur :

```
void * ng_pvtinit();
void ng_rewind(void *private, const char *group);
void ng_close(void *private);
int ng_next(void *private, char **host, char **user, char **domain);
int ng_test(void *private, const char *name, const char *host, const char
*user, const char *domain);
void ng_minimize(void *private);
```

La fonction *ng_pvtinit* est indispensable bien qu'elle se limite au renvoi d'un NULL si la routine d'appel n'exige pas de données privées.

Les fonctions autres que *ng_pvtinit* sont facultatives. L'utilisateur peut faire l'impasse sur tout ou partie de ces fonctions facultatives.

Utilisation de l'API à chargement dynamique

Vous devez affecter un nom au module défini par l'utilisateur et suivre pour ce faire une convention pré–établie. Vous devez également le configurer dans le système d'exploitation préalablement à son démarrage. Les sections suivantes traitent de l'affectation d'un nom au module API et de sa configuration.

Affectation d'un nom au module défini par l'utilisateur

Les noms de modules contenant des API définies par l'utilisateur se présentent généralement sous la forme suivante :

NameAddressfamily

où *Name* est le nom du module à chargement dynamique. La longueur de *Name* varie de 1 à 8 caractères.

Les mots–clé suivants sont réservés comme nom d'option utilisateur et ne peuvent pas être utilisés dans ce cas :

- local
- bind
- dns
- nis
- ldap

Addressfamily qui représente la famille d'adresses peut être assortie du chiffre *4* ou *6*. En l'absence de chiffre, la famille d'adresses est AF_UNSPEC. Avec le chiffre *4*, la famille d'adresses est AF_INET. Avec le chiffre *6*, la famille d'adresses est AF_INET6.

Tous les autres formats d'options utilisateur ne sont pas valables.

Si l'utilisateur a appelé *gethostbyname2* dans l'application, la famille d'adresses que l'utilisateur a affectée à l'appel système *gethostbyname2* écrase celle de l'option utilisateur. A titre d'exemple, avec une option utilisateur *david6* dans l'application, l'appel système est gethostbyname2(name, AF_INET). Puis, la famille d'adresses AF_INET écrase celle de l'option utilisateur (6, correspondant à AF_INET6).

Configuration d'une API dynamique

L'utilisateur dispose de trois modes de définition des routines de résolution à chargement dynamique :

Variable d'environnement NSORDER

Vous pouvez définir ou non plusieurs options utilisateurs dans la variable d'environnement NSORDER. Il n'y pas de limite dans le nombre d'options saisies ni dans leur ordre de saisie. Sur la ligne de commande, tapez par exemple :

```
export NSORDER=local, bind, bob, nis, david4, jason6
```

Dans ce cas, AIX appelle les modules de résolution de noms listés de gauche à droite jusqu'à résolution du nom. Les modules appelés local, bind et nis sont réservés par AIX, mais bob, david4 et jason6 sont des modules utilisateur.

Fichier de configuration /etc/netsvc.conf

Vous pouvez définir ou non plusieurs options du fichier de configuration /etc/netsvc.conf. Il n'y a pas de limite au nombre d'options saisies ni à leur ordre de saisie. A titre d'exemple :

```
hosts=nis, jason4, david, local, bob6, bind
```

Fichier de configuration /etc/irs.conf

Vous pouvez définir ou non plusieurs options du fichier de configuration /etc/irs.conf. Il n'y a pas de limite au nombre d'options saisies ni à leur ordre de saisie. A titre d'exemple :

```
hosts dns continue
hosts jason6 merge
hosts david4
```

L'utilisateur peut définir un maximum de 16 modules utilisateur à partir de l'une des sources ci–dessus.

La variable d'environnement *NSORDER* a la priorité la plus élevée, suivie du fichier de configuration /etc/netsve.conf, pour finir par le fichier de configuration /etc/irs.conf qui a le niveau de priorité le moins élevé. En présence d'une option utilisateur assortie d'un niveau de priorité élevé (NSORDER, par exemple), toutes les autres options utilisateur assorties d'un niveau de priorité inférieur (/etc/netsvc.conf et /etc/irs.conf, par exemple) ne sont pas prises en compte.

Procédures

Pour créer et installer un module contenant une API à chargement dynamique, procédez comme suit :

1. Créez tout d'abord le module à chargement dynamique en fonction des spécifications AIX.
2. L'utilisateur doit également créer un fichier (*rnd.exp*, par exemple) destiné à l'exportation de tous les symboles à utiliser.
3. AIX fournit le Makefile type permettant à l'utilisateur de créer un fichier de module à chargement dynamique (fichier *rnd.so*, par exemple). Le Makefile, le fichier d'exportation ainsi que le fichier de module utilisateur type se trouvent dans le répertoire */usr/samples/tcpip/dynload*.
4. Après compilation, l'utilisateur peut placer tous les fichiers d'objets à chargement dynamique dans le chemin d'accès */usr/lib/netsvc/dynload*.
5. L'utilisateur doit ensuite configurer les éléments suivants :
   - la variable d'environnement *NSORDER*
     ou l'un des fichiers de configuration,
   - /etc/netsvc.conf
     ou
   - /etc/irs.conf.
6. La fonctionnalité API à chargement dynamique est alors prête à l'emploi.

Chapitre 4. Sécurité IP (Internet Protocol)

Le protocole de sécurité IP permet de sécuriser les communications sur le réseau Internet et les réseaux d'entreprise en protégeant le flux de données au niveau de la couche IP. Il permet aux utilisateurs individuels ou aux entreprises de protéger l'échange de données de toutes les applications sans avoir à modifier ces applications. Ainsi, la transmission de tout type de données, de messagerie électronique ou d'applications par exemple, peut être sécurisée.

Le système de sécurité des données entre deux nœuds est matérialisé par la mise en œuvre d'un tunnel virtuel entre deux systèmes hôtes. C'est ce qu'on appelle créer un réseau privé virtuel (VPN – Virtual Private Network). Le tunnel de sécurité encapsule toutes les données IP échangées entre les deux hôtes conformément aux spécifications de l'utilisateur. L'intégrité des données est respectée, tout comme la confidentialité et l'authentification, en fonction de la configuration du tunnel.

Ce chapitre traite des points suivants :

Avantages d'un VPN (Virtual Private Network)

Un réseau privé virtuel est un prolongement du réseau privé interne d'une entreprise vers un réseau public tel qu'Internet. Il met en place une connexion privée sécurisée par le biais d'un tunnel privé. Les VPN permettent de transporter les informations en toute sécurité sur Internet, en reliant les utilisateurs distants, les succursales, et les différents partenaires commerciaux au sein d'un réseau d'entreprise étendu. Les prestataires de services Internet (ISP) offrent des moyens d'accès rentables à Internet par le biais de lignes directes ou de numéros de téléphone locaux. Les sociétés peuvent donc se passer de leurs options de réseau actuelles faisant appel à des lignes spécialisées coûteuses, des appels longue distance ou des numéros gratuits.

Sécurité

AIX utilise la sécurité IP (IP Sec), technologie de sécurité standard ouverte développée par l'IETF (Internet Engineering Task Force), en tant que partie intégrante des solutions VPN eNetwork. IP Sec fournit une protection basée sur le chiffrement de toutes les données au niveau de la couche IP de la pile de communications. La sécurité des données est assurée de manière transparente, sans modifications nécessaires au niveau des applications existantes. IP Sec constitue l'ossature de sécurité réseau standard choisie par l'IETF pour les environnements IP de versions 4 et 6.

IP Sec protège vos trafics de données par la mise en œuvre de trois méthodes sérieuses de chiffrement des données :

1. Authentification

   Processus consistant à vérifier l'identité d'un hôte ou d'un point d'extrémité.

2. Contrôle d'intégrité

   Processus consistant à vérifier qu'aucune modification des données n'est survenue au cours de leur transfert sur le réseau.

3. Chiffrement

   Processus garantissant la confidentialité des données par le "masquage" des données et des adresses IP privées en transit sur le réseau.

Les algorithmes d'authentification fournissent la preuve de l'identité de l'expéditeur et de l'intégrité des données en utilisant une fonction de chiffrement par hachage qui traite un paquet de données (champs d'en–tête IP immuables inclus) à l'aide d'une clé privée afin de produire un condensé unique. Du côté du destinataire, les données sont "décapsulées" à l'aide de la même fonction et de la même clé. Si les données ont subi une altération ou si la clé de l'émetteur est incorrecte, le datagramme est supprimé.

Le chiffrement fait appel à un algorithme et une clé pour modifier et rendre aléatoire les données qui se transforment ainsi en texte chiffré. Les données ainsi chiffrées sont illisibles en cours de transfert. Lorsqu'elles arrivent à destination, les données sont rétablies à l'aide du même algorithme et de la même clé (algorithmes de chiffrement symétriques). Le chiffrement doit être effectué en conjonction avec l'authentification de manière à vérifier l'intégrité des données chiffrées.

Ces services de base sont implémentés dans IP Sec au moyen de l'encapsulation IP (ESP – Encapsulating Security Payload) et de l'en–tête d'authentification (AH – Authentication Header). Avec ESP, la confidentialité est assurée par le chiffrement du paquet IP original, la création d'un en–tête ESP, et l'insertion des données chiffrées (le *texte chiffré*) dans le paquet ESP.

Lorsque seuls l'authentification et le contrôle d'intégrité des données sont requis, sans confidentialité, l'en–tête d'authentification (AH) peut être utilisé seul. Avec AH, les champs fixes de l'en–tête IP et les données sont traités par un algorithme de hachage afin de générer un condensé codé. Le destinataire utilise sa clé pour calculer et comparer le condensé, afin de vérifier que le paquet n'a pas été modifié et que l'identité de l'émetteur ne fait aucun doute.

Fonctions de sécurité IP

Le dispositif de sécurité IP d'AIX offre les fonctions suivantes :

- Prise en charge de l'en–tête d'authentification (AH) avec la RFC 2402 et de l'encapsulation (ESP) avec la RFC 2406.
- Actualisation automatique des clés à l'aide des tunnels du protocole IKE de l'IETF et des tunnels IBM.
- Actualisation automatique des clés à l'aide des tunnels manuel avec les touches définies de manière statique.
- Utilisation des modes Tunnel et Transport pour l'encapsulation
- Algorithmes d'authentification de HMAC MD5 et de HMAC SHA1
- Les algorithmes de chiffrement comprennent DES CBC 56 bits (64 bit IV), Triple DES, DES CBC 4 (32 bits IV), CDMF (DES 40 bits exportable).
- Prise en charge de la pile Dual IP (versions IP 4 et 6). IP version 6 peut être configuré à l'aide de tunnels manuels.
- Le trafic de IP versions 4 et 6 peut être encapsulé et filtré. Comme les piles IP sont distinctes, la fonction de sécurité IP pour chaque pile peut être configurée de manière indépendante.
- Des tunnels manuels peuvent être configurés de manière à garantir l'interfonctionnement avec d'autres systèmes qui ne prennent pas en charge les méthodes automatiques d'actualisation de clés IKE, et pour l'utilisation de tunnels IP V6.
- Filtrage du trafic sécurisé et non sécurisé par un certain nombre de caractéristiques IP, telles que les adresses IP source et destination, l'interface, le protocole, les numéros de port, etc.
- Génération et suppression automatique des règles de filtrage avec la plupart des types de tunnels.
- Utilisation de noms d'hôte pour l'adresse de destination lors de la définition des tunnels et des règles de filtrage. Les noms d'hôte sont convertis automatiquement en adresses IP (dans la mesure où la fonction DNS est disponible).
- Consignation des événements de sécurité IP dans le journal système.
- Utilisation étendue des opérations de suivi système et de statistiques pour l'identification des incidents.
- Les opérations par défaut définies par l'utilisateur lui permettent d'indiquer si le trafic qui ne correspond pas aux tunnels définis doit faire l'objet d'une autorisation d'accès ou d'un refus.

Fonctions IKE

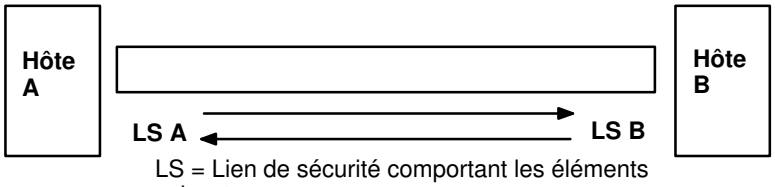
Les fonctions suivantes sont disponibles avec Internet Key Exchange pour AIX versions 4.3.2 et ultérieures :

- Authentification avec clés pré–partagées
- Utilisation du mode principal (identification du mode de protection) et du mode agressif.
- Prise en charge pour Diffie Hellman groupes 1 et 2.
- Prise en charge du chiffrement ESP pour DES, Triple DES, chiffrement nul. Prise en charge de l'authentification ESP avec HMAC MD5 et HMAC SHA1.
- Prise en charge de AH pour HMAC MD5 et HMAC SHA1.

- Séparation des politiques de sécurité avec définition de tunnels permettant ainsi la réutilisation des politiques de sécurité définies.

Liens de sécurité

La pierre angulaire sur laquelle reposent les communications sécurisées est le concept appelé *lien de sécurité*. Les liens de sécurité (LS) associent un ensemble spécifique de paramètres de sécurité à un type de trafic. Dans le cas de données sous sécurité IP, il existe un lien de sécurité pour chaque direction et pour chaque type d'en–tête, à savoir AH ou ESP. Les informations contenues dans le lien englobent les adresses IP des parties impliquées dans la communication, un identificateur unique appelé Security Parameters Index (SPI), les algorithmes sélectionnés pour l'authentification et/ou le chiffrement, les clés d'authentification et de chiffrement ainsi que la durée de vie des clés (voir figure). L'objectif de cette gestion des clés est de négocier et de calculer les liens de sécurité qui seront utilisés pour la protection du trafic IP.



LS = Lien de sécurité comportant les éléments suivants :

- Adresse de destination
- Valeur SPI
- Clé
- Algorithme de chiffrement et format
- Algorithme d'authentification
- Durée de vie de la clé

Mise en place d'un tunnel sécurisé entre les hôtes A et B

Gestion des clés et tunnels

Pour mettre en place une communication sécurisée entre deux hôtes, des LS doivent être négociés et gérés au cours de l'utilisation du tunnel. Trois types de tunnels sont pris en charge dans AIX. Ils utilisent une technique de gestion des clés différente. Ce sont les suivants :

- Tunnels IKE (clés changeant dynamiquement, norme IETF)
- Tunnels IBM (dynamiques, propriétaires)
- Tunnels manuels (statiques, clés persistantes, norme IETF)

Prise en charge du tunnel IKE

Les tunnels IKE sont basés sur les normes ISAKMP/Oakley développées par l'IETF. Avec ce protocole, les paramètres de sécurité sont négociés et rafraîchis et l'échange des clés se fait de manière sécurisée. Trois types d'authentification sont décrits dans les normes (clé pré–partagée, signature numérique et clé publique). Le premier type d'authentification (clé pré–partagée) est actuellement mis en place par AIX Version 4.3.3.

La négociation utilise une approche à deux phases. La première phase authentifie les parties impliquées dans la communication et précise les algorithmes à utiliser pour sécuriser la communication au cours de la deuxième phase. Au cours de cette phase, les paramètres de sécurité IP à utiliser au cours du transfert de données sont négociés, les liens de sécurité et les clés sont générés et échangés.

Algorithme	AH IP version 4	ESP IP version 4
HMAC MD5	X	X
HMAC SHA1	X	X
DES CBC 8		X
3DES CBC		X
ESP nul		X

Tunnels manuels

Les tunnels manuels fournissent une compatibilité en amont et interagissent avec les machines ne prenant pas en charge les protocoles de gestion des clés IKE. L'inconvénient de ces tunnels manuels est que leurs valeurs de clé sont statiques. En d'autres termes, les clés de chiffrement et d'authentification sont identiques pour toute la durée de vie du tunnel et doivent être mises à jour manuellement.

Algorithme	AH IP version 4	AH IP version 6	ESP IP version 4	ESP IP version 6
HMAC MD5	X	X	X	X
HMAC SHA1				
DES CBC 8			X	X
DES CBC 4			X	X
CDMF			X	X
3 DES CBC			X	X

Les tunnels IKE offrant une sécurité plus efficace, le choix se porte de préférence sur la méthode IKE de gestion de clés.

Fonctions de filtrage natif

Le *filtrage* est une fonction de base qui permet d'accepter ou de refuser les paquets entrants et sortants en fonction d'un certain nombre de critères. Ainsi, un utilisateur ou un administrateur système peut configurer le système hôte afin de contrôler le trafic entre cet hôte et d'autres systèmes hôtes. Le filtrage s'effectue à partir des propriétés des paquets, telles que les adresses source et de destination, la version IP (4 ou 6), les masques de sous–réseau, le protocole, le port, les propriétés de routage, la fragmentation, l'interface et la définition des tunnels.

Des règles, appelées *règles de filtre*, permettent d'associer certains types de trafic à un certain type de tunnel. Avec une configuration AIX de base pour tunnels manuels, lorsqu'un utilisateur définit un tunnel hôte à hôte, des règles de filtre sont générées automatiquement afin de canaliser tout le trafic de cet hôte vers le tunnel sécurisé. Si des types plus spécifiques de trafic sont souhaités (sous–réseau à sous–réseau, par exemple), les règles de filtre peuvent être modifiées ou remplacées de manière à permettre un contrôle précis du trafic transitant via un tunnel particulier.

Pour les tunnels IKE, les règles de filtre sont aussi générées automatiquement et insérées dans une table de filtres, une fois le tunnel activé.

De la même manière, lorsqu'un tunnel est modifié ou supprimé, les règles de filtre concernant ce tunnel sont automatiquement supprimées. La configuration de la sécurité IP s'en trouve considérablement simplifiée et par là–même le risque d'erreur humaine réduit. Les définitions de tunnel peuvent être diffusées et partagées avec d'autres machines ou pare–feu AIX à l'aide d'utilitaires d'importation et d'exportation. Cela contribue à simplifier l'administration d'un grand nombre de machines.

Les règles de filtre sont nécessaires pour associer des types particuliers de trafic à un tunnel, mais les données filtrées ne vont pas forcément passer par un tunnel. Ces règles permettent à AIX d'assurer des fonctions élémentaires de pare–feu pour les utilisateurs souhaitant limiter le flux de certains types de trafic à destination ou en provenance de leur machine. Ceci est particulièrement utile pour la gestion de machines au sein d'un réseau interne ou ne bénéficiant pas de la protection d'un pare–feu. En théorie, cela ressemble à l'établissement d'une zone démilitarisée (DMZ) ; les règles de filtre édifient un second rempart autour d'un groupe de machines en cas de compromis.

Une fois les règles de filtre générées, elles sont enregistrées dans une table et chargées dans le noyau. Lorsqu'un échange de paquets se prépare sur le réseau, les règles de filtre sont successivement étudiées, de haut en bas, afin de déterminer si le prochain paquet doit être accepté, refusé ou envoyé via un tunnel. Les critères définis dans la règle sont comparés aux caractéristiques du paquet jusqu'à ce qu'une correspondance soit établie ou que la règle par défaut soit atteinte.

La fonction de sécurité IP met également en œuvre un système de filtrage des paquets non sécurisés en fonction de critères définis par l'utilisateur dont la granularité est importante. Cela peut être utile pour le contrôle du trafic IP entre réseaux et machines n'exigeant pas le recours à la sécurité IP.

Installation de la sécurité IP

La fonction de sécurité IP sous AIX doit être installée et chargée séparément. Les principaux fichiers à installer sont les suivants :

- **bos.net.ipsec.rte** – Environnement d'exécution pour l'environnement et les commandes du noyau de sécurité IP.
- **bos.msg.***LANG***.net.ipsec** (*LANG* correspondant à la langue de votre choix, par exemple **en_US**)

Les fichiers suivants doivent également être installés pour la prise en charge du tunnel IKE :

- **bos.net.ipsec.keymgt**
- **bos.net.ipsec.websm**
- Les fichiers **bos.crypto** correspondant à votre pays.

Une fois installée, la fonction de sécurité IP peut être chargée séparément pour IP versions 4 et 6. Cette opération est effectuée en lançant les commandes **mkdev** ou via les menus SMIT du protocole de sécurité IP.

Chargement de la fonction de sécurité IP

Attention : le chargement de la fonction de sécurité IP active la fonction de filtrage. Aussi, avant le chargement, il est important de veiller à la création de règles de filtrage correctes. Dans le cas contraire, toutes les communications sortantes sont bloquées.

Si vous utilisez SMIT ou Web-based System Manager(raccourci **wsm network**), les modules de sécurité IP seront automatiquement chargés lors du démarrage de la fonction de sécurité IP. C'est le meilleur moyen pour vous assurer que les extensions de noyau et les démons IKE sont chargés dans le bon ordre.

Si le chargement s'est correctement déroulé, la commande **lsdev** affiche les unités de sécurité IP `disponibles (Available).`

```
lsdev -C -c ipsec
   ipsec_v4 Available IP Version 4 Security Extension
   ipsec_v6 Available IP Version 6 Security Extension
```

Une fois que l'extension du noyau de sécurité IP a été chargée, les tunnels et les filtres peuvent être configurés.

Configuration de la sécurité IP

Pour configurer la fonction de sécurité IP, les tunnels et les filtres doivent être configurés. Si un simple tunnel doit être défini pour l'ensemble des échanges de données, les règles de filtre peuvent être générées automatiquement. Pour définir un système de filtres plus élaboré, les règles peuvent être configurées séparément.

Vous pouvez configurer la sécurité IP à l'aide de l'application Web-based System Manager wsm network ou de SMIT (System Management Interface Tool). Si vous utilisez SMIT, les raccourcis suivants vous conduiront directement aux panneaux de configuration nécessaires :

ips4_basic Configuration de base pour IP version 4

ips6_basic Configuration de base pour IP version 6

Cette section de la configuration de la sécurité IP aborde les sujets suivants :

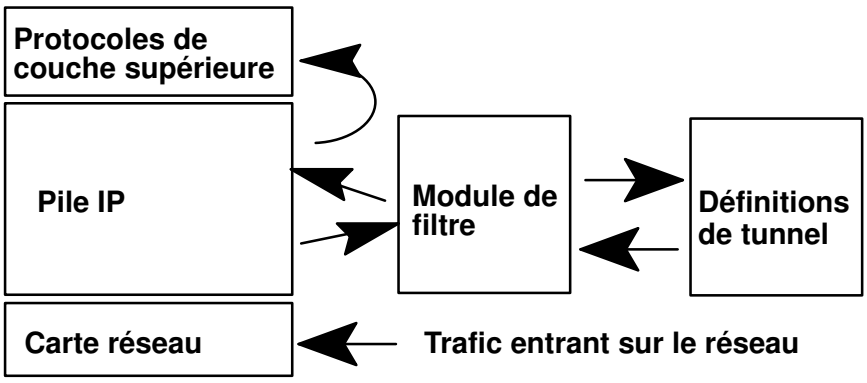
Tunnels / Filtres

La sécurité IP se distingue par deux composants liés mais distincts : *les tunnels* et les *filtres.* Les tunnels nécessitent les filtres, mais les filtres peuvent se passer de tunnels.

Le *filtrage* est une fonction de base qui permet d'accepter ou de refuser les paquets entrants ou sortants en fonction d'un certain nombre de critères. Ainsi, un administrateur système peut configurer le système hôte afin de gérer l'échange de données entre cet hôte et d'autres systèmes hôtes. Le filtrage s'effectue à partir des propriétés des paquets, telles que les adresses source et de destination, la version IP (4 ou 6), les masques de sous–réseau, le protocole, le port, les propriétés de routage, la fragmentation, l'interface et la définition des tunnels. Ce filtrage s'effectue au niveau de la couche IP ; aucune modification ne s'impose donc au niveau des applications.

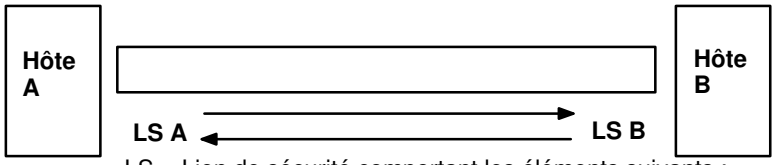
Les *tunnels* définissent un lien de sécurité entre deux systèmes hôtes. Ces liens de sécurité impliquent des paramètres de sécurité spécifiques qui sont partagés par les systèmes de part et d'autre du tunnel.

Le schéma suivant illustre la manière dont un paquet arrive sur la pile IP au niveau de la carte réseau. A partir de là, le module de filtrage est appelé pour déterminer si le paquet doit être autorisé ou refusé. Si un ID de tunnel est spécifié, le paquet subit un contrôle par rapport aux définitions de tunnel existantes. Si la décapsulation du tunnel se déroule correctement, la paquet est transmis au protocole de la couche supérieure. Cette fonction s'effectue dans l'ordre inverse pour les paquets sortants. Le tunnel s'appuie sur une règle de filtrage qui associe le paquet à un tunnel donné, mais la fonction de filtrage peut se produire sans transmission du paquet au tunnel.



Tunnels et liens de sécurité

Les tunnels servent à tout moment à authentifier ou chiffrer les données. Les tunnels sont définis en spécifiant un lien de sécurité entre deux systèmes hôtes (voir illustration). Le lien de sécurité définit les paramètres des algorithmes de chiffrement et d'authentification et des caractéristiques du tunnel.



LS = Lien de sécurité comportant les éléments suivants :
- Adresse de destination
- Valeur SPI
- Clé
- Algorithme de chiffrement et format
- Algorithme d'authentification
- Durée de vie de la clé

Mise en place d'un tunnel sécurisé entre les hôtes A et B

La valeur SPI (Security Parameter Index) et l'adresse de destination permettent d'identifier un lien de sécurité unique. Aussi, ces deux paramètres sont nécessaires pour définir de manière unique un tunnel. D'autres paramètres, comme l'algorithme de chiffrement, l'algorithme d'authentification, les clés et la durée de vie, peuvent être spécifiés. Vous pouvez toujours utiliser les valeurs par défaut.

Choix d'un type de tunnel

Le choix entre les tunnels IBM, les tunnels manuels ou, pour AIX versions 4.3.2 et ultérieures, les tunnels IKE, dépend de la prise en charge du tunnel par le système distant situé à l'autre extrémité et le type de gestion des clés choisi. Chaque fois que possible, les tunnels IKE sont préférables car ils proposent une négociation de clés sécurisée et une mise à jour de ces clés normalisée. Ils bénéficient également des nouveaux types d'en–tête de l'IETF ESP et AH et acceptent la protection contre les répétitions.

Les tunnels IBM peuvent être utilisés entre deux machines AIX quelconques exécutant AIX 4.3, ou entre un hôte AIX 4.3 et un hôte exécutant IBM Secure Network Gateway 2.2 ou IBM Firewall 3.1 ou 3.2. Les tunnels manuels peuvent être utilisés entre un hôte exécutant AIX Version 4.3 et toute autre machine dotée de la sécurité IP et proposant un ensemble commun d'algorithmes de chiffrement et d'authentification. Dans leur grande majorité, les fournisseurs proposent Keyed MD5 avec DES ou HMAC MD5 avec DES. Il s'agit du sous-ensemble de base qui fonctionne avec presque toutes les implémentations de la fonction de sécurité IP.

Lors de la configuration des tunnels manuels ou IBM, la procédure varie selon que vous configurez le premier hôte du tunnel ou le deuxième, dont les paramètres doivent correspondre à la configuration du premier hôte. Si vous configurez le premier hôte, les clés sont générées automatiquement, et les algorithmes peuvent être définis par défaut. Si vous

configurez le deuxième hôte, la meilleure solution consiste à importer, si possible, les informations du tunnel à partir du système distant.

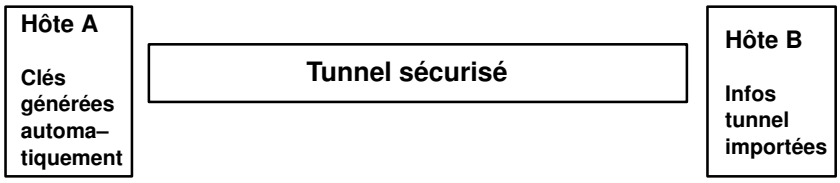
Autre élément important : déterminer si le système distant est situé derrière un pare-feu. Si tel est le cas, la configuration doit comporter les informations sur le pare-feu en question.

Configuration de base (tunnels manuels ou IBM)

Configuration des tunnels et des filtres

Pour la cas le plus simple de configuration d'un tunnel manuel, il n'est pas nécessaire de configurer séparément les règles de filtre. Si tout le trafic échangé entre les deux hôtes passe par le tunnel, les règles de filtre requises sont générées automatiquement. La procédure de configuration d'un tunnel consiste à définir le tunnel à une extrémité, importer la définition à l'autre extrémité, et à activer le tunnel et les règles de filtre aux deux extrémités. Le tunnel est alors prêt à l'emploi.

Les informations concernant le tunnel doivent être identiques aux deux extrémités si elles ne sont pas fournies de manière explicite (voir illustration). A titre d'exemple, les algorithmes de chiffrement et d'authentification spécifiés pour l'adresse source seront utilisés pour l'adresse de destination si les valeurs de destination ne sont pas spécifiées. Cette opération simplifie la création du tunnel.



Tunnel manuel avec les algorithmes HMAC MD5 et DES CBC 8

Création d'un tunnel manuel au niveau de l'hôte A

Vous pouvez configurer un tunnel à l'aide de l'application Web-based System Manager wsm network, du raccourci SMIT **ips4_basic** (pour IP version 4) ou **ips6_basic** (pour IP version 6), ou suivre la procédure suivante :

L'exemple suivant illustre la commande **gentun** utilisée pour créer un tunnel manuel :

```
gentun –v 4 –t manual –s 5.5.5.19 –d
5.5.5.8 –a HMAC_MD5 –e DES_CBC_8 –N 23567
```

Cette ligne de commande permet de créer un tunnel, dont la sortie (avec **lstun –v4**) se présente comme suit :

```
Tunnel ID           : 1
IP Version          : IP Version 4
Source              : 5.5.5.19
Destination         : 5.5.5.8
Policy              : auth/encr
Tunnel Mode         : Définitions
Send AH Algo        : HMAC_MD5
Send ESP Algo       : DES_CBC_8
Receive AH Algo     : HMAC_MD5
Receive AH Algo     : DES_CBC_8
Source AH SPI       : 300
Source ESP SPI      : 300
Dest AH SPI         : 23576
Dest ESP SPI        : 23576
Tunnel Life Time    : 480
Status              : Inactive
Target              : -
Target Mask         : -
Replay              : Non
New Header          : Oui
Snd ENC-MAC Algo    : -
Rcv ENC-MAC Algo    : -
```

Le tunnel est activé lorsque la commande **mktun** est lancée :

```
mktun -v 4 -t1
```

Les règles de filtre associées au tunnel sont générées automatiquement et la sortie (avec **lsfilt –v4**) se présente comme suit :

```
Rule 4:
Rule action             : permit
Source Address          : 5.5.5.19
Source Mask             : 255.255.255.255
Destination Address     : 5.5.5.8
Destination Mask        : 255.255.255.255
Source Routing          : yes
Protocol                : all
Source Port             : any 0
Destination Port        : any 0
Scope                   : both
Direction               : outbound
Logging control         : no
Fragment control        : all packets
Tunnel ID number        : 1
Interface               : all
Auto-Generated          : yes

Rule 5:
Rule action             : permit
Source Address          : 5.5.5.8
Source Mask             : 255.255.255.255
Destination Address     : 5.5.5.19
Destination Mask        : 255.255.255.255
Source Routing          : yes
Protocol                : all
Source Port             : any 0
Destination Port        : any 0
Scope                   : both
Direction               : inbound
Logging control         : no
Fragment control        : all packets
Tunnel ID number        : 1
Interface               : all
Auto-Generated          : yes
```

Ces règles de filtre sont activées en plus des règles de filtre par défaut via la commande **mktun –v 4 –t 1**.

Pour configurer l'autre extrémité, s'il s'agit d'un autre système AIX, la définition du tunnel peut être exportée vers l'hôte A, puis importée sur l'hôte B.

Exportation :

```
exptun –v 4 –t 1 –f /tmp
```

Cette opération permet d'exporter la définition du tunnel dans un fichier nommé **ipsec_tun_manu.exp** et les règles de filtre associées dans le fichier **ipsec_fltr_rule.exp** contenu dans le répertoire indiqué par l'indicateur **–f**.

Création d'un tunnel manuel au niveau de l'hôte B :

Pour créer l'extrémité du tunnel correspondante, les fichiers d'exportation sont copiés vers l'extrémité distante et importés sur le système distant AIX 4.3 à l'aide de la commande :

```
imptun –v 4 –t 1 –f /tmp
```

`1` étant le tunnel à importer et /*tmp* le répertoire des fichiers d'importation. Ce numéro de tunnel est généré par le système et doit être référencé à partir de la sortie via la commande **gentun** ou à l'aide de la commande **lstun** afin de répertorier les tunnels et déterminer le numéro de tunnel correct à importer. Dans le cas d'un seul tunnel figurant dans le fichier d'importation ou si la totalité des tunnels doivent être importés, alors l'option **–t** est nécessaire.

Si le système distant ne fonctionne pas sous AIX 4.3, le fichier d'exportation peut servir de référence pour la configuration de l'algorithme, des clés et des valeurs SPI de l'autre extrémité du tunnel.

Les fichiers d'exportation d'IBM Secure Network Gateway (SNG) peuvent être importés afin de créer des tunnels sous AIX 4.3. Pour ce faire, utilisez le paramètre **–n** lors de l'importation du fichier :

```
imptun -v 4 -f /tmp -n
```

Création d'un tunnel IBM au niveau de l'hôte A :

La configuration d'un tunnel IBM s'apparente à celle d'un tunnel manuel, mais certaines options sont différentes au niveau des algorithmes de chiffrement et les clés sont négociées dynamiquement, ce qui rend inutile l'importation des clés. Les tunnels IBM sont limités à l'algorithme Keyed MD5 pour l'authentification. Si vous souhaitez utiliser les algorithmes HMAC MD5 ou HMAC SHA, vous devez utilisez un tunnel manuel.

```
gentun -s 9.3.100.1 -d 9.3.100.245 -t IBM -e
DES_CBC_8 -n 35564
```

A partir de là, comme pour les tunnels manuels, le tunnel et la table des filtres doivent être activés pour rendre le tunnel actif :

```
mktun -v 4 -t1
```

Pour configurer l'autre extrémité, s'il s'agit d'un autre système AIX 4.3 avec la fonction de sécurité IP, la définition du tunnel peut être exportée vers l'hôte A, puis importée sur l'hôte B.

Exportation :

```
exptun -v 4 -f /tmp
```

Cette opération permet d'exporter la définition du tunnel dans un fichier nommé **ipsec_tun_ibm.exp** et les règles de filtre associées dans le fichier **ipsec_fltr_rule.exp** contenu dans le répertoire indiqué par l'indicateur **–f**.

Création d'un tunnel IBM au niveau de l'hôte B

La procédure est identique à celle utilisée pour créer l'autre extrémité du tunnel au niveau de l'hôte B pour un tunnel IBM. La définition du tunnel est exportée de l'hôte A vers l'hôte B. L'indicateur **–n** peut être utilisé pour un fichier exporté par un système exécutant IBM Secure Network Gateway ou IBM Firewall 3.1/3.2.

Règles de filtres statiques et exemples

Le filtrage peut être simple, utilisant en grande partie les règles de filtre générées automatiquement, ou élaboré en définissant des fonctions de filtre spécifiques à partir des propriétés des paquets IP. La mise en correspondance des paquets entrants s'effectue par comparaison de l'adresse source et de la valeur SPI avec les valeurs répertoriées dans la table des filtres. La parité doit donc être unique.

Chaque ligne de la table des filtres est une *règle*. Une série de règles permet de définir l'autorisation ou le refus d'accès des paquets au départ et à l'arrivée du système, et leur mode de routage. Les règles de filtre peuvent être créées à partir des adresses et des masques source et de destination, du protocole, du numéro de port, de la direction, du contrôle des fragments, du routage source, du tunnel et de l'interface.

L'exemple décrit ci–dessous illustre un ensemble de règles de filtres. Pour chaque règle, les champs sont présentés dans l'ordre suivant (un exemple de chaque champ de la règle 1 est illustré entre parenthèses) : Numéro_règle (`1`), Action (`permit`), Adr_source (`0.0.0.0`), Masque_source (`0.0.0.0`), Adr_dest (`0.0.0.0`), Masque_dest (`0.0.0.0`), Routage_source (`no`), Protocole (`udp`), Opérateur_prt_src (`eq`), Valeur_prt_src (`4001`), Opérateur_prt_dst (`eq`), Valeur_prt_dest (`4001`), Portée (`both`), Direction (`both`), Journalisation (`no`), Fragment (`all packets`), Tunnel (`0`)et Interface (`all`).

```
1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no udp eq 4001 eq 4001
both both no all packets 0 all

2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no ah any 0 any 0 both
both no all packets 0 all

3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no esp any 0 any 0 both
both no all packets 0 all

4 permit 10.0.0.1 255.255.255.255 10.0.0.2 255.255.255.255 no all
any 0 any 0 both outbound no all packets 1 all

5 permit 10.0.0.2 255.255.255.255 10.0.0.1 255.255.255.255 no all
any 0 any 0 both inbound no all packets 1 all

6 permit 10.0.0.1 255.255.255.255 10.0.0.3 255.255.255.255 no tcp
lt 1024 eq 514 local outbound yes all packets 2 all

7 permit 10.0.0.3 255.255.255.255 10.0.0.1 255.255.255.255 no
tcp/ack eq 514 lt 1024 local inbound yes all packets 2 all

8 permit 10.0.0.1 255.255.255.255 10.0.0.3 255.255.255.255 no
tcp/ack lt 1024 lt 1024 local outbound yes all packets 2 all

9 permit 10.0.0.3 255.255.255.255 10.0.0.1 255.255.255.255 no tcp
lt 1024 lt 1024 local inbound yes all packets 2 all

10 permit 10.0.0.1 255.255.255.255 10.0.0.4 255.255.255.255 no icmp
any 0 any 0 local outbound yes all packets 3 all

11 permit 10.0.0.4 255.255.255.255 10.0.0.1 255.255.255.255 no icmp
any 0 any 0 local inbound yes all packets 3 all

12 permit 10.0.0.1 255.255.255.255 10.0.0.5 255.255.255.255 no tcp
gt 1023 eq 21 local outbound yes all packets 4 all

13 permit 10.0.0.5 255.255.255.255 10.0.0.1 255.255.255.255 no
tcp/ack eq 21 gt 1023 local inbound yes all packets 4 all

14 permit 10.0.0.5 255.255.255.255 10.0.0.1 255.255.255.255 no tcp
eq 20 gt 1023 local inbound yes all packets 4 all

15 permit 10.0.0.1 255.255.255.255 10.0.0.5 255.255.255.255 no
tcp/ack gt 1023 eq 20 local outbound yes all packets 4 all

16 permit 10.0.0.1 255.255.255.255 10.0.0.5 255.255.255.255 no tcp
gt 1023 gt 1023 local outbound yes all packets 4 all

17 permit 10.0.0.5 255.255.255.255 10.0.0.1 255.255.255.255 no
tcp/ack gt 1023 gt 1023 local inbound yes all packets 4 all

18 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no all any 0 any 0 both
both yes all packets
```

La règle 1 concerne le démon de la clé de session IBM et n'apparaît que dans les tables de filtres du protocole IP version 4. Elle utilise le numéro de port 4001 afin de contrôler les paquets pour une actualisation de la clé de session. Cet exemple illustre le mode d'utilisation du numéro de port pour une tâche spécifique. Cette règle de filtre ne doit pas être modifiée sauf pour une configuration de la journalisation.

Les règles 2 et 3 servent à autoriser le traitement des en-têtes AH (Authentication Header) et des en-têtes ESP (Encapsulating Security Payload). Cette règle de filtre ne doit pas être modifiée sauf pour une configuration de la journalisation.

Les règles 4 et 5 représentent un ensemble de règles générées automatiquement qui filtrent les données échangées entre les adresses 10.0.0.1 et 10.0.0.2 via le tunnel 1. La règle 4 est réservée au trafic sortant et la règle 5 au trafic entrant.

Les règles 6 à 9 représentent un ensemble de règles définies par l'utilisateur permettant de filtrer les services sortants **rsh**, **rcp**, **rdump**, **rrestore** et **rdist** échangés entre les adresses 10.0.0.1 et 10.0.0.3 via le tunnel 2. A noter que la journalisation est définie sur `yes` et permet à l'administrateur de gérer ce type de trafic.

Les règles 10 et 11 représentent un ensemble de règles définies par l'utilisateur qui filtrent à la fois le trafic entrant et sortant **icmp** échangé entre les adresses 10.0.0.1 et 10.0.0.4 via le tunnel 3.

Les règles 12 à 17 représentent des règles de filtre définies par l'utilisateur permettant de filtrer le service FTP sortant échangé entre les adresses 10.0.0.1 et 10.0.0.5 via le tunnel 4.

La règle 18 est une règle générée automatiquement toujours placée en fin de table. Dans ce cas, elle autorise les paquets qui ne correspondent pas aux autres règles de filtre. Vous pouvez cependant refuser tous les paquets qui ne correspondent pas aux autres règles de filtre.

Chaque règle peut être affichée séparément (avec **lsfilt**) pour une meilleure lisibilité des différents champs. Par exemple :

```
Rule 1:
Rule action             : permit
Source Address          : 0.0.0.0
Source Mask             : 0.0.0.0
Destination Address     : 0.0.0.0
Destination Mask        : 0.0.0.0
Source Routing          : yes
Protocol                : udp
Source Port             : eq  4001
Destination Port        : eq  4001
Scope                   : both
Direction               : both
Logging control         : no
Fragment control        : all packets
Tunnel ID number        : 0
Interface               : all
Auto-Generated          : yes
```

Vous trouverez ci-dessous la liste de tous les paramètres pouvant être spécifiés dans une règle de filtre :

–v Version IP : 4 ou 6.

–a Action :

- **d** Refuser
- **p** Autoriser

–s Adresse source. Il peut s'agir d'une adresse IP ou du nom de l'hôte.

–m Masque de sous-réseau source.

–d Adresse de destination. Il peut s'agir d'une adresse IP ou du nom de l'hôte.

–M Masque de sous-réseau de destination.

–g Contrôle du routage source : `y` ou `n`.

–c Protocole : Les valeurs peuvent être `udp` , `icmp`, `tcp`, `tcp/ack`, `ospf`, `pip`, `esp` , `ah` et `all`.

–o Port source ou opération de type ICMP.

–p Port source ou valeur de type ICMP.

–O Port de destination ou opération de code ICMP.

–P Port de destination ou valeur de code ICMP.

–r Routage.

- **r** Paquets réacheminés
- **l** paquets origine/destination locale
- **b** Les deux

–l Gestion des journaux.

- **y** Inclure dans le journal
- **n** Ne pas inclure dans le journal.

–f Fragmentation.

- **y** S'applique aux en–têtes de fragment, aux fragments et aux non fragmentés
- **o** Ne s'applique qu'aux fragments et en–têtes de fragment
- **n** Ne s'applique qu'aux non fragmentés
- **h** Ne s'applique qu'aux non fragmentés et en–têtes de fragment

–t ID tunnel.

–i Interface, telle que `tr0` ou `en0`.

Pour plus d'informations sur genfilt et chfilt reportez-vous à *AIX Commands Reference*.

Règles de filtre générées automatiquement et définies par l'utilisateur

Certaines règles sont générées automatiquement pour l'utilisation du filtre de sécurité IP et du code tunnel. Parmi ces règles figurent celles décrites ci-dessus concernant le démon de clé de session destiné à actualiser les clés dans IKE (AIX versions 4.3.2 ou plus) ou les tunnels IBM (IP version 4 uniquement) et les règles chargées de traiter les paquets AH et ESP. Les règles de filtre sont également générées automatiquement lors de la définition des tunnels. Elles spécifient les valeurs de l'adresse source et de destination et du masque, ainsi que l'ID du tunnel. La totalité des données échangées entre ces adresses transitent via le tunnel. Comme les règles générées automatiquement autorisent la totalité du trafic via le tunnel, les règles définies par l'utilisateur peuvent être nécessaires afin de définir des restrictions sur certains types d'échanges. Ces règles définies par l'utilisateur doivent être placées avant les règles générées automatiquement car la première règle s'appliquant au paquet est utilisée. L'exemple ci-dessous illustre des règles de filtre définies par l'utilisateur permettant de filtrer les échanges de données en fonction de l'opération ICMP.

Comme les règles générées automatiquement autorisent la totalité du trafic via le tunnel, les règles définies par l'utilisateur peuvent être nécessaires afin de définir des restrictions sur certains types d'échanges. Ces règles définies par l'utilisateur doivent être placées avant les règles générées automatiquement car la première règle s'appliquant au paquet est utilisée. L'exemple ci-dessous illustre des règles de filtre définies par l'utilisateur permettant de filtrer les échanges de données en fonction de l'opération ICMP.

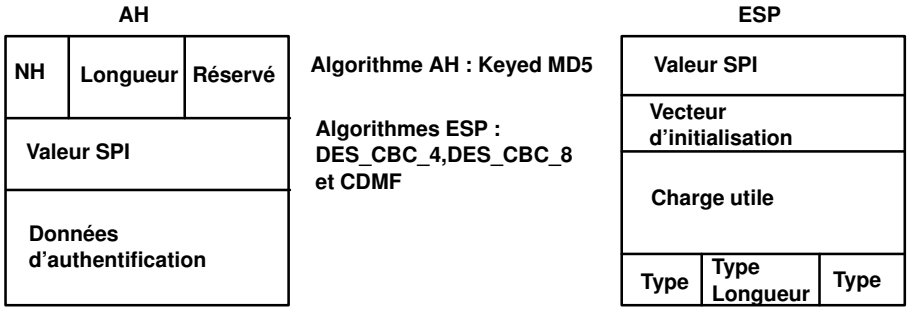
```
1 permit 10.0.0.1 255.255.255.255 10.0.0.4 255.255.255.255 no
icmp any 8
any 0 local outbound no all packets 3 all
2 permit 10.0.0.4 255.255.255.255 10.0.0.1 255.255.255.255 no
icmp any 0 any 0
local inbound no all packets 3 all
3 permit 10.0.0.4 255.255.255.255 10.0.0.1 255.255.255.255 no
icmp any 8 any 0
local inbound no all packets 3 all
4 permit 10.0.0.1 255.255.255.255 10.0.0.4 255.255.255.255 no
icmp any 0 any 0
local outbound no all packets 3 all
```

Les règles de filtre sont générées automatiquement lorsque les tunnels sont définis. Cela permet de simplifier la configuration d'un seul tunnel. Cette fonction peut être supprimée en spécifiant l'indicateur **–g** dans `gentun`. Vous pouvez rechercher un exemple de filtre avec les commandes **genfilt** afin de générer les règles de filtre pour les différents services TCP/IP dans **/usr/samples/ipsec/filter.sample**.

Configuration avancée des tunnels manuels

La configuration des tunnels autorise la définition d'un grand nombre de paramètres afin de garantir une compatibilité avec d'autres implémentations de sécurité IP. Certains exemples sont indiqués ici pour décrire les fonctions qui peuvent être sélectionnées.

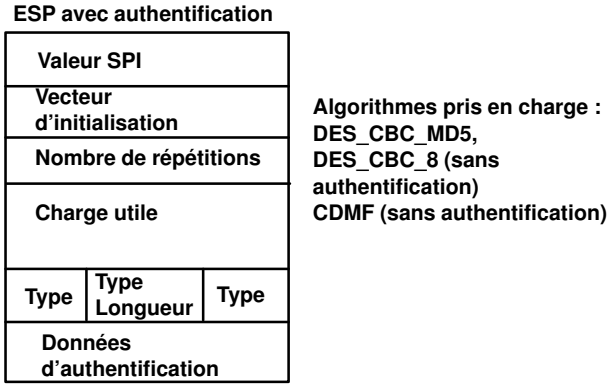
Les paquets sont formés pour les en-têtes AH pour l'authentification, les en-têtes ESP pour le chiffrement ou le nouveau format d'en–tête ESP qui autorise à la fois des données chiffrées et d'authentification dans le même paquet (voir l'illustration). Dans les normes RFC concernant AH et ESP définies en 1995, (RFC 1826 pour AH et RFC 1829 pour ESP), deux en-têtes étaient nécessaires pour définir l'authentification et le chiffrement.



Pour configurer un tunnel avec DES CBC MD5, l'en-tête combiné ESP est utilisé avec l'algorithme de chiffrement ESP défini avec DES_CBC_8 et l'algorithme d'authentification AH défini avec HMAC MD5. Pour utiliser cet algorithme d'authentification, indiquez-le avec l'indicateur **–b**, et indiquez ses clés avec l'indicateur **–c**. Par exemple :

```
gentun -v 4 -t manual -s 5.5.5.19 -d 5.5.5.23
-e DES_CBC_8 -b HMAC_MD5 -N 2349473
```

Cette commande génère un tunnel qui utilise l'algorithme DES CBC MD5 avec des clés générées automatiquement (voir l'illustration). Les données chiffrées et les données d'authentification sont contenues dans le même en-tête ESP. Elle prend en charge également les protections contre les répétitions, qui ne sont pas recommandées pour les tunnels manuels. Elle est disponible dans cette version pour garantir une compatibilité avec d'autres implémentations et pour les besoins des tests.



Configuration des tunnels IKE

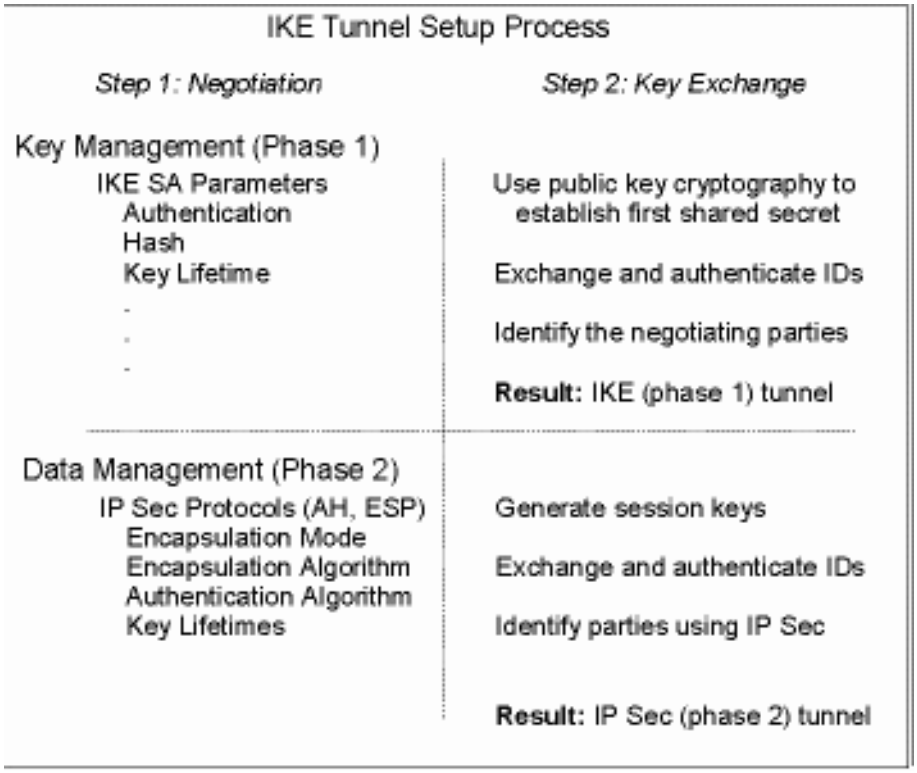
Les tunnels Internet Key Exchange (IKE) ont des paramètres de politique plus complexes. C'est pourquoi, l'interface Web-based System Manager doit être utilisée pour les configurer. La génération de tunnels IKE diffère de celle des tunnels IBM ou manuels car la définition de la politique de sécurité est distincte de la définition des points d'extrémité des tunnels. Dans l'IKE, le processus de négociation comporte deux étapes, appelées *phases*, qui peuvent avoir des politiques de sécurité distinctes.

Au démarrage de la négociation IKE, un canal sécurisé doit être défini. Il s'agit de la phase de *gestion de clés* ou *phase 1*. Au cours de celle–ci, chaque partie utilise des clés pré–partagées pour son authentification et transmet des données d'identification. Cette phase configure un lien de sécurité au sein duquel les deux parties déterminent leur mode de communication sécurisé, puis les protections à utiliser pour communiquer au cours de la deuxième phase. Un tunnel *IKE* ou *de phase 1* est ainsi généré.

La deuxième phase est appelée phase de *gestion de données* ou *phase 2*. Elle utilise le tunnel IKE afin de générer les liens de sécurité IP Sec pour AH et ESP qui protègent réellement le trafic. La deuxième phase détermine également les données utilisant le tunnel IP Sec. Elle peut définir par exemple :

- un masque de sous–réseau,
- une gamme d'adresses
- ou un protocole associé à un numéro de port

(voir figure).



Dans de nombreux cas, les points d'extrémité du tunnel IKE de gestion de clés sont identiques à ceux du tunnel IP Sec de gestion des données. Les points d'extrémité du tunnel IKE sont les identifiants des machines qui mènent la négociation. Les points d'extrémité du tunnel IP Sec décrivent le type de trafic utilisant le tunnel de sécurité IP. Pour les tunnels hôte à hôte simples, dans lesquels tout le trafic est protégé par le même tunnel, les points d'extrémité de tunnel de phases 1 et 2 sont identiques. Si les deux parties impliquées dans la négociation sont des passerelles, elles constituent les points d'extrémité du tunnel IKE, ceux des tunnels IP Sec sont les machines ou les sous–réseaux, voire la gamme d'adresses (en amont des passerelles) des utilisateurs du tunnel.

Paramètres de gestion de clés (phase 1) – Identification du tunnel

Tunnel de gestion de clés (phase 1)

Nom du tunnel IKE. Les points d'extrémité de la négociation doivent être spécifiés pour chaque tunnel. Il s'agit des deux machines devant transmettre et valider des messages IKE. Le nom du tunnel peut décrire les points d'extrémité du tunnel tels que `VPN Boston` ou `VPN Acme`.

Host Identity Type

Type d'ID utilisé dans l'échange IKE. Le type d'ID et la valeur doivent correspondre à la valeur de la clé pré–partagée afin de garantir la consultation des clés appropriées. Si un ID distinct est utilisé pour rechercher une valeur de clé pré–partagée, le *host ID* est celui de la clé et son *type* est KEY_ID. Ce dernier est utile dans le cas d'un hôte ayant plusieurs valeurs de clés pré–partagées.

Host Identity Valeur de l'ID d'hôte représentée comme une adresse IP, un nom de domaine pleinement qualifié (FQDN) ou un utilisateur du nom de domaine pleinement qualifié (*user@FQDN*).

IP Address Adresse IP de l'hôte distant. Cette valeur est requise lorsque le type d'ID de l'hôte est KEY_ID ou chaque fois que ce type ne peut pas être résolu en une adresse IP. A titre d'exemple, si le nom d'utilisateur ne peut pas être résolu avec un serveur de noms local, il est nécessaire d'entrer l'adresse IP du point d'extrémité distant.

Politique relative aux clés (phase 1)

Lors de la configuration d'un tunnel IKE avec l'application réseau Web-based System Manager (raccourci **wsm network**), vous pouvez choisir entre plusieurs politiques de gestion de clés prédéfinies qui s'appliquent dans la plupart des cas. Elles varient en fonction du type d'algorithmes de chiffrement et d'authentification définis.

Vous pouvez également personnaliser la politique de gestion de clés en définissant les paramètres à utiliser lors de la négociation IKE. Pour la phase 1, l'utilisateur doit déterminer certaines propriétés de sécurité en matière de gestion de clés afin de procéder à l'échange. Ces propriétés sont entièrement reprises dans l'aide du Web-based System Manager et dans la documentation relative à la commande **ike**.

Politique de gestion des données (phase 2)

Les paramètres de gestion des données sont les mêmes paramètres de sécurité IP que ceux qui sont utilisés pour les tunnels manuels. Ils décrivent le type de protection à utiliser pour l'échange de données dans ce tunnel. Vous pouvez démarrer plusieurs tunnels de phase 2 sous le même tunnel de phase 1. Il existe plusieurs politiques prédéfinies pour simplifier la configuration. Elles peuvent également être utilisées comme modèle de mise en œuvre des mesures de sécurité personnalisées.

Pour mettre en œuvre ce type de politique, il est possible d'en définir les paramètres spécifiques, auquel cas le nom de la politique doit être saisi pour établir la corrélation entre les points d'extrémité du tunnel et la politique correspondante.

Les types d'ID des points d'extrémité suivants décrivent le type de données devant utiliser le tunnel de données de sécurité IP :

Host, **Subnet** ou **Range**
Ces éléments précisent si le trafic de données empruntant le tunnel est destiné à un hôte, à un sous–réseau ou à une gamme d'adresses en particulier.

Host/Subnet ID Contient l'identité d'hôte ou de sous–réseau des systèmes locaux ou distants acheminant des données par ce tunnel. Détermination des ID envoyées au cours de la négociation de phase 2 et des règles de filtres établies si la négociation se déroule correctement.

Subnet mask Décrit toutes les adresses IP au sein du sous–réseau (par exemple, hôte 9.53.250.96 et masque 255.255.255.0)

Starting IP Address Range
Adresse IP de démarrage pour la gamme d'adresses devant utiliser le tunnel (par exemple, 9.53.250.96 de 9.53.250.96 à 9.53.250.93).

Ending IP Address Range
Adresse IP de fin pour la gamme d'adresses devant utiliser le tunnel (par exemple, 9.53.250.93 de 9.53.250.96 à 9.53.250.93)

Port Description des données utilisant un numéro de port spécifique (par exemple, 21 ou 23)

Protocol Description des données acheminées via un protocole spécifique (par exemple, TCP ou UDP). Détermination du protocole envoyé au cours de la négociation de phase 2 et des règles de filtres établies si la négociation se déroule correctement. Les protocoles des points d'extrémité local et distant doivent correspondre.

Les paramètres de gestion des données sont entièrement repris dans l'aide du Web-based System Manager et dans la documentation relative à la commande **ike**.

Exemple de configuration d'un tunnel IKE

Il existe des scénarios standard qui décrivent les types de situations rencontrés par la plupart des clients lors de la configuration des tunnels, dans le cas d'une succursale, d'un partenaire commercial et pour un accès distant.

Dans le cas d'une succursale, le client a deux réseaux sécurisés qu'il souhaite interconnecter (le groupe Engineering sur deux sites différents). Dans cet exemple, il existe des passerelles et tout le trafic transitant par celles–ci utilise le même tunnel. Le trafic aux deux extrémités du tunnel est décapsulé et passe en clair dans le réseau interne de la société.

Dans la première phase de la négociation IKE, le lien de sécurité IKE est créé entre les deux passerelles. Le trafic qui emprunte le tunnel de sécurité IP est celui des deux sous–réseaux. En outre, les ID de sous–réseau sont utilisées dans la négociation de phase 2. Un numéro de tunnel est généré suite à la saisie des paramètres du tunnel et de la politique sécuritaire. Pour lancer le tunnel, utilisez la commande **ike**.

Dans le scénario Partenaire commercial, les réseaux ne sont pas sécurisés. En outre, il se peut que l'administrateur réseau veuille limiter l'accès à un nombre plus restreint d'hôtes en amont de la passerelle de sécurité. Dans ce cas, le tunnel entre les hôtes acheminera des données protégées par IP Sec devant être utilisées entre deux hôtes en particulier. Ce faisant, le protocole du tunnel de phase 2 est AH ou ESP.

Dans le scénario de l'accès distant, les tunnels doivent être configurés à la demande et assortis d'un niveau de sécurité élevé. Les adresses IP ne doivent pas revêtir une signification particulière. Toutefois, il est préférable d'utiliser des noms de domaines pleinement qualifiés ou des *user at*. Vous pouvez aussi utiliser KEYID pour associer une clé à un ID d'hôte.

Accédez à WebSM pour configurer le tunnel. Utilisez **wsm network** comme raccourci pour passer à la section TCP /IP. Sous Virtual Private Networking (réseau privé virtuel), lancez la

fonction de sécurité IP en cliquant dans la partie supérieure sur l'option "Selected" (Sélectionné). Ce faisant, les extensions du noyau de sécurité IP sont chargées et les démons isakmpd et tmd sont activés. Un tunnel est créé. Il résulte de la définition des points d'extrémité de phases 1 et 2 ainsi que de leurs politiques sécuritaires associées. La phase 1 est la phase d'authentification. Elle demande des temps de calcul importants et n'est pas souvent utilisée. Elle configure un canal de sécurité entre les parties impliquées dans la négociation. Ce canal est nécessaire préalablement au calcul définitif des clés et des paramètres de la fonction de sécurité IP. La phase 2 décrit le type de trafic empruntant un tunnel spécifique. Elle peut être configurée pour un hôte unique ou un groupe d'hôtes (en utilisant des subnets ou des gammes IP) avec le protocole et les numéros de ports définis. Le tunnel de phase 1 peut être utilisé pour protéger plusieurs négociations de phase 2 et rafraîchissements de clés tant que celles–ci interviennent entre les deux mêmes points d'extrémité (entre deux passerelles, par exemple).

Pour définir les points d'extrémité de tunnel de phase 1, cliquez sur "Internet Key Exchange (IKE) Tunnels" (Tunnels IKE). Les données entrées à ce niveau déclinent l'identité des systèmes prenant part aux négociations. Dans la plupart des cas, les adresses IP sont utilisées et une politique compatible avec le point d'extrémité distant doit être sélectionnée. IBM_low_prekey et IBM_med_prekey utilisent le chiffrement DES et des clés pré–partagées en mode agressif. IBM_high_prekey utilise le chiffrement Triple DES en mode principal, également appelé mode de protection d'identité. Utilisez des politiques compatibles à chaque point d'extrémité ou demandez à l'administrateur à l'extrémité distante d'en définir une. Il est possible de créer une politique assortie de plusieurs options afin de permettre une certaine souplesse dans l'offre ou la mise en concordance d'une politique.

Les clés pré–partagées doivent également être entrées au niveau de l'onglet correspondant et cette valeur doit être identique sur les machines distantes et locales. Faites précéder cette valeur de 0X (valeur hexadécimale).

L'option "Key Management (Phase 1) Protection Policies" (politiques de protection de la gestion des clés) est utilisée pour sélectionner la politique spécifique associée au tunnel. Vous avez le choix entre plusieurs politiques prédéfinies ou vous pouvez en créer une nouvelle.

De même, les politiques et les points d'extrémité des tunnels de phase 2 sont créés en définissant les politiques et les tunnels correspondants. A ce niveau, le tunnel peut être lancé à l'aide de l'interface utilisateur graphique de WebSM ou à partir de la ligne de commande en entrant la commande **ike**.

Pour lancer une négociation de tunnel ou pour permettre au système destinataire d'agir comme un répondeur (en fonction du rôle imparti), la commande **ike** peut être utilisée avec un numéro de tunnel, tel qu'illustré dans l'exemple suivant :

```
ike cmd=activate numlist=1
```

Les adresses IP peuvent également être utilisées. A titre d'exemple :

```
ike cmd=activate ipaddr=9.3.97.100,9.3.97.256
```

L'exécution des commandes peut prendre plusieurs secondes. C'est pourquoi, la commande ne se réaffiche qu'après lancement de la négociation. Pour vérifier le bon déroulement de la commande, utilisez l'option de liste pour afficher l'état du tunnel.

```
ike cmd=list
Phase 1 Tunnel ID       [1]
Phase 2 Tunnel ID       [1]
```

Cette liste affiche les tunnels de phases 1 et 2 actuellement activés. Pour dresser une liste complète du tunnel, procédez comme suit :

```
ike cmd=list verbose
Phase 1 Tunnel ID       1
Local ID Type:          Fully_Qualified_Domain_Name
Local ID:               bee.austin.ibm.com
Remote ID Type:         Fully_Qualified_Domain_Name
```

```
Remote ID:              ipsec.austin.ibm.com
Mode:                   Aggressive
Security Policy:        BOTH_AGGR_3DES_MD5
Role:                   Initiator
Encryption Alg:         3DES-CBC
Auth Alg:               Preshared Key
Hash Alg:               MD5
Key Lifetime:           28800 Seconds
Key Lifesize:           0 Kbytes
Key Rem Lifetime:       28737 Seconds
Key Rem Lifesize:       0 Kbytes
Key Refresh Overlap:    5%
Tunnel Lifetime:        2592000 Seconds
Tunnel Lifesize:        0 Kbytes
Tun Rem Lifetime:       2591937 Seconds
Status:                 Active
Phase 2 Tunnel ID       1
Local ID Type:          IPv4_Address
Local ID:               10.10.10.1
Local Subnet Mask:      N/A
Local Port:             any
Local Protocol:         all
Remote ID Type:         IPv4_Address
Remote ID:              10.10.10.4
Remote Subnet Mask:     N/A
Remote Port:            any
Remote Portocol:        all
Mode:                   Oakley_quick
Security Policy:        ESP_3DES_MD5_SHA_TUNNEL_NO_PFS
Role:                   Initiator
Encryption Alg:         ESP_3DES
AH Transform:           N/A
Auth Alg:               HMAC-MD5
PFS:                    No
SA Lifetime:            600 Seconds
SA Lifesize:            0 Kbytes
SA Rem Lifetime:        562 Seconds
SA Rem Lifesize:        0 Kbytes
Key Refresh Overlap:    15%
Tunnel Lifetime:        2592000 Seconds
Tunnel Lifesize:        0 Kbytes
Tun Rem Lifetime:       2591962 Seconds
Assoc P1 Tunnel:        0
Encap Mode:             ESP_tunnel
Status:                 Active
```

L'activation du tunnel IKE entraîne l'insertion des règles de filtres du nouveau tunnel dans la table de filtres dynamique. Ces entrées peuvent être visualisées à l'aide de la commande lsfilt avec l'option –d pour les règles de filtres dynamiques :

```
1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no udp eq 4001 eq 4001
both both no all packets 0 all

2 *** Dynamic filter placement rule *** no

0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 yes all any 0 any 0 both
both no all packets 0 all

*** Dynamic table ***

0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no udp eq 500 eq 500
local both no all packets 0

0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no ah any 0 any 0 both
```

```
inbound no all packets 0

0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no esp any 0 any 0 both
inbound no all packets 0

1 permit 10.10.10.1 255.255.255.255 10.10.10.4 255.255.255.255 no
all any 0 any 0 both outbound yes all packets 1

1 permit 10.10.10.4 255.255.255.255 10.10.10.1 255.255.255.255 no
all any 0 any 0 both inbound yes all packets 1
```

Cet exemple présente une machine avec un tunnel IKE uniquement. La règle de filtre dynamique (règle n°2 dans cet exemple de table statique) peut être déplacée par l'utilisateur pour contrôler le placement de toutes les autres règles définies par ses soins. Les règles de la table dynamique sont générées automatiquement parallèlement à la négociation des tunnels. Les règles correspondantes sont insérées dans la table des filtres. Ces règles peuvent être affichées mais pas éditées.

Pour activer les fonctions de journalisation des règles de filtres dynamiques, choisissez l'option yes (oui) au niveau de la règle n°2 :

```
chfilt –v 4 –n 2 –l y
```

Pour plus d'informations sur la journalisation du trafic IKE, reportez–vous à la section Fonctions de journalisation, page 4-25.

Pour désactiver le tunnel, utilisez l'option remove (supprimer).

```
ike cmd=remove numlist=1
```

Règles de filtres prédéfinies

Un certain nombre de règles de filtres prédéfinies sont générées automatiquement avec certains événements. Lorsque l'unité `ipsec_v4` ou `ipsec_v6` est chargée, une règle prédéfinie est insérée dans la table des filtres puis activée. Par défaut, la règle prédéfinie est Permit All (tout autoriser), mais vous pouvez aussi leur attribuer la règle Deny All (tout refuser).

Remarque : Dans le cas d'une configuration à distance, assurez–vous que la règle Deny All n'est pas activée avant la fin de la configuration. Vous évitez ainsi l'interruption de votre session sur la machine. Afin d'éviter ce cas de figure, attribuez par défaut la règle Permit All ou configurez un tunnel sur la machine à distance avant d'activer ipsec.

Il existe une règle prédéfinie pour les tables de filtres IP versions 4 et 6. Vous pouvez leur attribuer indépendamment la règle Deny All. Cela permet de bloquer l'échange de données sauf si ces données sont définies par des règles de filtres supplémentaires. L'autre option à modifier parmi les règles prédéfinies est **chfilt** associée à l'option **–l**, qui permet de consigner les paquets respectant cette règle.

Pour prendre en charge les tunnels IKE, une règle de filtre dynamique est placée dans la table de filtres IPv4, à un endroit précis. La position de la règle peut être contrôlée par l'utilisateur qui peut la faire remonter ou descendre au sein de la table des filtres. Une fois le démon de gestion du tunnel et le démon **isakmpd** initialisés pour la négociation des tunnels IKE, des règles sont automatiquement générées dans la table de filtres dynamique afin de traiter les messages IKE ainsi que les paquets AH et ESP.

Règles de filtre prédéfinies

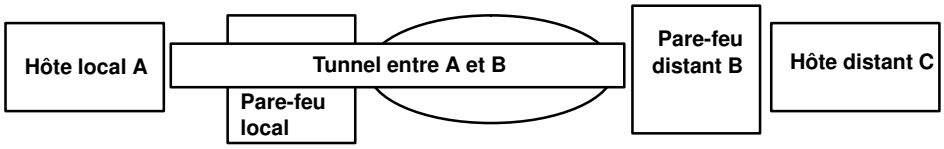
Un certain nombre de règles de filtre prédéfinies sont générées automatiquement avec certains événements. Lorsque la fonction de sécurité IP est chargée, une règle prédéfinie est insérée dans la table des filtres puis activée. Par défaut, la règle prédéfinie est Permit All (Tout autoriser). Cette règle vous donnera tous les accès dans le cas d'une configuration à distance. Il existe une règle prédéfinie à la fois pour les filtres IP Version 4 et IP Version 6. Vous pouvez leur attribuer la règle Deny All (Tout refuser). Cela permet de bloquer

l'échange de données sauf si les données sont définies par des règles de filtre supplémentaires. L'autre option à modifier parmi les règles prédéfinies est **chfilt** associée à l'option **–l**, qui permet de consigner les paquets respectant cette règle.

Hôte–pare–feu–hôte

L'option de configuration des tunnels hôte – pare-feu – hôte (voir schéma) permet de créer un tunnel entre votre système hôte et un pare-feu, puis de générer automatiquement les règles de filtre nécessaires pour établir une communication correcte entre votre système hôte et l'hôte situé derrière le pare-feu. Les règles de filtre générées automatiquement autorisent toutes les règles entre les deux hôtes hors pare-feu via le tunnel spécifié. Les règles par défaut, pour les protocoles UDP (User Datagram Protocol), AH (Authentication Header) et ESP (Encapsulating Security Paylooad), doivent déjà gérer la communication entre l'hôte et le pare-feu. Le pare-feu doit être configuré de manière appropriée pour compléter la configuration. Vous devez utiliser le fichier d'exportation à partir du tunnel que vous avez créé pour entrer les valeurs SPI et les clés nécessaires au pare-feu.

Hôte - Pare-feu - Hôte



Fonctions de journalisation

Cette section décrit la configuration et le format des journaux système relatifs à la sécurité IP. Dans les communications entre les hôtes, la journalisation des paquets échangés peut être lancée par le démon **syslogd**. D'autres messages importants concernant la sécurité IP y figurent également. Un administrateur peut contrôler ces informations de journalisation pour une analyse du trafic ou dans le cadre d'une opération de débogage. Pour configurer les fonctions de journalisation, procédez comme suit :

1. Editez le fichier **/etc/syslog.conf** et ajoutez l'entrée suivante :

   ```
   local4.debug  var/adm/ipsec.log
   ```

   Utilisez la fonction `local4` pour enregistrer les événements liés aux échanges et à la sécurité IP. Les niveaux de priorité standard d'AIX s'appliquent. Nous vous recommandons de définir le niveau de priorité pour le `débogage` jusqu'à ce que l'échange de données via les tunnels de sécurité IP et les filtres offrent une stabilité et un mouvement corrects.

   Remarque : La consignation des événements de filtre peut entraîner une activité importante au niveau de l'hôte de sécurité IP et nécessiter une capacité de stockage importante.

2. Enregistrez **/etc/syslog.conf**.
3. Sélectionnez le répertoire du fichier journal et créez un fichier vierge portant le même nom. Dans le cas ci-dessus, passez dans le répertoire `/var/adm` et lancez la commande suivante :

   ```
   touch ipsec.log
   ```

4. Lancez une commande d'**actualisation** via le sous-système **syslogd** :

   ```
   refresh –s syslogd
   ```

5. Lorsque vous créez des règles de filtre pour votre système hôte, si vous souhaitez consigner les paquets qui respectent une règle en particulier, attribuez au paramètre **–l** de la règle la valeur **Y** (oui) à l'aide des commandes **genfilt** ou **chfilt**.
6. Enfin, activez la journalisation des paquets et lancez le démon **ipsec_logd** à l'aide de la commande suivante :

```
mkfilt -g start
```

Pour arrêter la journalisation des paquets, lancez la commande suivante :

```
mkfilt -g stop
```

L'exemple de fichier journal ci–dessous contient des informations sur le trafic et la sécurité IP.

```
1. Aug 27 08:08:40 host1 : Filter logging daemon ipsec_logd (level
2.20) initialized at 08:08:40 on 08/27/97A

2. Aug 27 08:08:46 host1 : mkfilt: Status of packet logging set to
Start at 08:08:46 on 08/27/97

3. Aug 27 08:08:47 host1 : mktun: IBM tunnel 1, 9.3.97.244,
9.3.97.130 activated.

4. Aug 27 08:08:47 host1 skeyd: Inserted new context for tunnel ID
1 local SPI: 1336 remote SPI: 1336 .

5. Aug 27 08:08:47 host1 : mkfilt: #:1 permit 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 udp eq  4001 eq  4001  both both l=n f=y t=0 e= a=

6. Aug 27 08:08:47 host1 : mkfilt: #:2 permit 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 ah any 0 any 0  both both l=n f=y t=0 e= a=

7. Aug 27 08:08:47 host1 : mkfilt: #:3 permit 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 esp any 0 any 0  both both l=n f=y t=0 e= a=

8. Aug 27 08:08:47 host1 : mkfilt: #:4 permit 10.0.0.1
255.255.255.255 10.0.0.2 255.255.255.255 icmp any 0 any 0 local
outbound l=y f=y t=1 e= a=

9. Aug 27 08:08:47 host1 : mkfilt: #:4 permit 10.0.0.2
255.255.255.255 10.0.0.1 255.255.255.255 icmp any 0 any 0 local
inbound l=y f=y t=1 e= a=

10. Aug 27 08:08:47 host1 : mkfilt: #:6 permit 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 all any 0 any 0  both both l=y f=y t=0 e= a=

11. Aug 27 08:08:47 host1 : mkfilt: Filter support (level 1.00)
initialized at 08:08:47 on 08/27/97

12. Aug 27 08:08:48 host1 : #:6 R:p  o:10.0.0.1 s:10.0.0.1
d:10.0.0.20 p:udp sp:3327 dp:53 r:l a:n f:n T:0 e:n l:67

13. Aug 27 08:08:48 host1 : #:6 R:p  i:10.0.0.1 s:10.0.0.20
d:10.0.0.1 p:udp sp:53 dp:3327 r:l a:n f:n T:0 e:n l:133

14. Aug 27 08:08:48 host1 : #:6 R:p  i:10.0.0.1 s:10.0.0.15
d:10.0.0.1 p:tcp sp:4649 dp:23 r:l a:n f:n T:0 e:n l:43

15. Aug 27 08:08:48 host1 : #:6 R:p  o:10.0.0.1 s:10.0.0.1
d:10.0.0.15 p:tcp sp:23 dp:4649 r:l a:n f:n T:0 e:n l:41

16. Aug 27 08:08:48 host1 : #:6 R:p  i:10.0.0.1 s:10.0.0.15
d:10.0.0.1 p:tcp sp:4649 dp:23 r:l a:n f:n T:0 e:n l:40

17. Aug 27 08:08:51 host1 : #:4 R:p  o:10.0.0.1 s:10.0.0.1
d:10.0.0.2 p:icmp t:8 c:0 r:l a:n f:n T:1 e:n l:84

18. Aug 27 08:08:51 host1 : #:5 R:p  i:10.0.0.1 s:10.0.0.2
d:10.0.0.1 p:icmp t:0 c:0 r:l a:n f:n T:1 e:n l:84
```

```
19. Aug 27 08:08:52 host1 : #:4 R:p  o:10.0.0.1 s:10.0.0.1
d:10.0.0.2 p:icmp t:8 c:0 r:l a:n f:n T:1 e:n l:84

20. Aug 27 08:08:52 host1 : #:5 R:p  i:10.0.0.1 s:10.0.0.2
d:10.0.0.1 p:icmp t:0 c:0 r:l a:n f:n T:1 e:n l:84

21. Aug 27 08:32:27 host1 : Filter logging daemon terminating at
08:32:27 on 08/27/97l
```

Les paragraphes suivants traitent des entrées du journal :

1. Démon de journalisation des filtres activé.
2. Journalisation des paquets activée avec **mkfilt –g start**.
3. Activation du tunnel IBM, affichage de l'ID du tunnel, adresse source, adresse de destination et date/heure.
4. Le démon **skeyd** a inséré le contexte du tunnel, ce qui signifie que le tunnel IBM est prêt pour l'échange de données.

5–10. Les filtres sont activés. Le fichier journal affiche toutes les règles de filtre chargées.

11. Message affichant l'activation des filtres.

12–13. Ces entrées indiquent une recherche DNS d'un hôte.

14–16. Ces entrées indiquent une connexion Telnet partielle (pour des raisons de place, les autres entrées ne sont pas citées dans l'exemple).

17–20. Ces entrées indiquent des tests de ligne (ping).

21. Arrêt du démon de journalisation des filtres.

L'exemple ci–dessous illustre deux hôtes négociant un tunnel de phases 1 et 2, puis acheminant le trafic Telnet à travers le tunnel de phase 2 venant d'être créé.

```
1.  Aug 9 12:32:26 host 1  Tunnel Manager: 0: TM is processing a
Connection_request_msg

2.  Aug 9 12:32:26 host 1  Tunnel Manager: 1: Creating new P1
tunnel object (tid)

3.  Aug 9 12:32:26 host 1  Tunnel Manager: 0: Built a
P1_init_request_msg

4.  Aug 9 12:32:41 host 1  Tunnel Manager: 1: TM is processing a
P1_sa_created_msg (tid)


5.  Aug 9 12:32:41 host 1  Tunnel Manager: 1: Received good P1 SA,
updating P1 tunnel (tid)

6.  Aug 9 12:32:41 host 1  Tunnel Manager: 0: Checking to see if
any tunnels P2 tunnels need to start

7.  Aug 9 12:32:56 host 1  Tunnel Manager: 0: TM is processing a
Connection_request_msg

8.  Aug 9 12:32:57 host 1  Tunnel Manager: 0: Connection object
contains a P2 request

9.  Aug 9 12:32:57 host 1  Tunnel Manager: 0: Received a connection
object for an active P1 tunnel

10.  Aug 9 12:32:57 host 1  Tunnel Manager: 1: Created blank P2
tunnel (tid)
```

```
11.  Aug 9 12:32:57 host 1  Tunnel Manager: 0: Added reference of
new P2 to the P1 list

12.  Aug 9 12:32:57 host 1  Tunnel Manager: 0: Checking to see if
any P2 tunnels need to start

13.  Aug 9 12:32:57 host 1  Tunnel Manager: 1: Starting
negotiations for P2 (P2 tid)

14.  Aug 9 12:33:11 host 1  Tunnel Manager: 0: TM is processing a
P2_sa_created_msg

15.  Aug 9 12:33:11 host 1  Tunnel Manager: 1: received
P2_sa_created for an existing tunnel as initiator (tid)

16.  Aug 9 12:33:11 host 1  Tunnel Manager: 0: Writing filter rules

17.  Aug 9 12:35:54 host 1  Tunnel Manager: 0: TM is processing a
List_tunnels_msg

18.  Aug 9 13:01:31 host 1  mkfilt: Status of packet logging set to
Start at 13:01:31 on 08/09/98

19.  Aug 9 13:01:32 host 1  ipsec_logd: Filter logging daemon
ipsec_logd (level 2.20) initialized at 13:01:32 on 08/09/98

20.  Aug 9 13:01:32 host 1  ipsec_logd:  TC_LOG6: Tunnel interface
module for IPv6 was started at 12:31:39 on 08/09/98

21.  Aug 9 13:01:32 host 1  ipsec_logd:  TC_LOG4: Tunnel cache for
IPv4 was cleared at 12:31:39 on 08/09/98

22.  Aug 9 13:01:32 host 1  ipsec_logd:  TC_LOG4: Tunnel 1 with ESP
SPI 300 and AH SPI 0 for IPv4 was activated at 12:33:11 on 08/09/98

23.  Aug 9 13:03:14 host 1  mkfilt:  Filter rules updated at
13:03:14 on 08/09/98

24.  Aug 9 13:03:14 host 1  mkfilt:  #:1 permit
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 (0) udp 500 udp 500 both both l=y
f=n t=0

25.  Aug 9 13:03:14 host 1  mkfilt:  #:2 permit
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 all any 0 any 0 both both l=y f=n
t=0

26.  Aug 9 13:03:14 host 1  mkfilt:  Filter rules updated at
13:03:14 on 08/09/98

27.  Aug 9 13:03:14 host 1  mkfilt:  Filter support (level 1.00)
initialized at 13:03:14 on 08/09/98

28.  Aug 9 13:03:26 host 1  ipsec_logd:  #:7001 R:p O:10.10.10.1
S:10.10.10.1 D:10.10.10.4 P:tcp SP:32793 DP:23 R:r I:tr0 F:n T:1
L:41

29.  Aug 9 13:03:26 host 1  ipsec_logd:  #:7001 R:p I:10.10.10.1
S:10.10.10.4 D:10.10.10.1 P:tcp SP:23 DP:32793 R:r I:tr0 F:n T:1
L:41

30.  Aug 9 13:03:26 host 1  ipsec_logd:  #:7001 R:p O:10.10.10.1
S:10.10.10.1 D:10.10.10.4 P:tcp SP:32793 DP:23 R:r I:tr0 F:n T:1
L:40
```

```
31.  Aug 9 13:03:26 host 1  ipsec_logd:  #:7001 R:p O:10.10.10.1
S:10.10.10.1 D:10.10.10.4 P:tcp SP:32793 DP:23 R:r I:tr0 F:n T:1
L:41
```

Les paragraphes suivants traitent des entrées du journal.

1–4	La commande **ike cmd=activate phase=1** active une connexion.
5	Le gestionnaire de tunnel (Tunnel Manager) reçoit un lien de sécurité de phase 1 valide envoyé par le répondeur.
6	Ce gestionnaire vérifie si la commande **ike cmd=activate** dispose ou non d'une valeur de phase 2 pour poursuivre plus avant. Il n'en est rien.
7–13	La commande **ike cmd=activate phase=2** active un tunnel de phase 2.
14–15	Le gestionnaire de tunnel (Tunnel Manager) reçoit un lien de sécurité de phase 2 valide envoyé par le répondeur.
16	Ce gestionnaire écrit les règles de filtres dynamiques.
17	La commande **ike cmd=list** visualise les tunnels IKE.
18–19	La fonction de journalisation des paquets est activée.
20–22	Le tunnel de phase 2 est inséré dans le cache de tunnel.
23–27	Les règles de filtres sont actualisées.
28–31	Les paquets d'une session Telnet sont acheminées par le tunnel de phase 2.

Etiquettes des entrées de champs

Les champs des entrées du fichier journal sont abrégés afin de réduire l'espace DASD requis :

Numéro de la règle à l'origine de la consignation de ce paquet.

R Type de règle.

- **p** Autoriser.
- **d** Refuser.

i/o Direction du paquet lorsqu'il a été intercepté par le code de support du filtre. Identifie l'adresse IP de la connexion associée au paquet :

- Pour les paquets entrants (i), il s'agit de la connexion définie pour la réception du paquet.
- Pour les paquets sortants (o), il s'agit de la connexion que la couche IP à défini pour gérer la transmission du paquet.

s Indique l'adresse IP de l'expéditeur du paquet (issue de l'en-tête IP).

d Indique l'adresse IP du destinataire présumé du paquet (issue de l'en-tête IP).

p Indique le protocole de niveau supérieur utilisé pour créer le message dans la partie des données du paquet. Il peut s'agir d'un nombre ou d'un nom, par exemple : `udp` , `icmp` , `tcp` , `tcp/ack` , `ospf` , `pip` , `esp` , `ah` ou `all` .

sp/t Indique le numéro de port du protocole associé à l'expéditeur du paquet (issu de l'en-tête TCP/UDP). Avec un protocole ICMP ou OSPF, ce champ est remplacé par **t**, désignant le type IP.

dp/c Indique le numéro de port du protocole associé au destinataire présumé du paquet (issu de l'en-tête TCP/UDP). Avec le protocole ICMP, ce champ est remplacé par **c**, désignant le code IP.

– Indique l'absence d'informations disponibles

r Indique si le paquet possède un lien de filiation local.

- **f** Paquets réacheminés
- **l** Paquets locaux
- **o** Sortant
- **b** Les deux

l Indique la longueur (octets) d'un paquet donné.

f Identifie le paquet et indique s'il s'agit d'un fragment.

T Indique l'ID du tunnel.

i Indique l'interface de la réception du paquet.

Coexistence de la sécurité IP et de Secured Network Gateway 2.2/IBM Firewall 3.1/3.2 d'IBM

Si vous avez installé AIX 4.3 avec la fonction de sécurité IP, cette dernière sera désactivée avec IP version 6 si vous installez un produit IBM Firewall postérieurement. Le produit IBM Firewall remplace la fonction de sécurité IP par sa propre implémentation.

Pour plus d'informations, reportez-vous à la section Interfonctionnement, page 4-34.

Identification des incidents

Vous trouverez dans la présente section des conseils et astuces pour vous aider à résoudre les incidents qui se produisent. Il est recommandé de configurer la journalisation des incidents dès le début. Les journaux sont très utiles pour identifier les incidents liés aux filtres et aux tunnels. (Reportez–vous à la section Fonctions de journalisation, page 4-25 pour plus d'informations en la matière).

Erreur : L'exécution de la commande **mktun** génère le message d'erreur suivant :

```
insert_tun_man4(): write failed : The requested resource
is busy.
```

Incident : Le tunnel que vous souhaitez activer est déjà actif ou une collision des valeurs SPI s'est produite.

Solution : Lancez la commande **rmtun** pour désactiver le tunnel, puis exécutez la commande mktun pour le réactiver. Vérifiez si les valeurs SPI du tunnel défaillant correspondent à un autre tunnel actif. Chaque tunnel doit posséder ses propres valeurs SPI qui sont uniques.

Erreur : L'exécution de la commande **mktun** génère le message d'erreur suivant :

```
Device ipsec_v4 is in Defined status.

Tunnel activation for IP Version 4 not performed.
```

Incident : Vous n'avez pas rendu disponible la fonction de sécurité IP.

Solution : Lancez la commande suivante :

```
mkdev -l ipsec -t 4
```

Vous devez remplacer l'option **–t** par 6 si la même erreur se produit lors de l'activation du tunnel Version 6. Les unités doivent être disponibles. Pour vérifiez l'état de l'unité de sécurité IP, lancez la commande suivante :

```
lsdev -Cc ipsec
```

Erreur: L'exécution de la commande **chfilt** génère le message d'erreur suivant :

```
Cannot modify the first rule.
```

ou

```
Cannot modify a pre_defined filter rule.
```

Incident : Vous n'êtes pas autorisé à modifier ces règles de filtre. Vous pouvez cependant définir leur journalisation.

Solution : Pour consigner ces règles, il suffit de lancer la commande suivante :

```
chfilt -v (4 ou 6) -n (numéro de filtre) -l y
```

Pour configurer les règles par défaut destinées à transmettre les paquets AH (Authentication Header) ou ESP (Encapsulating Security Payload) uniquement à des hôtes donnés, vous devez désactiver la génération automatique des règles à l'aide du paramètre **–g** associé à la commande **gentun**. Vous pouvez ensuite ajouter les mêmes règles que les paquets AH et ESP, avec l'adresse IP de l'hôte spécifique comme source et l'adresse IP de l'hôte partenaire comme destination. Assurez-vous que ces règles sont placées avant les règles de trafic du tunnel proprement dit.

Erreur : L'exécution de la commande **gentun** génère le message d'erreur suivant :

```
Invalid Source IP address
```

Incident : Vous avez saisi une adresse IP incorrecte comme adresse source.

Solution : Pour les tunnels IP version 4, vérifiez si vous avez indiqué une adresse IP version 4 disponible pour la machine locale. Vous ne pouvez pas attribuer à l'adresse source un nom d'hôte lorsque vous générez des tunnels. En revanche, cette possibilité est offerte pour l'adresse de destination.

Pour les tunnels IP version 6, vérifiez si vous avez indiqué une adresse IP version 6 disponible. Si vous entrez `netstat -in` et qu'aucune adresse IP version 6 n'existe, exécutez /**usr**/**sbin**/**autoconf6** (interface) pour générer automatiquement une adresse locale (avec l'adresse MAC) ou utilisez **ifconfig** pour attribuer manuellement une adresse.

Erreur : L'exécution de la commande **mktun** génère le message d'erreur suivant :

```
insert_tun_man4(): write failed : A system
call received a parameter that is not valid.
```

Incident : La génération du tunnel s'est produite avec une combinaison ESP et AH incorrecte ou sans l'utilisation du nouveau format d'en-tête lorsque cela s'avère nécessaire.

Solution : Vérifiez la nature des algorithmes d'authentification en cours d'utilisation par le tunnel en question. N'oubliez pas que les algorithmes HMAC_MD5 et HMAC_SHA requièrent le nouveau format d'en-tête. Le nouveau format d'en-tête peut être modifié à l'aide du raccourci SMIT **ips4_basic** ou du paramètre **–z** associé à la commande **chtun**. Rappelez-vous également que DES_CBC_4 ne peut pas être utilisé avec le nouveau format d'en-tête.

Débogage des erreurs au niveau du tunnel IKE

Organigramme du tunnel IKE

Les tunnels IKE sont configurés via la commande **ike** ou les écrans VPN du Web-based System Manager avec deux démons :

tmd Démon du gestionnaire de tunnel (Tunnel Manager)

isakmpd Démon ISAKMP

Pour que les tunnels IKE soient correctement configurés, ces deux démons doivent être exécutés. Si la fonction de sécurité IP est lancée lors du redémarrage, l'exécution de ces démons se fait automatiquement. Dans le cas contraire, ils doivent être lancés manuellement.

Le gestionnaire de tunnel demande à **isakmpd** de lancer un tunnel. Si le tunnel existe déjà ou n'est pas valable (en cas d'adresse distante erronée, par exemple), un message d'erreur apparaît. Une fois la négociation lancée, son exécution peut prendre un certain temps, en fonction de la durée d'attente sur le réseau. La commande **ike cmd=list** peut indiquer l'état du tunnel afin de savoir la négociation s'est bien déroulée. Le gestionnaire de tunnel consigne également des événements dans le journal système **syslog** au niveau des sections **debug**, **event** et **information**, utilisées pour surveiller l'état d'avancement de la négociation.

Procédez comme suit :

1.. Utilisez le Web-based System Manager ou la commande **ike** pour lancer un tunnel.

2.. Le démon **tmd** envoie au démon **isakmpd** une demande de connexion pour la gestion de clés (phase 1).

3.. Le démon **isakmpd** répond par le message `SA created` ou par l'affichage d'un message d'erreur.

4.. Le démon **tmd** envoie au démon **isakmpd** une demande de connexion pour un tunnel de gestion des données (phase 2).

5.. Le démon **isakmpd** répond par le message `SA created` ou par l'affichage d'un message d'erreur.

6.. Les paramètres de tunnel sont insérés dans le cache de tunnel du noyau.

7.. Les règles de filtres sont ajoutées à la table de filtres dynamique du noyau.

Lorsque la machine agit comme un répondeur, le démon **isakmpd** informe le démon **tmd** du gestionnaire de tunnel du bon déroulement de la négocation. Un nouveau tunnel est inséré dans le noyau. Dans ces cas–là, le processus commence à l'étape 3 et se poursuit jusqu'à l'étape 7, sans demande de connexion de la part du démon **tmd**.

Fonction de journalisation du démon isakmpd

Le démon **isakmpd** consigne les événements dans un journal séparé en raison de leur nombre et de leur taille. La fonction de journalisation est activée par la commande **ike cmd=log**. Le fichier de configuration **/etc/isakmpd.conf** peut être défini pour qu'il soit fait mention des fichiers de sortie à chaque niveau de journalisation. La définition des niveaux peut être **none**, **errors**, **events** et **information**.

Le code du démon **isakmpd** s'active ou répond en envoyant ou en évaluant une proposition. Si cette proposition est acceptée, un lien de sécurité est généré et le tunnel est configuré. Si cette proposition est refusée ou si le délai de connexion expire avant la fin de la négociation, le démon renvoie un message d'erreur. Les entrées du journal système **syslog** à partir de **tmd** indiquent la réussite ou non de la négociation. Consultez le journal **isakmpd** pour connaître la cause exacte d'un échec de négociation.

Fonctions de suivi

Il s'agit d'outils de débogage utilisés pour le suivi des événements du noyau. La fonction de suivi peut être utilisée pour obtenir de plus amples informations sur les erreurs ou les événements qui se sont produits dans le filtre du noyau et le code du tunnel.

SMIT possède une fonction de suivi pour la sécurité IP disponible via le menu Configuration avancée de la sécurité IP. Parmi les informations qui entrent dans le champ d'application de cette fonction de suivi figurent les informations sur les erreurs, les filtres, les tunnels, l'encapsulation/décapsulation et le chiffrement. Par définition, le suivi d'erreurs fournit les informations les plus importantes. L'utilitaire de suivi d'informations peut générer un volume d'informations important et nuire aux performances du système. Cette opération de suivi vous fournit des indices permettant d'identifier l'incident. Le suivi d'informations est également nécessaire si vous vous adressez à un technicien IBM chargé de la sécurité IP. Pour accéder à la fonction de suivi, utilisez le raccourci SMIT **smit ips4_tracing** (pour IP version 4) ou **smit ips6_tracing** (pour IP version 6).

ipsecstat

Vous pouvez lancer la commande **ipsecstat** pour générer l'exemple de rapport suivant. Ce rapport indique que les unités de sécurité IP sont disponibles, que trois algorithmes d'authentification et trois algorithmes de chiffrement sont installés, et qu'il existe un rapport sur l'activité des paquets. Ces informations peuvent servir à identifier l'origine d'un incident si vous cherchez à résoudre les incidents liés au trafic de sécurité IP.

```
IP Security Devices:
ipsec_v4 Available
ipsec_v6 Available

Authentication Algorithm:
HMAC_MD5 -- Hashed MAC MD5 Authentication Module
HMAC_SHA -- Hashed MAC SHA Hash Authentication Module
KEYED_MD5 -- Keyed MD5 Hash Authentication Module

Encryption Algorithm:
CDMF -- CDMF Encryption Module
DES_CBC_4 -- DES CBC 4 Encryption Module
DES_CBC_8 -- DES CBC 8 Encryption Module
3DES_CBC -- Triple DES CBC Encryption Module

IP Security Statistics -
Total incoming packets:  1106
Incoming AH packets:326
Incoming ESP packets:  326
Srcrte packets allowed:  0
Total outgoing packets:844
Outgoing AH packets:527
Incoming ESP packets:  527
Total incoming packets dropped:  12
  Filter denies on input:  12
  AH did not compute: 0
  ESP did not compute:0
  AH replay violation:0
  ESP replay violation:  0
Total outgoing packets dropped:0
  Filter denies on input:0
Tunnel cache entries added: 7
Tunnel cache entries expired:  0
Tunnel cache entries deleted:  6
```

Interfonctionnement

Les sections qui suivent décrivent des solutions d'interfonctionnement. Pour plus d'informations, reportez-vous à la section Coexistence entre la fonction Sécurité IP et IBM Secured Network Gateway 2.2/IBM Firewall 3.1 ou 3.2, page 4-30.

IBM Firewall 3.1/3.2, IBM Secured Network Gateway (SNG) 2.2

Les produits IBM Firewall 3.1, 3.2 et IBM SNG 2.2 fonctionnent comme coexploitant du tunnel avec la fonction de sécurité IP d'AIX 4.3. Le tunnel peut être créé sur le pare–feu et exporté, puis importé sur un hôte AIX 4.3 exécutant la fonction de sécurité IP via l'option **–n** associée à la commande **imptun**. Cependant, un script appelé **ipsec_convert** est envoyé comme exemple de script shell permettant de convertir un fichier d'exportation de tunnel de sécurité IP en fichiers nécessaires par IBM Firewall 3.1/3.2 ou IBM SNG 2.2 pour l'importation.

Un certain nombre d'éléments sont en prendre en considération lors de l'exportation d'un tunnel dont le coexploitant est IBM Firewall 3.1, 3.2 ou IBM SNG 2.2. Ce sont les suivants :

- IBM Firewall 3.1/3.2 et IBM SNG 2.2 utilisent uniquement l'algorithme KEYED_MD5 avec AH, et ne pourront pas importer un tunnel de type HMAC_MD5 ou HMAC_SHA1 avec AH.
- IBM Firewall 3.1/3.2 et IBM SNG 2.2 ne prennent pas en charge la fonction de protection contre les répétitions.
- IBM Firewall 3.1/3.2 et IBM SNG 2.2 n'acceptent pas la valeur 0 (zéro) comme durée de vie correspondant à une durée infinie.

- De plus, la fonction de sécurité IP crée des tunnels avec ses propres numéros d'ordre pour les ID des tunnels ; lors de l'importation vers le pare-feu, assurez-vous que ces numéros ne sont pas déjà utilisés.
- IBM Firewall 3.1/3.2 et IBM SNG 2.2 ne prennent pas en charge les tunnels IP version 6.
- Assurez-vous que la mise à jour de SNG 2.2 s'est effectuée avec le niveau de service correct.

Sécurité IP du logiciel FTP

La pile TCP/IP et la fonction de sécurité IP du logiciel FTP fonctionnent comme coexploitant du tunnel avec la fonction de sécurité IP d'AIX 4.3. Suivez les instructions du logiciel FTP pour ajouter la fonction Sécurité IP. A partir de la table de configuration de sécurité IP du logiciel FTP, vous pouvez ajouter un adresse destinée à définir une communication sécurisée. Ensuite, une page s'affiche avec les champs de saisie de configuration Sécurité IP. Vous avez généré la valeur SPI AH source et la clé confidentielle partagée (pour AH), mais vous devez indiquer la valeur SPI AH de destination et la clé confidentielle partagée dans les champs appropriés. La page contient également une valeur SPI ESP et une clé ESP source générées automatiquement. Lorsque vous sélectionnez l'option correspondant au chiffrement, la valeur SPI ESP source et la clé ESP source s'affichent.

Pour assurer une compatibilité, suivez les étapes suivantes :

- Sur le système hôte AIX 4.3, ajoutez un tunnel à l'aide des paramètres de sécurité IP du logiciel FTP pour la valeur et la clé SPI AH cible et la valeur et la clé SPI ESP.
- Notez que la page de configuration de sécurité IP du logiciel FTP n'accepte que des nombres hexadécimaux pour les champs de saisie. Vous devez convertir les valeurs SPI AH et ESP générées par le logiciel FTP en valeurs décimales avant de les attribuer à la fonction de sécurité IP d'AIX 4.3.
- Lorsque vous entrez les valeurs SPI et les clés dans la page de configuration de sécurité IP du logiciel FTP, n'indiquez pas **0x**. Le logiciel FTP ne reprendra pas les zéros à gauche.
- Notez que la règle à suivre doit être uniquement authentification après chiffrement (encr/auth), authentification seulement (auth) ou chiffrement seulement (encr).
- Seuls les algorithmes de chiffrement DES_CBC_4 et DES_CBC_8 peuvent être utilisés.
- Seul l'algorithme Keyed_MD5 doit être utilisé pour l'authentification.
- Entrez les valeurs avec précaution. En effet une saisie incorrecte peut remettre en cause le bon fonctionnement du tunnel.
- Lorsque vous ajoutez un nouveau tunnel ou lorsque vous modifiez un tunnel, vous devez relancer Windows 95 sur le système disposant de la fonction de sécurité IP du logiciel FTP.

Informations de référence sur la fonction de sécurité IP

Liste des commandes

gentun	Crée une définition de tunnel
mktun	Active une ou plusieurs définitions de tunnel
chtun	Change la définition d'un tunnel
rmtun	Supprime la définition d'un tunnel
lstun	Répertorie une ou plusieurs définitions de tunnel
exptun	Exporte une ou plusieurs définitions de tunnel
imptun	Importe une ou plusieurs définitions de tunnel
genfilt	Crée une définition de filtre
mkfilt	Active une ou plusieurs définitions de filtre
mvfilt	Déplace une règle de filtre
chfilt	Change une définition de filtre
rmfilt	Supprime la définition d'un filtre
lsfilt	Répertorie une ou plusieurs définitions de filtre
expfilt	Exporte une ou plusieurs définitions de filtre
impfilt	Importe une ou plusieurs définitions de filtre
ipsec_convert	Indique l'état de la sécurité IP
ipsecstat	Indique l'état de la sécurité IP
ipsectrcbuf	Indique le contenu du tampon de suivi de la sécurité IP
unloadipsec	Décharge un module de chiffrement

Liste des méthodes

defipsec	Définit une instance de sécurité IP pour IP version 4 ou IP version 6
cfgipsec	Configure et charge **ipsec_v4** ou **ipsec_v6**
ucfgipsec	Annule la configuration de **ipsec_v4** ou **ipsec_v6**

Chapitre 5. Unités TTY et communications série

Ce chapitre est consacré à la gestion des unités de terminal TTY. Il traite des points suivants :

Généralités TTY

Une unité de terminal tty est une unité en mode caractère qui effectue des entrées-sorties caractère par caractère. La communication entre ces unités et les programmes qui y accèdent en lecture ou en écriture est contrôlée par l'interface tty. On trouve parmi les unités tty :

- Modems
- Terminaux ASCII
- Console Système (LFT)
- **aixterm** sous AIXwindows.

Il est possible d'ajouter, de supprimer, d'afficher ou de modifier des unités tty comme n'importe quelle autre unité du système, à l'aide de l'application Web-based System Manager Devices, via SMIT ou des commandes propres aux unités.

Variable TERM pour différents écrans et terminaux

Les informations relatives aux fonctions des terminaux sont stockées dans la base de données **terminfo**. Chaque terminal est décrit par la variable d'environnement **TERM** dans la base de données **terminfo**. Les programmes y trouvent toutes les données nécessaires à l'établissement de la communication avec une unité tty courante.

Valeurs TERM pour divers terminaux	
Ecran/Terminal	**Valeur**
Terminal ASCII 3161	ibm3161
Terminal ASCII 3163	ibm3161
DEC VT100 (terminal)	vt100
DECVT220	vt220
Station écran ASCII 3151 ou 3161 avec cartouche	ibm3161-C
Station écran ASCII 3162	ibm3161
Station écran ASCII 3162 avec cartouche	ibm3162
Ecran 6091	lft
AIXwindows	aixterm

Pour des informations sur les entrées de la base de données **terminfo**, reportez-vous au format de fichier **terminfo**. Pour convertir les entrées **termcap** en entrées **terminfo**, reportez-vous à la commande **captoinfo**. (Le fichier **termcap** contient la description des terminaux des anciens systèmes Berkeley.)

Définition des caractéristiques de terminal TTY

Le *protocole de liaison* fournit une interface utilisateur indépendante du matériel entre l'ordinateur et une unité asynchrone. Ainsi, un utilisateur peut supprimer une simple ligne ou interrompre un processus en cours en entrant une séquence de caractères. Vous avez la possibilité de définir vous même ces séquences, ainsi que les caractéristiques des terminaux (vitesse de communication, par exemple), à l'aide de l'application Web-based System ManagerchdevDevices, via l'outil SMIT ou la commande **stty**.

La plupart des applications (shells et éditeurs compris) sont conçues pour communiquer avec des terminaux appliquant le protocole de liaison POSIX (par défaut). Pour basculer sur le protocole de liaison Berkeley, vous disposez de la commande **stty**.

Définition des attributs de l’unité TTY raccordée

L’établissement d’une communication entre l’hôte et l’unité tty raccordée exige :

- un câble de communication,
- des attributs de communication (vitesse de liaison, longueur de mot, parité, bit d’arrêt et interface) identiques sur l’hôte et l’unité tty raccordée.

Gestion des unités TTY

Pour effectuer une tâche décrite dans le tableau suivant, une unité tty doit être installée.

Gestion des tâches liées aux unités TTY		
raccourci Web-based System Manager: **unités wsm** (application Devices) OU		
Restrictions d'accès FTP	*Raccourci SMIT*	*Commande ou fichier*
Liste des unités TTY définies	**smit lsdtty**	**lsdev –C –c tty –H**
Ajout d'un terminal TTY	**smit mktty**	**mkdev –t tty**[1,2]
Associer un terminal TTY à un autre port[3]	**smit movtty**	**chdev –l** *Nom* **–p** *Nom Parent* **–w** *Emplacement Connexion*[2,4]
Modifier/afficher les caractéristiques d'un terminal TTY	**smit chtty**	**lsattr –l** *Nom* **–E** (afficher); **chdev –l** *Nom* (modifier)[4]
Suppression d'un terminal TTY[3]	**smit rmtty**	**rmdev –l** *Nom*
Configuration d'un terminal TTY défini (rendre disponible)	**smit mktty**	**mkdev –l** *Nom*

Remarques :

1. D'autres indicateurs peuvent être utilisés pour définir plus précisément la nouvelle unité tty. Dans l'exemple ci dessous, il s'agit de définir et de configurer l'unité tty RS–232 connectée au port `0` sur la carte asynchrone 8 ports `sa3` avec un débit de `19200` (attribut `speed`), la valeur des autres attributs étant extraite du fichier `foo` :

   ```
   mkdev -t tty -s rs232 -p sa3 -w 0 -a speed=19200 -f foo
   ```

2. Les commandes **mkdev** et **chdev** prennent en charge les options incompatibles avec Web-based System Manager ou SMIT.
3. Désactivez l'unité tty avant d'effectuer cette tâche. Reportez-vous à la commande **pdisable**.
4. Utilisez des indicateurs pour modifier les caractéristiques spécifiques d'une unité tty à partir de la ligne de commande.

Si vous ajoutez ou modifiez une unité tty à partir de la ligne de commande, reportez-vous à la liste ci-dessous pour rechercher le nom *d'attribut* que vous devez spécifier avec l'indicateur **–a** *Attribute***=***valeur* pour la caractéristique à définir. Par exemple, spécifiez `a speed=`*`valeur`* pour définir le débit en bauds de l'unité tty.

Caractéristique	**Attribut**
Activation de la CONNEXION	login
Vitesse de transmission (BAUDS)	speed
PARITE	parity
BITS par caractère	bpc
Nombre de BITS D'ARRET	stops
DELAI avant passage à déf. de port suivante	timeout
Etablissement de liaison XON-XOFF	xon
Type de TERMINAL	term
CONTROLE DE FLUX à utiliser	flow_disp

PROTOCOLE OUVERT à utiliser	open_disp
Attributs STTY pour le temps d'EXECUTION	runmodes
Attributs STTY pour la CONNEXION	logmodes
EXECUTION gestionnaire activité du shell	shell
Nom de CONNEXION	logger
ETAT de l'unité au moment de l'AMORCAGE	autoconfig
Nombre de mémoires tampons D'EMISSION	tbc
Niveau de déclenchement de la RECEPTION	rtrig
Modules STREAMS à ajouter à l'ouverture	modules
Fichier mappe d'ENTREE	imap
Fichier mappe de SORTIE	omap
Fichier mappe de JEU DE CODES	csmap
Caractère INTERRUPT	intr
Caractère QUIT	quit
Caractère ERASE	erase
Caractère KILL	kill
Caractère END OF FILE	eof
Caractère END OF LINE	eol
Deuxième caractère EOL	eol2
Caractère DELAY SUSPEND PROCESS	dsusp
Caractère SUSPEND PROCESS	susp
Caractère LITERAL NEXT	lnext
Caractère START	start
Caractère STOP	stop
Caractère WORD ERASE	werase
Caractère REPRINT LINE	reprint
Caractère DISCARD	discard

Utilitaire d'écran dynamique

L'utilitaire d'écran dynamique, ou commande **dscreen**, permet de connecter un terminal physique à plusieurs sessions de terminal virtuel (écrans) simultanément. Il a été conçu principalement pour les terminaux à pages de mémoire écran multiples (écrans IBM 3151 modèle 310 ou 410 avec cartouche d'extension, par exemple). En effet, sur ce type de terminal, passer d'un écran virtuel à l'autre revient à changer de page écran de terminal physique, ce qui permet de sauvegarder et de restaurer chaque image d'écran virtuel. La commande **dscreen** peut également être appliquée à des terminaux sans pages de mémoire écran multiples pour passer d'une session écran virtuel à l'autre, mais dans ce cas, l'apparence de l'écran sera modifiée.

Remarque : Pour une prise en charge complète de **dscreen**, le terminal doit pouvoir sur commande passer d'une page écran interne à l'autre et mémoriser la position du curseur sur chaque page. **dscreen** peut être exploité sur des terminaux intelligents ou non, mais les images écran ne sont pas sauvegardées lors des changements d'écran sur les terminaux non intelligents.

Fichier de configuration de terminal dsinfo

Le fichier dsinfo, fichier de configuration de terminal pour **dscreen**, sert à définir différents jeux de touches à utiliser avec cette commande, notamment lorsque les touches initialement définies ne sont pas compatibles avec une application exploitée sur le système.

Le type de terminal défini dans le fichier dsinfo admet par défaut une seule page de mémoire écran. Si le terminal utilisé en accepte davantage, ce fichier doit être modifié pour intégrer la séquence nécessaire au contrôle de la mémoire de page. Reportez-vous au manuel de référence du terminal pour connaître la séquence de contrôle spécifique.

Le fichier dsinfo par défaut est **/usr/lbin/tty/dsinfo**. Utilisez l'indicateur **–i** pour en spécifier un autre. Les informations développées dans cette section se rapportent au fichier par défaut mais elles sont valables pour n'importe quel autre fichier dsinfo créé.

Pour plus d'informations, reportez-vous à la section "Affectation d'écran dynamique" page 5-8.

Affectation de touches

L'exécution de **dscreen** ouvre un écran virtuel. Certaines touches du clavier ne sont pas transmises à cet écran : **dscreen** les intercepte et exécute, à leur activation, les actions suivantes : Les opérations sont les suivantes :

sélection	Sélectionne un écran
Block	Bloque toute entrée et sortie.
New	Ouvre une nouvelle session écran.
End	Arrête **dscreen**.
Quit	Quitte **dscreen**.
Previous	Revient à l'écran précédent.
List	Affiche les touches affectées à **dscreen** et leur fonction respective.

La fonction de chaque touche dépend du terminal et de sa définition dans le fichier **/usr/lbin/tty/dsinfo**.

Touche de sélection (Select)

A chaque écran virtuel créé est affectée une touche de sélection. Lorsqu'elle est activée, elle :

- assure le basculement du terminal physique à la page vidéo associée à l'écran virtuel,
- réachemine les entrées-sorties entre le terminal physique et l'écran virtuel.

Une fois que toutes les touches de sélection définies dans le fichier **dsinfo** ont été associées à un écran virtuel, il n'est plus possible de créer d'écran. Les sessions écran individuelles sont fermées lorsque le processus shell initial s'arrête. La touche associée est alors libérée, à disposition d'un autre écran virtuel. **dscreen** s'arrête à la fermeture du dernier écran actif.

Touche de blocage (Block)

Les touches de blocage servent à arrêter les sorties (comme le fait la séquence de touche Ctrl–S en contrôle de flux IXON), permettant ainsi d'établir de façon transparente des sessions de terminal sur deux ordinateurs utilisant un terminal à deux ports série.

Touche de création d'écran (New)

Appuyer sur une touche de création d'écran définit un nouvel écran logique et lui affecte une touche de sélection. Chaque écran créé requiert :

- une des touches de sélection définies dans le fichier dsinfo,
- une pseudo unité de terminal **dscreen**,
- suffisamment de mémoire pour les diverses structures de suivi d'écran,
- un processus pour l'exécution du shell.

A défaut d'un de ces éléments, l'écran ne peut être créé. Un message s'affiche.

Touches d'arrêt et de sortie (End et Quit)

Un touche d'arrêt (end) provoque :

- la diffusion d'un signal **SIGHUP** à toutes les sessions écran,
- l'élimination des erreurs,
- la sortie à l'état 0.

Une touche de sortie (quit) entraîne les mêmes opérations, avec l'état de sortie 1.

Touche d'écran précédent (Previous)

Une touche d'écran précédent (Previous) bascule sur l'écran précédemment affiché.

Remarque :

1. Restez sur le même écran tant qu'une écriture est en cours. En effet, si une séquence d'échappement est tronquée, le terminal est placé dans un état inconnu.
2. Certains écrans de terminal peuvent mémoriser la position du curseur sur un écran sans enregistrer les modes (insertion, vidéo inverse, etc.). Dans ce cas, évitez d'utiliser ces modes en passant d'un écran à l'autre.

Touche de listage (List)

La touche de listage (List) affiche la liste des touches (reconnues par **dscreen**, avec leur fonction, sur l'écran du terminal. Lorsqu'un écran est créé via **dscreen**, le message `Press KEY for help` s'affiche (*KEY* est le nom de la touche de listage affichée sur le terminal). Ce message n'est émis *que* si une touche de listage a été définie.

Affectation d'écran dynamique

Dans le fichier **/usr/lbin/tty/dsinfo**, l'entrée de description du terminal comporte autant de touches de sélection d'écran que de pages écran physiques définies pour le terminal. Si le nombre de touches de sélection dépasse celui des pages écran physiques, **dscreen** affecte dynamiquement des pages écran physiques aux écrans virtuels.

Si un écran virtuel dépourvu de page de mémoire écran est sélectionné, **dscreen** lui affecte l'écran physique le moins récemment utilisé. Selon les spécifications mises à jour dans le fichier **/usr/lbin/tty/dsinfo**, il peut être indiqué que l'écran physique est connecté à un écran virtuel différent, par exemple, l'écran est effacé.

Description du fichier dsinfo

Le fichier **dsinfo** est une base de données de descriptions de terminal à l'usage de l'utilitaire d'écrans multiples **dscreen**. Ce fichier rassemble les informations suivantes :

- les touches **dscreen** avec leur fonction,
- le nombre de pages mémoire écran du terminal,
- les séquences de codes envoyées ou reçues pour l'utilisation des fonctions ci-dessus.

Dans le fichier **dsinfo** par défaut, les entrées sur le type de terminal se présentent sous la forme de données de terminal 3151 ASCII du type :

```
# The Cartridge for Expansion (pn: 64F9314) needed for this entry
ibm3151|3151|IBM 3151,
dsks=\E!a^M|Shift-F1|,            # Selects first screen
dsks=\E!b^M|Shift-F2|,            # Selects second screen
dsks=\E!c^M|Shift-F3|,            # Selects third screen
dsks=\E!d^M|Shift-F4|,            # Selects fourth screen
dskc=\E!e^M|Shift-F5|,            # Creates a new screen
dske=\E!f^M|Shift-F6|\E pA\EH\EJ, # Go to screen 1 and end
dskl=\E!g^M|Shift-F7|,            # Lists function keys (help)
dskp=\E!h^M|Shift-F8|,            # Go to previous screen
dskq=\E!i^M|Shift-F9|\E pA\EH\EJ, # Go to screen 1 and quit
dsp=\E pA|\EH\EJ,                 # Terminal sequence for screen 1
dsp=\E pB|\EH\EJ,                 # Terminal sequence for screen 2
dsp=\E pC|\EH\EJ,                 # Terminal sequence for screen 3
dsp=\E pD|\EH\EJ,                 # Terminal sequence for screen 4
dst=10,                           # Allow 1 second timeout buffer
```

Format d'entrée

Les entrées du fichier **dsinfo** sont des champs séparés par une virgule. Le premier champ est constitué de la liste des noms possibles du terminal, séparés par une barre verticale (|). Tout texte précédé d'un astérisque (#) est un commentaire, ignoré par **dscreen**. Les autres champs sont des chaînes décrivant les fonctions du terminal à l'utilitaire **dscreen**. Les séquences d'échappement reconnues dans ces chaînes sont les suivantes :

Séquence Escape	Description
\E,\e	Echappement
\n,\l	Ligne suivante
\r	Retour chariot
\t	Tabulation
\b	Retour arrière
\f	Page suivante
\s	Espace
nnn	Valeur octale *nnn*
^*x*	Ctrl–*x* pour toute valeur *x* appropriée

Tout autre caractère précédé d'une barre oblique inverse (\ ) génère le caractère lui-même. Les chaînes sont entrées sous la forme *type=chaîne*, *type* étant le type de chaîne et *chaîne*, sa valeur.

Dans le fichier **dsinfo**, veillez à séparer les champs par une virgule. Si la virgule est omise ou tronquée en fin d'entrée, le fichier est inexploitable par l'utilitaire **dscreen** et une erreur est envoyée à l'écran.

Types de chaîne

Voici les différents types de chaîne :

dskx Les chaînes de 4 lettres commençant par dsk décrivent une touche. La dernière lettre (*x*) indique la fonction assignée à la touche :

Type	Fonction
dsks	Bascule d'un écran à l'autre
dskb	Bloque les entrées-sorties
dske	Met fin à **dscreen**
dskq	Quitte **dscreen** (Etat en sortie=1)
dskc	Crée un écran
dskp	Revient à l'écran précédent
dskl	Affiche les touches et leur fonction

Une chaîne de 4 lettres commençant par dsk*x* et suffixée par une autre lettre que s, b, e, q, c, p ou l ne génère aucune action **dscreen** interne, mais est répertoriée, reconnue et exécutée. La chaîne dskn (aucune opération) doit être utilisée lorsqu'aucune action **dscreen** n'est souhaitée.

La chaîne des valeurs de chaque touche se compose de trois sous-chaînes séparées par une barre verticale (|).

Remarque : Utilisez \| pour inclure le caractère | dans l'une des sous-chaînes.

La première sous-chaîne représente la séquence de caractères envoyée par le terminal lors de l'activation de la touche. La deuxième sous-chaîne fournit le libellé de la touche lors de l'affichage de la liste des touches. La troisième sous-chaîne est la séquence de caractères envoyée par **dscreen** au terminal lors de l'activation de la touche avant l'exécution de l'action demandée par cette dernière.

dsp Chaîne décrivant un écran physique sur le terminal. Une chaîne dsp doit être spécifiée pour chaque écran physique du terminal. Cette chaîne se compose de deux sous-chaînes séparées par une barre verticale (|).

La première sous-chaîne est la séquence de caractères à envoyer au terminal pour l'affichage et la sortie sur la page physique du terminal.

La seconde sous-chaîne est envoyée au terminal lorsque la page est utilisée pour un nouvel élément. Elle correspond généralement à la séquence de vidage d'écran et est envoyée dans deux cas :

1. lors de la création d'une session de terminal virtuel,
2. lorsque le nombre de terminaux virtuels est supérieur au nombre d'écrans physiques. Si un terminal virtuel requiert de **dscreen** plusieurs utilisations d'un même écran physique, il envoie cette séquence à l'écran pour lui indiquer que son contenu ne concorde pas avec la sortie du terminal virtuel connecté.

   Remarque : Pour éviter toute confusion, il est déconseillé de travailler avec plus de terminaux virtuels que d'écrans physiques : ne définissez pas plus de touches de sélection d'écran (dsks=) que d'écrans physiques (dsp=) dans l'entrée dsinfo.

dst A Chaîne de type dst qui définit le délai d'attente (en dixièmes de secondes) en entrée de **dscreen**. La valeur de la chaîne est un nombre décimal (maximum 255 ; par défaut : **1** [ou 0,1 seconde]).

Lorsque **dscreen** reconnaît un préfixe de séquence de touches d'entrée mais qu'il ne dispose pas de tous les caractères de la séquence, il attend les caractères manquants pour l'identifier. Passé le délai imparti, les caractères sont envoyés à l'écran virtuel et ne sont pas interprétés par **dscreen** comme partie intégrante d'une séquence de touches d'entrée.

Il peut être nécessaire d'augmenter le délai si une ou plusieurs des touches **dscreen** correspondent en fait à une série de touches (par exemple Ctrl–Z 1, Ctrl–Z 2, Ctrl–Z 3 ... pour la sélection d'écran, Ctrl–Z N pour un nouvel écran, etc.).

Exemple 1

L'entrée **/usr/lbin/tty/dsinfo** se rapporte à un Wyse–60 avec trois sessions d'écran :

```
wy60|wyse60|wyse model 60,
dsks=^A‘^M|Shift-F1|,
dsks=^Aa^M|Shift-F2|,
dsks=^Ab^M|Shift-F3|,
dskc=\200|Ctrl-F1|,
dske=\201|Ctrl-F2|\Ew0\E+,
dskl=\202|Ctrl-F3|,
dsp=\Ew0|\E+,
dsp=\Ew1|\E+,
dsp=\Ew2|\E+,
```

Cette entrée attribue :

- les séquences Maj–F1 à Maj–F3 à la sélection des écrans 1 à 3,
- la séquence Ctrl–F1 à la création d'un écran,
- la séquence Ctrl–F2 à l'envoi, vers l'écran, de`Esc w 0 Esc +` (passage à la fenêtre 0 et vidage de l'écran) et à l'arrêt de **dscreen**,
- la séquence Ctrl–F3 à l'affichage des touches et de leur fonction.

Chaque fois qu'un écran physique est utilisé pour un nouvel écran, la séquence `Esc +` est envoyée au terminal, ce qui vide l'écran.

Exemple 2

Cet exemple concerne un Wyse–60 avec trois sessions d'écran, un des écrans se trouvant sur un second ordinateur communiquant via le second port série du terminal :

```
wy60-1|wyse60-1|wyse model 60 - first serial port
dsks=^A‘^M|Shift-F1|,
dsks=^Aa^M|Shift-F2|,
dsks=^Ab^M|Shift-F3|\Ed#^Ab\r^T\Ee9,
dskc=\200|Ctrl-F1|,
dske=\201|Ctrl-F2|\Ed#\201^T\Ew0\E+,
dskl=\202|Ctrl-F3|,
dsp=\Ew0|\E+,dsp=\Ew1|\E+,
wy60-2|wyse60-2|wyse model 60 - second serial port
dsks=^A‘^M|Shift-F1|\Ed#^A‘\r^T\Ee8,
dsks=^Aa^M|Shift-F2|\Ed#^Aa\r^T\Ee8,
dsks=^Ab^M|Shift-F3|,
dskc=\200|Ctrl-F1|,
dske=\201|Ctrl-F2|\Ed#\201^T\Ew0\E+,
dskl=\202|Ctrl-F3|,
dsp=\Ew2|\E+,
```

dscreen doit être exécuté (avec l'option **t**) sur les deux ordinateurs, le premier équipé d'un terminal wy60–1 et le second d'un terminal wy60–2. L'entrée wy60–1 est examinée en premier.

Les deux premières entrées de touches ne sont pas modifiées par rapport à l'entrée wy60-2 initiale. La troisième, de type dskb, demande le blocage des entrées et des sorties. Lorsque cette touche est activée, la séquence :

```
Esc d # Ctrl-A b CR Ctrl-T Esc e 9
```

est envoyée au terminal. Dès lors, la sortie est bloquée et **dscreen** poursuit l'analyse des entrées de séquences de touches mais ignore les autres entrées.

La séquence `Esc d #` place le terminal en mode d'impression transparente (mode TPM) qui renvoie, jusqu'à réception d'un Ctrl–T, tous les caractères vers l'autre port série.

Les caractères `Ctrl-A b CR` sont envoyés vers l'autre port série, indiquant au process **dscreen** de l'autre ordinateur qu'il doit activer la fenêtre associée à la séquence Maj–F3.

La séquence Ctrl–T sort du mode TPM. Esc e 9 fait basculer le terminal sur l'autre port série AUX pour la communication des données.

Dès lors, l'autre ordinateur prend le relais et envoie une séquence `Esc w 2` pour basculer sur le troisième écran physique et reprendre la communication normale.

L'entrée wy60–2 observe le même format que pour les touches Maj–F1 et Maj–F2 :

- bascule en mode TPM,
- envoie la chaîne de touches de fonction à l'autre ordinateur,
- désactive le mode TPM,
- bascule sur l'autre port série.

La touche de fin Ctrl–F2 fonctionne de façon identique sur les deux ordinateurs : elle envoie la séquence de touches de fin à l'autre ordinateur par le biais du mécanisme d'impression transparente, fait passer le terminal dans la fenêtre 0, vide l'écran et quitte.

Modems

Les modems assurent les communications série via des lignes téléphoniques ordinaires. Cette section présente les normes relatives aux modems et explique comment installer et configurer les modems courants.

Généralités

Un *modem* est un dispositif qui permet de connecter deux ordinateurs via des lignes téléphoniques ordinaires. Le système téléphonique actuel est incapable de prendre en charge les variations de tension requises pour une connexion numérique directe. Le modem supprime cette contrainte en convertissant les informations numériques en fréquences transmissibles via une ligne téléphonique (modulation) et en rétablissant ces signaux en données numériques à réception (démodulation). Les modems sont couramment utilisés avec les protocoles BNU (Basic Network Utilities) et autres versions d'UUCP (UNIX–to–UNIX Copy Program). Un modem à haut débit (supérieur à 14 400 bps) peut être utilisé avec le protocole SLIP (Serial Line Internet Protocol) pour fournir en sus la connectivité TCP/IP.

On exprime souvent la vitesse des modems en *bauds* au lieu de bps (bits par seconde). Le baud est en fait l'unité de mesure du débit de modulation. Sur les modèles plus anciens, où un seul bit était codé à chaque changement de signal, le débit en bauds équivalait à la vitesse du modem. A des vitesses supérieures, les modems fonctionnent généralement à un débit de 2 400 (voire 1 200) bauds et codent deux ou plusieurs bits par changement de signal. La vitesse d'un modem en bps est le produit du nombre de bits de données par signal par le nombre de bauds (par exemple, 2 400 bauds x 6 bits par changement de signal = 14 400 bps). La plupart des modèles actuels peuvent communiquer à diverses vitesses (par exemple 14 400, 9 600, 7 800, 4 800 et 2 400 bps).

Normes de télécommunication

Sur les anciens modèles, les vitesses (300, 1 200 et 2 400 bps) étaient précisément définies. Mais pour atteindre des vitesses plus élevées, les constructeurs de modems ont commencé à développer diverses technologies, chacune selon des méthodes propriétaires incompatibles entre elles. De nos jours, ces communications à haut débit sont normalisées par le comité UIT–TSS (ex–CCITT : Consultative Committee for International Telephony and Telegraphy).

Les modems à haut débit modernes se révèlent bien plus lents que d'autres modes de téléinformatique. Ainsi, un modem à haut débit fonctionne généralement à 28 800 bps alors qu'une connexion Ethernet atteint 10 000 000 bps. Pour intensifier le débit de données, ces modems offrent généralement des algorithmes de compression qui permettent d'atteindre des vitesses de 57 600 bps (pour un débit de 14 400 bps) et 115 200 bps (pour un débit de 28 800 bps). Ces algorithmes de compression, on le voit, dépendent des données transmises. Si les données sont déjà compressées (par la commande **compress**, par exemple), les recompresser offre peu ou pas d'intérêt et peut même ralentir le débit. Pour l'exploitation d'un modem avec compression des données, la vitesse de la connexion ETTD/ETCD entre le terminal et le modem doit être supérieure au débit de données nominal de la connexion entre modems. Par exemple, sur un modem V.32*bis* avec compression de données V.42*bis*, le débit de données du modem (vitesse de communication via les lignes téléphoniques) est 14 400 bps. Si la compression V.42*bis* est active, le débit de données réel peut atteindre 57 600 bps. Pour s'adapter au débit supérieur offert par la compression de données, la vitesse de la connexion ATTD/ATCD entre l'ordinateur et le modem doit être fixée à 57 600 bps.

> **Avertissement :** Certains modems offrant la compression et des schémas de modulation modernes peuvent développer un débit de données supérieur à celui accepté par certains systèmes ou certaines cartes asynchrones.

De nos jours, le comité UIT–TSS (ex-CCITT) établit des normes de communication haut débit incluant des algorithmes de compression de données. Les normes édictées sont généralement appelées V.*nn*, *nn* représentant un numéro. Il existe aussi une autre norme, moins connue : le protocole MNP (Microcom Networking Protocol). Disponible dans les versions (ou classes) 1-9, il s'agit d'un protocole haut débit et haute performance qui a été mis en place très tôt et s'est imposé comme standard de facto avant l'avènement des normes CCITT.

Normes de communications UIT-TSS

Voici une liste non exhaustive des normes de communication courantes définies par l'UIT–TSS.

V.29	Norme ITU–TSS pour communication en semi-duplex 9600 bps.
V.32	Norme ITU–TSS pour communication en duplex intégral à 9600 bps.
V.32*bis*	Norme ITU–TSS pour communication à 14 400 bps. V.32*bis* est une révision de la norme V.32.
V.34	Norme ITU–TSS pour communication à 28 400 bps. Cette norme vise un débit de données de 28 800 via un codage de bits multiple au lieu du schéma de compression de données utilisé par MNP Classe 9 (ex-norme V.*fast)*.
V.42	Norme de compression de données ITU–TSS.
V.42bis	Norme révisée de compression de données ITU–TSS.

Normes de communication MNP

MNP classe 1	Méthode asynchrone, en semi-duplex, orientée octets pour le transfert des données avec 70 % d'efficacité. Peu courante sur les modems modernes.
MNP classe 2	Equivalent de la norme MNP classe 1 en duplex intégral. Peu courante sur les modems modernes.
MNP classe 3	Méthode synchrone, en duplex intégral, orientée bits pour le transfert des données avec 108 % d'efficacité (réalisation d'une efficacité supérieure à 100 % du fait de l'élimination des bits de départ et d'arrêt requis pour une connexion asynchrone ; la connexion ETTD/ETCD entre le modem et le système est cependant asynchrone).
MNP classe 4	Amélioration de la norme MNP classe 3 incluant un mécanisme de variation de la taille des paquets (assemblage adaptatif de paquets) et d'élimination des charges administratives redondantes (optimisation de la phase de données). Un modem conforme à MNP classe 4 offre environ 120 % d'efficacité.
MNP classe 5	Fonctions de la classe 4 complétées par la compression des données. Un modem conforme à MNP classe 5 offre 200 % d'efficacité.
MNP classe 6	Norme permettant l'incorporation dans un modem de plusieurs techniques de modulation incompatibles (négociation de liaison universelle). Les modems conformes à MNP classe 6 peuvent entamer la communication à basse vitesse et négocier une transition vers une vitesse supérieure. Inclut un schéma de duplexage statistique qui alloue dynamiquement l'utilisation de la modulation en semi-duplex pour simuler un service en duplex intégral. Englobe la totalité des fonctions de MNP classe 5.
MNP classe 7	Norme incorporant une méthode améliorée de compression de données. Combinée avec la classe 4, elle réalise une efficacité de 300 %.

MNP classe 8	Non applicable
MNP classe 9	Norme alliant à la technologie V.32 la compression de données améliorée pour atteindre un débit de 28 800 bps.

Modems génériques

Pour installer un modem :

1. Raccordez-le.
2. Ajoutez une unité tty pour ce modem.
3. Configurez le modem.

Raccordement du modem

Utilisez les câbles qui conviennent, dont voici les références et les descriptions : Reportez–vous à la documentation de l'unité système pour plus d'informations sur les câbles à utiliser.

Ajout d'un TTY pour le modem

Assurez-vous que le système est sous tension et le modem hors tension. Utilisez le raccourci Web-based System Manager, les **unités wsm** ou le raccourci SMIT **smit mktty**. Voici quelques exemples de configuration de ports pour tty :

Carte mère	SA0
***Numéro de port**	{0}
ETAT de l'unité à l'amorçage	{available}
Activation de la CONNEXION	disable
Débit en bauds	{9600}
PARITE	{8}
BITS par caractère	{8}
Nombre de BITS D'ARRET	{1}
DELAI avant passage à déf. de port suivante	{0}
Etablissement de liaison XON-XOFF	yes
Type de TERMINAL	{dumb}

Notez que les paramètres suivants dépendent de votre configuration :

- Numéro de port dépend du port et de la carte auxquels le modem est raccordé.
- Vitesse de transmission (BAUDS) dépend des caractéristiques du modem.
- Activation de la CONNEXION dépend de l'utilisation du port.

Les valeurs possibles pour Activation de la CONNEXION sont :

Valeur	Description
DESACTIVATION	Le tty est désactivé dans le fichier /**etc**/**inittab**. Aucune commande getty n'est lancée sur ce port au démarrage du système.
ACTIVATION	Le port exécute immédiatement un getty. Cette valeur concerne plutôt les modems d'appel et les connexions au terminal.
PARTAGE	Le port lance un getty lorsqu'un signal de porteuse est confirmé par un ETCD (équipement terminal de circuit de données), tel qu'un modem. Un port partagé peut être utilisé en appel et en réception sans intervention de l'utilisateur, mais alors l'unité ETCD ne doit confirmer le signal de porteuse que lorsqu'il est effectivement établi.
RETARD	Le port ne lance de getty qu'après réception d'un caractère dans le tampon d'entrée : l'ETCD envoie un caractère à l'ETTD (équipement terminal de transmission de données) ou transmet un caractère à partir de l'ETTD/ETCD distant. Un port différé peut être utilisé pour l'appel et la réception mais son utilisateur doit envoyer un caractère (ou deux) avant que le port n'annonce la connexion.

Configuration du modem

Vous avez le choix entre les deux méthodes ci-après.

Envoi de commandes AT via cu

Si BNU (Basic Network Utilities) est installé sur votre système, vous pouvez utiliser la commande **cu** comme suit :

1. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Devices** (à moins qu'elle n'y figure déjà). Cette configuration vaut pour la plupart des modems compatibles Hayes. Remplacez le signe # par le numéro de votre port.

   ```
   Direct tty# - Any direct
   ```

2. Entrez les commandes ci-dessous (lisez les commentaires avant d'exécuter les commandes).

`pdisable tty#`	
`cu -l tty#`	Utilise `cu -ml tty#` si ix24051 est installé pour **cu**.
`AT&F`	Restaure la configuration par défaut d'usine.
`ATE1`	Dans l'état "commande", renvoie les caractères du clavier vers l'écran (vérifiez que la porteuse n'est pas activée (ON) sur le port ou le modem).

   Remarque : Vous ne devez spécifier qu'une des quatre commandes suivantes.

`AT&D2`	Contrôle le signale TDP (terminal de données prêt). Lors d'une désactivation du signal TDP, le modem raccroche et passe à l'état "commande".
`AT&D3`	Contrôle le signal TDP. Lors d'une désactivation du signal TDP, le modem raccroche et réinitialise.
`AT&W`	Enregistre les paramètres mémorisables de la configuration courante dans la mémoire du modem.
`AT&C1`	Suit l'état du signal de détection de porteuse (le modem peut se déconnecter).

   Remarque : Spécifiez cette commande uniquement si la précédente a entraîné la déconnexion du modem.

`cu -l tty#`	
`ATS0=1`	Place le modem en mode de réponse automatique (Autoanswer).
`ATS9=12`	Définit le temps de réponse de détection de porteuse. (valeur par défaut : 6 ; valeurs possibles : 1 à 255).
`AT&W`	Enregistre les paramètres mémorisables de la configuration courante dans la mémoire du modem.
`~.`	Met fin à la session **cu**.

3. Entrez *une* des commandes suivantes :

```
penable  tty#
pshare   tty#
pdelay   tty#
pdisable tty#
```

Le modem est à présent doté de la configuration de base requise pour la plupart des communications système. En cas de problème, appelez **cu** par la commande **cu -dl** pour lancer un suivi de diagnostics sur la connexion.

Envoi de commandes AT via un programme C

Si la méthode précédente n'aboutit pas ou que BNU n'est pas installé, exécutez le programme C ci-après. Créez un fichier appelé **motalk.c** contenant le code ci-après. Sauvegardez le fichier. Compilez-le puis exécutez-le en suivant les indications données en commentaire dans le programme.

```
/*************************************************************/
/*  MoTalk - A "C" program for modem setup.                  */
/*           This program is meant as an aid only and is     */
/*           not supported by IBM.                           */
/*                  compile:  cc -o motalk motalk.c          */
/*                  Usage:  motalk /dev/tty? [speed]         */
/*************************************************************/
#include <errno.h>
#include <stdio.h>
#include <signal.h>
#include <fcntl.h>
#include <termio.h>
FILE *fdr, *fdw;
int fd;
struct termio term_save, stdin_save;
void Exit(int sig)
{
   if (fdr) fclose(fdr);
   if (fdw) fclose(fdw);
   ioctl(fd, TCSETA, &term_save);
   close(fd);
   ioctl(fileno(stdin), TCSETA, &stdin_save);
   exit(sig);
}
main(int argc, char *argv[])
{
   char *b, buffer[80];
   int baud=0, num;
   struct termio term, tstdin;
   if (argc < 2 || !strcmp(argv[1], "-?"))
   {
      fprintf(stderr, "Usage: motalk /dev/tty? [speed]\n");
      exit(1);
   }
   if ((fd = open(argv[1], O_RDWR | O_NDELAY)) < 0)
   {
      perror(argv[1]);
```

```
      exit(errno);
   }
   if (argc > 2)
   {
      switch(atoi(argv[2]))
      {
         case   300: baud = B300;
                     break;
         case  1200: baud = B1200;
                     break;
         case  2400: baud = B2400;
                     break;
         case  4800: baud = B4800;
                     break;
         case  9600: baud = B9600;
                     break;
         case 19200: baud = B19200;
                     break;
         case 38400: baud = B38400;
                     break;
         default:    baud = 0;
                     fprintf(stderr, "%s: %s is an unsupported
baud\n", argv[0],argv[2]);
                     exit(1);
         }
      }
   /* Save stdin and tty state and trap some signals */
   ioctl(fd, TCGETA, &term_save);
   ioctl(fileno(stdin), TCGETA, &stdin_save);
   signal(SIGHUP, Exit);
   signal(SIGINT, Exit);
   signal(SIGQUIT, Exit);
   signal(SIGTERM, Exit);
   /*  Set stdin to raw mode, no echo */
   ioctl(fileno(stdin), TCGETA, &tstdin);
   tstdin.c_iflag = 0;
   tstdin.c_lflag &= ~(ICANON | ECHO);
   tstdin.c_cc[VMIN] = 0;
   tstdin.c_cc[VTIME] = 0;
   ioctl(fileno(stdin), TCSETA, &tstdin);
   /*  Set tty state */
   ioctl(fd, TCGETA, &term);
   term.c_cflag |= CLOCAL|HUPCL;
   if (baud > 0)
   {
      term.c_cflag &= ~CBAUD
      term.c_cflag |= baud;
   }
   term.c_lflag &= ~(ICANON | ECHO); /* to force raw mode */
   term.c_iflag &= ~ICRNL; /* to avoid non-needed blank lines */
   term.c_cc[VMIN] = 0;
   term.c_cc[VTIME] = 10;
   ioctl(fd, TCSETA, &term);
   fcntl(fd, F_SETFL, fcntl(fd, F_GETFL, 0) & ~O_NDELAY);
   /*  Open tty for read and write */
   if ((fdr = fopen(argv[1], "r")) == NULL )
   {
      perror(argv[1]);
      exit(errno);
   }
   if ((fdw = fopen(argv[1], "w")) == NULL )
   {
      perror(argv[1]);
      exit(errno);
```

```
    }
    /*  Talk to the modem */
    puts(”Ready... ^C to exit”);
    while (1)
    {
       if ((num = read(fileno(stdin), buffer, 80)) > 0)
          write(fileno(fdw), buffer, num);
       if ((num = read(fileno(fdr), buffer, 80)) > 0)
          write(fileno(stdout), buffer, num);
       Exit (0);
    }
}
```

Modems Hayes et compatibles

1. Modifiez la configuration de tty à l’aide du raccourci Web-based System Manager, des **unités wsm** ou du raccourci SMIT, **smit chtty**.

   Vous trouverez ci-après des exemples de configuration de modem. (`tty0` est donné à titre d’exemple et le débit, fonction de votre modem, est généralement fixé au maximum autorisé.)

TTY	tty0
TTY type	tty
Interface TTY	rs232
Description	Asynchronous Terminal
Etat	Available
Emplacement	00–00–s1–00
Unité mère	sa0
Numéro de port	s1
Activation de la CONNEXION	share
Débit en bauds	2400
PARITE	none
BITS par caractère	8
Nombre de BITS D’ARRET	1
DELAI avant passage à déf. de port suivante	0
Etablissement de liaison XON-XOFF	no
Type de TERMINAL	dumb
Fichier mappe d’ENTREE	none
Fichier mappe de SORTIE	none
Fichier mappe de JEU DE CODES	sbcs

   Attributs STTY pour le RUN TIME :

   `[hupcl,cread,brkint,icrnl,opost,tab3,onlcr,icanon,echo,echoe,echo k,echoctl,`
   `echoke,imaxbel,iexten]`

   (aucun **ixon/ixoff** requis)

   Attributs STTY pour la connexion :

   `[hupcl,cread,echoe,cs8]`

   (aucun **ixon/ixoff** requis)

2. Ajoutez dans le fichier **/usr/lib/uucp/Systems** :

```
hayes Nvr HAYESPROG 2400
```

3. Ajoutez dans le fichier **/usr/lib/uucp/Devices** :

```
# For programming the hayes modem only:
HAYESPROG tty0 - 2400 HayesProgrm2400
#regular ACU entry:
ACU tty0 - Any hayes
```

4. Ajoutez dans le fichier **/usr/lib/uucp/Dialers** :

```
# This Entry is used to PROGRAM the modem ONLY:
# the next 3 lines should be made into one:
HayesProgrm2400     =,-,     "" \d\dAT\r\c OK AT&F\r\c OK
ATM1\r\c OK
AT&D3\r\c OK AT&K3&C1\r\c OK ATL0E0Q2\r\c OK ATS0=1\r\c OK
AT&W\r\c
OK
hayes     =,-,     "" \dAT\r\c OK ATDT\T\d\r\c CONNECT
```

5. Pour programmer le modem, entrez `cu -d hayes`. Aucune connexion n'étant établie avec un autre système, la commande échoue. Le modem est programmé si `sendthem AT&W` et `OK got it` s'affichent en sortie.

   Si vous n'effectuez pas de transferts de fichier binaire ou que vous n'utilisez pas BNU, sortez de **&K3**, et positionnez XON–XOFF sur **Yes** dans SMIT ou vérifiez dans Web-based System Manager. Autre méthode, plus efficace : activez le contrôle de flux matériel, via les paramètres de SMIT et les entrées `Dialers` ci-dessus.

Une fois le modem programmé, définissez la procédure de liaison RTS (demande pour émettre) de façon que le pilote d'unité système utilise le contrôle de flux matériel. Pour ce faire, le modem doit être connecté à un autre système (afin d'élever la fréquence de porteuse) et la commande ci-dessous exécutée :

```
stty add rts < /dev/tty0
```

Veillez à remplacer `tty0` par votre numéro de tty. Cette configuration n'est valable que pour la session en cours. Pour que RTS soit automatiquement ajouté au lancement du système, tapez et compilez le programme **addrts.c** ci-après. Insérez ensuite dans le fichier **/etc/rc** une ligne d'appel du programme (qui ne requiert pas que la fréquence de porteuse soit élevée) :

```
addrts /dev/tty0
```

Le chemin d'accès complet à cette commande doit être spécifié si le programme **addrts** n'est pas dans un répertoire de PATH (indiquez votre numéro de tty à la place de `tty0`).

Ajout d'une procédure RTS (demande pour émettre) sur les ports TTY

```
/*            C Program to add RTS discipline to tty port(s).

   Tips:
         To make the program more permanent, insert the file name of
         the compiled version (complete with path) at the end of your
         "/etc/rc" file and the changes will take effect again at next
         reboot.

         NOTE: This program is supplied "as is" and is NOT supported by
               IBM.  It is intended as an aid to administrators only.

 ____________________________________________________________________
     To create:     vi addrts.c <enter>

     To compile:    cc -o addrts  addrts.c
     Usage is:      addrts /dev/tty##
 ____________________________________________________________________ */
/*                          Program starts now                      */
#include <stdio.h>
#include <fcntl.h>
#include <termios.h>
#include <sys/tty.h> main (argc,argv)
{
   int argc;
   char *argv[];
   int fd;
   if ( (fd = open(argv[1], O_NDELAY|O_RDWR)) <0 )
   {
      printf("%s: could not open %s\n",argv[0],argv[1]);
      exit (22);
   }
   ioctl(fd, TXADDCD, "rts");
   /*  adds rts to the tty in the argument */
   close(fd);
}
```

Conseils

Voici quelques informations et conseils relatifs à la configuration de divers modems.

Modem IBM 7855

Remarque : `tty0` est utilisé en guise d'exemple. Remplacez `tty0` par le tty auquel le modem est raccordé.

Pour utiliser le modèle IBM 7855 comme modèle d'appel et de réception sur le système, le modem doit être configuré pour accepter les commandes AT. Pour ce faire, appuyez simultanément sur les touches fléchées gauche et droite du modem. Vous devez lire sur le panneau avant :

```
<Exit     Enter>
```

Appuyez sur la flèche droite (Enter), puis sur la flèche vers le bas jusqu'à ce que s'affiche `First Setup`. Appuyez ensuite sur la flèche droite. Appuyez sur la flèche vers le haut jusqu'à ce que `Asynchronous AT` s'affiche. Pour sortir du menu, appuyez sur la flèche vers la gauche.

1. Modifiez la configuration de tty à l'aide du raccourci Web-based System Manager, des **unités wsm** ou du raccourci SMIT, **smit chtty**.

2. Sélectionnez le tty pour le modem et effectuez les modifications. Voici des exemples de configuration :

   Remarque : Les options non pertinentes pour cette opération ne sont pas citées dans la liste ci–dessous.

TTY	tty0
TTY type	tty
Interface TTY	rs232
Description	Asynchronous Terminal
Etat	Available
Emplacement	00–00–s1–00
Unité mère	sa0
Numéro de port	s1
Activation de la CONNEXION	share
Débit en bauds	19200
PARITE	none
BITS par caractère	8
Nombre de BITS D'ARRET	1
DELAI avant passage à déf. de port suivante	0
Etablissement de liaison XON-XOFF	no
Type de TERMINAL	dumb
Fichier mappe d'ENTREE	none
Fichier mappe de SORTIE	none
Fichier mappe de JEU DE CODES	sbcs

   Attributs STTY pour le RUN TIME :

   ```
   [hupcl,cread,brkint,icrnl,opost,tab3,onlcr,icanon,echo,echoe,echo
   k, echoctl,echoke,imaxbel,iexten](aucun ixon/ixoff requis)
   ```

   Attributs STTY pour la connexion :

   ```
   [hupcl,cread,echoe,cs8]
   ```

   (aucun **ixon**/**ixoff** requis)

3. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Systems** les deux lignes suivantes (commencez à la colonne la plus à gauche) :

   ```
   ibm7855 Nvr IBMPROG 19200
   slip Nvr SLIPPROG 19200
   ```

4. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Devices** les lignes suivantes (commencez à la colonne la plus à gauche) :

```
IBMPROG tty0 - Any IBMProgrm
SLIPPROG tty0 - Any SlipProgrm

# Usual ACU entry
ACU tty0 - Any ibm

# ACU entry to quietly dial the modem.
ACUQ tty0 - Any ibmq

# IBM7855 ACU entry to negotiate for error correction and compression
ACUECLC tty0 - Any ibmeclc

# IBM7855 ACU entry to negotiate for error correction and compression
# using large (256 byte) data block size
ACUECLB tty0 - Any ibmeclclb

# IBM 7855 ACU entry to use ECL without compression
ACUECL tty0 - Any ibmecl
```

5. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Dialers** les lignes suivantes (commencez à la colonne la plus à gauche) :

```
# IBM 7855 program. Use ibmeclcbc for 256 byte block size.  However,
# Noisey lines may obtain better throughput by setting the block size to
# be 64 bytes; compressed files will show better throughput
# by turning off compression.
# The following 3 lines should be joined into one line:
IBMProgrm       =,-,    "" \dATQ0\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OK AT&C1\R2\Q2\M14\r\c OK AT&B8N1L0E0\r\c OK ATS0=1\r\c
OK ATQ1&W0&Y0\r\c ""

# The following 3 lines should be joined into one line:
SlipProgrm      =,-,    "" \dATQ0\r\c OK AT&F\r\c OK ATM1\r\c OK
AT&D3\r\c OK AT&C0\R2\Q2\r\c OK AT&B8N1L0E0\r\c OK
ATS0=1\r\c OK ATQ1&W\r\c ""

ibm     =,-,    "" \dATQ0\r\c OK ATDT\T\d\r\c CONNECT
ibmq    =,-,    "" \dATQ0\r\c OK ATM0DT\T\d\r\c CONNECT

#IBM 7855 with ECLC and Compression
# (Note two backslashes are needed before the N; cu won't send \N
# without preceeding it with a \)
ibmeclc =,-,    "" \dAT\\N3%C1Q0\r\c OK ATDT\T\d\r\c CONNECT

#IBM 7855 ECLC Compression with 256 byte block size
ibmeclclb       =,-,    "" \dAT\\N3%C1Q0\A3\r\c OK ATDT\T\d\r\c CONNECT

# IBM 7855 ECL without compression
ibmecl  =,-,    "" \dAT\\N3%C0Q0\r\c OK ATDT\T\d\r\c CONNECT
```

Programmation du modèle IBM 7855

1. Désactivez (temporairement) le port à l'aide de la commande : `pdisable tty0.`
2. Sur la ligne de commande, entrez `cu -d ibm7855`.

   La commande échoue, aucune connexion n'étant établie, mais, si vous obtenez en sortie :

   ```
   Sendthem (ATQ1&W0&Y0^MNO CR)
   expect: ("")
   got it
   ```

la programmation a abouti. Le message `ASYN8N A 9600 a` s'affiche sur l'afficheur à l'avant. `pshare tty0` est alors possible.

Une fois le modem programmé, vous pouvez définir la procédure RTS qui permet le contrôle de flux matériel. Pour ce faire, le modem doit être connecté à un autre système (afin d'élever la fréquence de porteuse) et la commande ci-dessous exécutée :

```
stty add rts < /dev/tty0
```

Veillez à remplacer tty0 par votre numéro de tty. Ce changement n'est effectif que pour la session en cours.

Pour que RTS soit automatiquement ajouté au lancement du système, tapez et compilez le programme **addrts.c** ci-après, et insérez dans le fichier /**etc**/**rc** une ligne d'appel du programme (qui ne requiert pas que la fréquence de porteuse soit élevée).

```
/* C Program to add RTS discipline to tty port(s).

  Tips:
          To make the program more permanent, insert the file name of
          the compiled version (complete with path) at the end of your
          "/etc/rc" file and the changes will take effect again at next
          reboot.  Usage is addrts /dev/tty##.


      NOTE: This program is supplied "as is" and is NOT supported by
                IBM.  It is intended as an aid to administrators only.
 ____________________________________________________________________________
     To create:     vi addrts.c <enter>
     To compile:    cc -o addrts  addrts.c
 ____________________________________________________________________________ */
/*         Program starts now                                                 */
#include <stdio.h>
#include <fcntl.h>
#include <termios.h>
#include <sys/tty.h>
main (argc,argv)
        int argc;
        char *argv[];
{
        int fd;
        if ( (fd = open(argv[1], O_NDELAY|O_RDWR)) <0 ) {
                printf("%s: could not open %s\n",argv[0],argv[1]);
                exit (22);
                }
        ioctl(fd, TXADDCD, "rts");  /*  adds rts to the tty in the
argument */
        close(fd);
}
```

Modèle MultiTech MULTIMODEM II

1. Utilisez les commandes AT **L5**, **L6** et **L7** pour afficher les paramètres du modem.

```
ATL5
B1 E1 M1 Q0 R0 V1 X0 &E1 &E4 &E6 &E8 &E10 &E13 &E15
$MB9600 $SB9600 $BA0 &W0

OK
ATL6
S0   S2   S3   S4   S5   S6   S7   S8   S9   S10  S11  S13  S24  S25  S30
001  043  013  010  008  002  045  002  025  007  070  037  020  001  000

OK
ATL7
$A0 &A0 #A0 &B0 &BS1 &C1 $D0 &D2 #DB0 $EB0 %E1 #F0 $F1 &G0 #L0 $MI0 &M0
&P0 #P2 &Q0 $R0 &R1 &RF1 &S0 $SP0 &SF0 #T1 $V0 $V6 $VD0 &X0 Y0
$MB9600 $SB9600 $BA0 &W0
OK
```

Remarque : Dans l'exemple ci-dessus, le registre s9 a été défini à 25. Sa valeur par défaut est 6. Normalement, il doit prendre une valeur comprise entre 15 et 20.

2. Sur les modems configurés pour des débits de 9600 bauds maximum, l'établissement de liaison matérielle RTS/CTS doit avoir été ajouté au port tty. Pour cela, vous avez le choix entre :

   a. Appliquer la procédure suivante :

   - Ajoutez **clocal** aux attributs stty de Runtime pour votre tty, via **smit chtty**.
   - Sur la ligne de commande, entrez : `pdisable ttyN` (`N` est votre numéro de tty).
   - Exécutez la commande `stty add rts < /dev/ttyN`.
   - Exécutez la commande `stty get < /dev/ttyN`. RTS doit apparaître en ligne.

   b. Exécuter le programme C :

```
/*  C Program to add RTS discipline to tty port(s).

  NOTE: This program is supplied "as is" and is NOT supported by
        IBM.  It is intended as an aid to administrators only.
*/
/*                          Program starts now
*/
#include <stdio.h>
#include <fcntl.h>
#include <termios.h>
#include <sys/tty.h>
main()
{
   int fd;
      fd = open("/dev/tty0", O_NDELAY|O_RDWR);
      ioctl(fd, TXADDCD, "rts");      /*  adds rts to tty0
*/
      close(fd);
}
/*                             END Program
*/
```

Modem de périphériques pratiques

1. Modifiez la configuration de tty à l'aide du raccourci Web-based System Manager, des **unités wsm** ou du raccourci SMIT, **smit chtty**.
2. Sélectionnez le tty pour le modem et effectuez les modifications. tty0 est donné à titre d'exemple et le débit, fonction de votre modem, est généralement fixé au maximum autorisé. Voici des exemples de configuration :

   Remarque : Les options non pertinentes pour cette opération ne sont pas citées dans la liste ci–dessous.

TTY	tty0
TTY type	tty
Interface TTY	rs232
Description	Asynchronous Terminal
Etat	Available
Emplacement	00–00–s1–00
Unité mère	sa0
Numéro de port	s1
Activation de la CONNEXION	share
Débit en BAUDS	2400
PARITE	none
BITS par caractère	8
Nombre de BITS D'ARRET	1
DELAI avant passage à déf. de port suivante	0
Etablissement de liaison XON-XOFF	no
Type de TERMINAL	dumb
Fichier mappe d'ENTREE	none
Fichier mappe de SORTIE	none
Fichier mappe de JEU DE CODES	sbcs

   Attributs STTY pour le RUN TIME :

   ```
   [hupcl,cread,brkint,icrnl,opost,tab3,onlcr,icanon,echo,echoe,echo
   k,
   echoctl,echoke,imaxbel,iexten](aucun ixon/ixoff requis)
   ```

   Attributs STTY pour la CONNEXION :

   ```
   [hupcl,cread,echoe,cs8](aucun ixon/ixoff requis)
   ```

3. Ajoutez dans le fichier **/usr/lib/uucp/Systems** la ligne :

   ```
   pracper Nvr PRACPERPROG 2400
   ```

4. Ajoutez dans le fichier **/usr/lib/uucp/Devices** :

   ```
   # For programming the Practical Peripherals modem only:
   PRACPERPROG tty1 - 2400 PracPerProgram2400

   # regular ACU entry:
   ACU tty1 - Any hayes
   ```

5. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Dialers** :

```
# This Entry is used to PROGRAM the modem ONLY:
# the next 3 lines should be made into one:
PracPerProgram2400      =,-,    "" \d\dAT\r\c OK AT&F\r\c OK
ATM1\r\c OK
AT&D3\r\c OK AT&C1\r\c OK ATL0E0\r\c OK ATS0=1S9=20\r\c OK
AT&W\r\c
OK

hayes   =,-,    "" \dAT\r\c OK ATDT\T\d\r\c CONNECT
```

6. Pour programmer le modem, entrez le commande `cu -d pracper`. La commande échoue, aucune connexion n'étant établie, mais le modem est programmé si vous obtenez `sendthem AT&W` puis `OK got it` en sortie.

Une fois le modem programmé, vous pouvez définir la procédure RTS qui permet le contrôle de flux matériel. Pour ce faire, le modem doit être connecté à un autre système (afin d'élever la fréquence de porteuse) et la commande **stty add rts < /dev/tty0** exécutée. Veillez à remplacer tty0 par votre numéro de tty. Ce changement n'est effectif que pour la session en cours. Pour que RTS soit automatiquement ajouté au lancement du système, tapez et compilez le programme **addrts.c** ci-après, et insérez dans le fichier **/etc/rc** une ligne d'appel du programme (qui ne requiert pas que la fréquence de la porteuse soit élevée).

Modem Telebit T1600

1. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Systems** :

```
telebit Nvr TELEPROG 19200
```

2. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Devicesca** :

```
#
#  Devices entry to use to program the T1600
#
TELEPROG tty0 - 19200 TelebitProgram
#
#  19200, 9600 baud (fast) Telebit Trailblazer modem
#
ACU       tty0 - 19200 tbfast \D
ACUTB     tty0 - 19200 tbfast \D
ACU96     tty0 - 9600 tbfast \D
#
#  2400 baud Telebit Trailblazer modem
#
ACU       tty0 - 2400 tb2400 \D
ACU24     tty0 - 2400 tb2400 \D
#
#  1200 baud Telebit Trailblazer modem
#
ACU       tty0 - 1200 tb1200 \D
ACU12     tty0 - 1200 tb1200 \D
```

3. Ajoutez dans le fichier **/usr/lib/uucp/Dialers** :

```
#
# Entry to program the modem ONLY
# The next 3 lines should be made into one long line:
TelebitProgram  =,-,    "" \dAT&F\r\c OK
ats0=1s2=255s7=60s11=50s41=2s45=255s51=252s63=1s58=2s64=1\r\c OK
ATs69=2s105=0s111=30s255=0M0&C1Q2&D3&Q0&R3&S1&T5\r\c OK
ATE0X12&W\r\c OK
#
# Telebit T1600 Dialers entries
#
tbfast  =,-,     "" \dATs50=255s7=60\r\c OK\r ATDT\T\r\c
CONNECT-\d\c-CONNECT
tb2400  =,-,     "" \dATs50=3\r\c OK\r ATDT\T\r\c CONNECT
tb1200  =,-,     "" \dATs50=2\r\c OK\r ATDT\T\r\c CONNECT
```

4. Pour programmer le modem, entrez `cu -d telebit`. Cette ligne est interprétée par la commande **cu** comme une demande de connexion à un système et la commande échoue. Vérifiez que la sortie de la commande est OK.

Modem Telebit T2000

1. Ajoutez dans le fichier **/usr/lib/uucp/Systems** :

```
telebit Nvr TELEPROG 19200
```

2. Ajoutez dans le fichier **/usr/lib/uucp/Devices** :

```
#
#  Devices entry to use to program the T2000
#
TELEPROG tty0 - 19200 TelebitProgram
#
#  19200, 9600 baud (fast) Telebit Trailblazer modem
#
ACU       tty0 - 19200 tbfast \D
ACUTB     tty0 - 19200 tbfast \D
ACU96     tty0 - 9600 tbfast \D
#
#  2400 baud Telebit Trailblazer modem
#
ACU       tty0 - 2400 tb2400 \D
ACU24     tty0 - 2400 tb2400 \D
#
#  1200 baud Telebit Trailblazer modem
#
ACU       tty0 - 1200 tb1200 \D
ACU12     tty0 - 1200 tb1200 \D
#
#  For sites with MNP modems
#
ACUM12     tty0 - 1200 tb12mnp \D
ACUM24     tty0 - 2400 tb24mnp \D
```

3. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Dialers** :

```
#
# Entry to program the modem ONLY
#
# The next 4 lines will be made into one:
TelebitProgram  =,-,    "" \dAT&F\r\c OK
ats2=255s7=60s11=50s41=2s45=255s51=252s52=2s54=3s58=2s64=1\r\c OK
ATs69=1s92=1s96=0s105=0s110=1s111=30s130=3s131=1F1M0Q6TV1W0X3Y0&P
0&T5\r\c
OK ATE0&W\r\c OK  00
#
# Telebit T2000 dialers Entries:
#
tbfast  =,-,     "" \dATs50=255s7=60\r\c OK\r ATDT\T\r\c
CONNECT-\d\c-CONNECT
tb2400  =,-,     "" \dATs50=3\r\c OK\r ATDT\T\r\c CONNECT
tb1200  =,-,     "" \dATs50=2\r\c OK\r ATDT\T\r\c CONNECT
tb24mnp =,-,     "" \dAT\r\c OK ATS0=0S95=2S50=3S41=0\r\c OK
ATDT\T\r\c CONNECT
tb12mnp =,-,     "" \dAT\r\c OK ATS0=0S95=2S50=2S41=0\r\c OK
ATDT\T\r\c CONNECT
```

4. Pour programmer le modem, entrez `cu -d telebit`. Cette ligne est interprétée par la commande **cu** comme une demande de connexion à un système et la commande échoue. Vérifiez que la sortie de la commande est OK.

Modem Telebit T3000

1. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Systems** :

```
telebit Nvr TELEPROG 19200
```

2. Ajoutez dans le fichier /**usr**/**lib**/**uucp**/**Devices** :

```
#
#  Devices entry to use to program the T3000
#
TELEPROG tty1 - 19200 TelebitProgram
#
#  19200, 9600 baud (fast) Telebit Trailblazer modem
#
ACU       tty1 - 19200 tbfast \D
ACUTB     tty1 - 19200 tbfast \D
ACU96     tty1 - 9600 tbfast \D
#
#  2400 baud Telebit Trailblazer modem
#
ACU       tty1 - 2400 tb2400 \D
ACU24     tty1 - 2400 tb2400 \D
#
#  1200 baud Telebit Trailblazer modem
#
ACU       tty1 - 1200 tb1200 \D
ACU12     tty1 - 1200 tb1200 \D
#
#  For sites with MNP modems
#
ACUM12     tty1 - 1200 tb12mnp \D
ACUM24     tty1 - 2400 tb24mnp \D
```

3. Ajoutez dans le fichier **/usr/lib/uucp/Dialers** :

```
#
# Entry to program the modem ONLY
# The following 4 lines should be made into one long line:
TelebitProgram  =,-,    "" \dAT&F\r\c OK
ats0=1s2=255s7=60s11=50s41=2s45=255s51=252s63=1s58=2s64=1\r\c OK
ATs69=2s105=0s111=30s255=0M0&C1Q2&D3&Q0&R3&S1&T5\r\c OK
ATE0X12&W\r\c
OK  00
#
# Telebit T2000 dialers Entries:  The tbfast won't work for the
T3000,
# but the rest should.
#
tbfast  =,-,     "" \dATs50=255s7=60\r\c OK\r ATDT\T\r\c
CONNECT-\d\c-CONNECT
tb2400  =,-,     "" \dATs50=3\r\c OK\r ATDT\T\r\c CONNECT
tb1200  =,-,     "" \dATs50=2\r\c OK\r ATDT\T\r\c CONNECT
tb24mnp =,-,     "" \dAT\r\c OK ATS0=0S95=2S50=3S41=0\r\c OK
ATDT\T\r\c CONNECT
tb12mnp =,-,     "" \dAT\r\c OK ATS0=0S95=2S50=2S41=0\r\c OK
ATDT\T\r\c CONNECT
```

4. Pour programmer le modem, entrez `cu -d telebit`. Cette ligne est interprétée par la commande *cu* comme une demande de connexion à un système et la commande échoue. Vérifiez dans la sortie de mise au point de la commande que `ATE0X12&W` a été envoyé et `OK` reçu. Dans l'affirmative, le modem est programmé.

Modems UDS

1. Modifiez la configuration de tty à l'aide du raccourci Web-based System Manager, des **unités wsm** ou du raccourci SMIT, **smit chtty**.
2. Sélectionnez le tty pour le modem et effectuez les modifications. Vous trouverez ci–dessous des exemples de modification (`tty0` correspond au tty dans cet exemple) :

   Remarque : Les options non pertinentes pour l'opération ne sont pas citées.

TTY	tty0
TTY type	tty
Interface TTY	rs232
Description	Asynchronous Terminal
Etat	Available
Emplacement	00–00–s1–00
Unité mère	sa0
Numéro de port	s1
Activation de la CONNEXION	share
Débit en BAUDS	19200
PARITE	none
BITS par caractère	8
Nombre de BITS D'ARRET	1
DELAI avant passage à déf. de port suivante	0
Etablissement de liaison XON-XOFF	no
Type de TERMINAL	dumb
Fichier mappe d'ENTREE	none
Fichier mappe de SORTIE	none
Fichier mappe de JEU DE CODES	sbcs

Attributs STTY pour le RUN TIME :

```
[hupcl,cread,brkint,icrrnl,opost,tab3,onlcr,icanon,echo,echoe,ech
ok, echoctl,
echoke,imaxbel,iexten](aucun ixon/ixoff requis)
```

Attributs STTY pour la connexion :

```
[hupcl,cread,echoe,cs8](aucun ixon/ixoff requis)
```

3. Ajoutez dans le fichier **/usr/lib/uucp/Systems** :

```
uds Nvr UDSPROG Any
```

4. Ajoutez dans le fichier **/usr/lib/uucp/Devices** :

```
------------begin text to insert--------
# For programming the UDS modem only:
UDSPROG tty0 - 9600 udsmodemPROGRAM

# regular ACU entry:
ACU tty0 - Any uds
-------------end text to insert---------

**  Ajoutez dans le fichier /usr/lib/uucp/Dialers file:  **

------------begin text to insert--------
# the next 2 lines should be made into one:
udsmodemPROGRAM =,-,    "" \dAT&FQ2\r\c OK
ATE0Y0&C1&D2&S1%B5%E0*LC\r\c
OK AT&W\r\c OK

uds     =,-,     "" \dAT\r\c OK\r ATDT\T\d\r\c CONNECT
```

5. Pour programmer le modem, entrez `cu -d uds`. Cette ligne est interprétée par la commande **cu** comme une demande de connexion à un système et la commande échoue. Vérifiez la sortie de la commande.

Modem Telebit T3000 90202-01 WordBlazer

Lorsque vous utilisez un modem T3000 sur un concentrateur 128 ports (exploité sous AIX version 3.2.3 étendue), modifiez les données de configuration tty à l'aide du raccourci Web-based System Manager, des **unités wsm** ou du raccourci SMIT, **smit chtty**, puis appliquez les données de configuration suivantes, à la fois dans l'interface utilisateur et sur le modem. N'utilisez *pas* le débit de 38400 bauds indiqué, sauf si votre dispositif série accepte ce débit. Modifiez la vitesse en conséquence.

Exemples de données de configuration (ne sont citées que les entrées à modifier) :

Type de TERMINAL	dumb
Activation de la CONNEXION	share
Débit en BAUDS	38 400 (peut–être 19 200 ou débit inférieur)
PARITE	none
BITS par caractère	8
Etablissement de liaison XON-XOFF	no (à 9600 bauds et plus, utiliser RTS/CTS)

Configuration tty pour modem sur carte 128 ports :

Porteuse forcée :	disable
Exécution traitement cooked sur la carte :	disable
Utilisation des brochages RJ-45 secondaires :	disable

Configuration conseillée pour les commandes et registres du modem :

Remarques :

1. Utilisez `AT&V` avec ce modem pour visualiser les valeurs courantes.
2. Modifiez le registre 51 pour tenir compte de la vitesse de votre matériel ETTD.
3. Le registre 92 est *essentiel* si vous envisagez de vous connecter à des modems ayant un débit inférieur. Sa valeur conseillée est 1.

AT&C1	Lorsque le modem local détecte un signal de porteuse d'un modem distant, le signal CD passe à l'état ON une fois le code de résultat CONNECT envoyé à l'ETTD.
AT&D3	Réinitialise le modem et passe en mode commande une fois le signal DTR basculé de ON sur OFF.
AT&S1	DSR passe sur ON lorsque le modem détecte un signal de réponse, et reste sur ON tout au long de la connexion.
ATS0=1	Place le modem en mode de réponse automatique (Autoanswer). Le modem répond à l'appel après une sonnerie.
ATS9=15	Définit à 15 l'heure de redétection de la porteuse.
ATS50=0	Définit la vitesse de modulation (0 pour une vitesse déterminée automatiquement).
ATS51=253	Définit la vitesse de l'interface ETTD (vitesse de communication entre l'ordinateur et le modem et non entre les modems). 253 est utilisée pour 38400 bps.
ATS59=15	Active les suffixes CONNECT.
ATS92=1	Sélection de la séquence de réponse.
ATQ2	Demande au modem de générer des codes de résultat à l'émission d'un appel et supprime ces codes à la réception de l'appel.
ATX12	Active les codes de résultat prolixes (verbose).

Résolution des incidents

Cette section identifie les incidents liés à l'utilisation d'un modem :

Symptôme	Cause	Solution
Le modem (ou un autre dispositif raccordé au port série) ralentit progressivement le système ou le bloque. Sa mise hors tension permet généralement de revenir à la normale.	Sur un modem intelligent, CD est toujours positionné sur ON. Le système le détecte et envoie une annonce de connexion, que le modem tente d'interpréter comme une commande. N'y parvenenant pas, le modem renvoie un écho au port tty du système. Ce cycle boucle à l'infini.	Appliquez au port tty un report de connexion (delay) sur le système pour qu'il n'y ait pas d'annonce de connexion émise. Ainsi, seul un retour chariot valide issu d'une connexion hôte générera une annonce de connexion. Vous pouvez également modifier le profil AT du modem pour que CD ne soit positionné sur ON qu'à détection d'un signal de porteuse valide sur la ligne téléphonique.

Questionnaire

Avant de faire appel à l'assistance technique, rassemblez les informations suivantes :

- Système Xtra ?
- Version du système d'exploitation ? Depuis quand l'utilisez-vous ?
- Le modem a-t-il déjà fonctionné ?
- Type du modem ? Type du modem à l'autre extrémité de la connexion téléphonique ?
- Type de carte (64 ports, 128 ports, S1,...) raccordée au modem ?
- Numéro du port auquel le modem est connecté ?
- Numéro de tty auquel le modem est connecté ?
- Type de câblage utilisé ?
- Quelle configuration de connexion (share, delay, enable) ?
- Est-il possible de connecter votre modem à d'autres modems ?
- Est-il possible de connecter d'autres modems au vôtre ?
- Quelle sont les valeurs définies au niveau de Web-based System Manager, de SMIT, du modem ou du port, pour :
  - XON/XOFF ?
  - RTS/CTS ?
  - débit BPS ?
- Effectuez les vérifications suivantes :
  - Le port se verrouille-t-il par intermittence ?
  - Pouvez-vous composer un numéro d'appel ? Les autres peuvent-ils vous appeler ?
  - Relevez-vous d'autres symptômes ?
- Ces erreurs s'affichent-elles à la console ? Quel est leur libellé ?
- Ces erreurs figurent-elles dans le compte rendu d'erreurs (**errpt** ou **errpt –a**) ?
- Quelle commande utilisez-vous pour composer un numéro d'appel ?
- Quels logiciels sont impliqués dans le système ?

Récapitulatif des commandes AT

Voici un récapitulatif du jeu de commandes Hayes Smartmodem. Ces commandes comprennent le jeu de commandes AT utilisé par un grand nombre de modems. Ces informations sont extraites de l'ouvrage Hayes Smartmodem 2400 *Quick Reference Card*, publié par Hayes Microcomputer Products, Inc.

AT	Préfixe de commande, placé en tête de la ligne de commande.
<CR>	Retour chariot (ligne suivante), placé en fin de la ligne de commande.
A	Décroche, reste en mode commande.
A/	Répète la ligne de commande précédente. Commande ni précédée de **AT** ni suivie de **<CR>**/.
B0	Applique la norme CCITT V.22 pour les communications 1 200 bps.
B1	Applique la norme Bell 212A pour les communications 1 200 bps.
D	Entre en mode émission, compose le numéro qui suit et tente de passer en ligne. D est généralement suivi de T (tonalité) ou parfois de P (impulsion).
DS=*n*	Compose le numéro stocké à l'emplacement *n.*

E0 Désactive l'écho de caractère dans l'état "commande".

E1 Active l'écho de caractère dans l'état "commande".

H0 Décroche le téléphone.

H1 Fait fonctionner le support commutateur et le relais auxiliaire.

I0 Renvoie le code d'identification du produit.

I1 Calcule le total de contrôle sur le micrologiciel ROM et renvoie le résultat.

I2 Calcule le total de contrôle sur le micrologiciel ROM et renvoie en résultat OK ou ERROR.

L0 Haut-parleur désactivé.

L1 Règle le haut-parleur à un niveau sonore faible.

L2 Règle le haut-parleur à un niveau sonore moyen.

L3 Règle le haut-parleur à un niveau sonore élevé.

M0 Haut-parleur désactivé.

M1 Active le haut parleur jusqu'à détection d'un signal de porteuse.

M2 Haut-parleur toujours en service.

M3 Haut-parleur actif jusqu'à détection d'un signal de porteuse, sauf pendant la numérotation.

O0 Passe à l'état en ligne.

O1 Passe à l'état en ligne et lance une resynchronisation d'égalisation.

Q0 Le modem renvoie les codes de résultat.

Q1 Le modem ne renvoie pas les codes de résultat.

Sr Positionne le pointeur sur le registre r.

Sr=*n* Positionne le registre r à *n.*

V0 Affiche les codes de résultat sous forme numérique.

V1 Affiche les codes de résultat sous forme littérale (verbose).

X0 Active les fonctions représentées par les codes de résultat 0–4.

X1 Active les fonctions représentées par les codes de résultat 0–5, 10.

X2 Active les fonctions représentées par les codes de résultat 0–6, 10.

X3 Active les fonctions représentées par les codes de résultat 0–5, 7, 10.

X4 Active les fonctions représentées par les codes de résultat 0–7, 10.

Y0 Désactive la déconnexion long space.

Y1 Active la déconnexion long space.

Z Réinitialise le modem.

&C0 Suppose la porteuse de données toujours présente.

&C1 Contrôle la présence de la porteuse de données.

&D0 Ignore le signal DTR.

&D1 Passe à l'état "commande" lors d'une désactivation de DTR.

&D2 Raccroche et passe à l'état "commande" lors d'une désactivation de DTR.

&D3 Réinitialise lors d'une désactivation de DTR.

&F Réactive la configuration par défaut (d'usine).

&G0 Pas de tonalité de garde.

&G1 Tonalité de garde de 500 Hz.

&G2 Tonalité de garde de 1800 Hz.

&J0 Prise télécom RJ–11/RJ41/RJ45S.

&J1 Prise télécom RJ–11/RJ–13.

&P0 Numérote avec un rapport de conjonction/disjonction 39/61.

&P1 Numérote avec un rapport de conjonction/disjonction 33/67.

&Q0 Fonctionne en mode asynchrone.

&Qn Fonctionne en mode synchrone *n.*

&R0 Contrôle la présence du signal CTS (prêt à émettre) en fonction du signal RTS (demande pour émettre).

&R1 Ignore le signal RTS et suppose la présence systématique d'un signal CTS.

&S0 Suppose la présence du signal DSR (modem prêt).

&S1 Contrôle la présence du signal DSR.

&T0 Met fin au test en cours.

&T1 Lance une boucle analogique locale.

&T3 Lance une boucle numérique.

&T4 Accepte une requête émise par un modem distant pour RDL.

&T5 Refuse une requête émise par un modem distant pour RDL.

&T6 Lance une boucle numérique distante.

&T7 Lance une boucle numérique distante avec autotests.

&T8 Lance une boucle analogique locale avec autotests.

&V Affiche la configuration active, les profils utilisateur et les numéros mémorisés.

&Wn Sauvegarde les paramètres mémorisables de la configuration active comme profil utilisateur *n*.

&X0 Signal d'horloge de transmission émis par le modem.

&X1 Signal d'horloge de transmission émis par le terminal de données.

&X2 Signal d'horloge de transmission émis par la porteuse réceptrice.

&Yn Rappelle le profil utilisateur *n*.

&Zn=*x* Stocke le numéro de téléphone *x* à l'emplacement *n*.

Récapitulatif des registres S

Registre	Intervalle	Description
S0	0–255	Nombre de sonneries avant décrochage.
S1	0–255	Compteur de sonnerie (incrémenté à chaque sonnerie).
S2	0–127	Code ASCII du caractère d'échappement.
S3	0–127	Code ASCII du caractère de retour chariot.
S4	0–127	Code ASCII du caractère de ligne suivante.
S5	0–32, 127	Code ASCII du caractère de retour arrière.
S6	2–255	Délai, en secondes, entre le décroché et la numérotation.
S7	1–55	Délai, en secondes, entre la tonalité de porteuse et de numérotation.
S8	0–255	Durée, en secondes, de la pause marquée par une virgule.
S9	1–255	Délai minimum de réponse de détection de porteuse (en dixièmes de seconde).
S10	1–255	Temps entre la perte de porteuse et le raccrochage (en dixièmes de seconde).

S11	50–255	Durée/intervalle des tonalités (en millisecondes).
S12	50–255	Temps de garde avant et après la séquence d'échappement (en deux–centièmes de seconde).
S13	—	Réservé.
S14	—	Réservé.
S15	—	Réservé.
S16	—	Réservé les fonctions de ce registre sont contrôlées par les commandes **&T**.
S17	—	Réservé.
S18	0–255	Durée du test du compteur (en secondes).
S19	—	Réservé.
S20	—	Réservé.
S21	—	Réservé.
S22	—	Réservé.
S23	—	Réservé.
S24	—	Réservé.
S25	0–255	Temps de détection de changement DTR (en centièmes de seconde).
S26	0–255	Délai entre une demande RTS et la réponse CTS (en centièmes de seconde).
S27	—	Réservé.

Récapitulatif des codes de résultat

Message numérique	Message littéral	Description
0	OK	Commande exécutée correctement.
1	CONNECT	Connexion établie à 0-300 bps.
2	RING	Détection d'une sonnerie.
3	NO CARRIER	Signal de porteuse perdu ou non détecté.
4	ERROR	Erreur de syntaxe dans la ligne de commande, ou commande, total de contrôle ou longueur invalide.
5	CONNECT 1200	Connexion établie à 1200 bps.
6	NO DIALTONE	Absence de tonalité d'invitation à numéroter.
7	BUSY	Détection d'une tonalité d'occupation.
8	NO ANSWER	Pas de réponse du système appelé.
9	CONNECT 2400	Connexion établie à 2400 bps.

Modificateurs de numérotation

Liste et description des modificateurs de numérotaion :

0–9 # * A–D	Chiffres et caractères de numérotation
P	Réglage de l'impulsion
T	Réglage de la tonalité
,	Pause pour traitement du caractère suivant
!	Signal d'accroche
@	Attente d'un silence
W	Attente de tonalité
;	Retour à l'état "commande" après numérotation
R	Mode inversé
S=*n*	Compose le numéro stocké à l'emplacement *n.*

Emulation ATE

L'émulation de terminal asynchrone ATE est un logiciel en option qui permet à un système d'émuler un terminal sur un système distant. ATE donne accès à la plupart des systèmes compatibles avec des terminaux asynchrones, y compris avec les connexions RS-232C ou RS-422A. Il est possible de configurer ATE de façon que le système distant perçoive votre terminal comme station de travail raccordée ou terminal DEC VT100.

Généralités sur la configuration d'ATE

Avant d'exécuter ATE, vous devez installer le logiciel et configurer les ports et connexions. ATE admet les connexions par câbles (directes) ou par modem. Les connexions RS-232C locales permettent de relier des machines distantes d'au maximum 15 mètres l'une de l'autre, les connexions RS-422A permettant d'aller jusqu'à 1 200 mètres.

Assurez-vous au préalable que l'unité tty à appeler (la vôtre ou celle du système distant) via ATE est prête à accepter l'appel.

Pour en savoir plus, reportezvous à la section "Configuration d'ATE", page 5-39.

Remarque : Vous ne pouvez utiliser ATE que si vous êtes membre d'un groupe UUCP (UNIX-to-UNIX Copy Program). Un superutilisateur (bénéficiant des droits d'accès root) peut utiliser Web-based System Manager ou définir ce type de groupe via SMIT.

Personnalisation d'ATE

Lors de la première exécution d'ATE, le programme crée un fichier **ate.def** par défaut dans le répertoire courant. Ce fichier regroupe les paramètres utilisés par ATE qui définissent :

- les caractéristiques de transmission de données,
- les fonctionnalités du système local,
- le fichier répertoire des numéros d'appel,
- les touches de contrôle.

Pour modifier ces paramètres, éditez le fichier **ate.def**.

Si vous souhaitez disposer de plusieurs configurations d'ATE, conservez les versions correspondantes du fichier **ate.def** dans des répertoires distincts. Il suffit alors d'exécuter ATE à partir du répertoire ad hoc. Bien entendu, cette solution, qui nécessite plusieurs exemplaires du fichier **ate.def**, mobilise davantage d'espace de stockage système.

Pour plus d'informations sur l'édition du fichier **ate.def**, reportez-vous à la section "Edition du fichier par défaut d'ATE" dans le manuel *AIX 4.3 Guide de l'utilisateur : communications et réseaux*.

Pour changer temporairement la configuration sans modifier le fichier par défaut, vous disposez des sous-commandes **alter** et **modify**. Les modifications apportées par ce biais sont annulées dès que vous quittez le programme avec **quit**, et les valeurs du fichier **ate.def** sont de nouveau appliquées.

Une fois installé, ATE sollicite le fichier répertoire de numéros d'appel **/usr/lib/dir** du système. Vous pouvez le modifier temporairement - pour la durée de la connexion par modem : vous retrouvez alors les valeurs initiales dès la fin de la connexion et non à la sortie d'ATE. Un utilisateur racine peut ajouter dans le fichier **/usr/lib/dir** les numéros d'appel des modems utilisés par tous les utilisateurs. Chaque utilisateur a également la possibilité de créer ses propres fichiers répertoires et de modifier ses exemplaires du fichier **ate.def** pour permettre à ATE d'accéder à ces répertoires.

Pour en savoir plus sur l'utilisation d'ATE avec un répertoire de numéros d'appel personnalisé, reportez-vous à "Création d'un répertoire de numéros d'appel ATE" dans le manuel *AIX 4.3 Guide de l'utilisateur : communications et réseaux*.

Vous pouvez inclure dans le fichier répertoire les numéros d'appel fréquemment utilisés et modifier le débit, la longueur des données, les bits d'arrêt, la parité, l'écho et le retour de ligne d'un numéro d'appel. Pour établir la connexion avec un numéro non répertorié, lancez la sous-commande **connect**.

Remarque : Un fichier répertoire peut contenir jusqu'à 20 lignes (chacune correspondant à une entrée). Au-delà, les lignes sont ignorées par ATE.

Modification des caractéristiques ATE

Les caractéristiques d'ATE répertoriées ci-dessous peuvent être modifiées par l'utilisateur via la méthode indiquée.

Remarque : Toutes les caractéristiques d'ATE sont modifiables dans le fichier **ate.def**.

Modification des caractéristiques ATE	
Caractéristique	**Via**
Touches de contrôle	Fichier **ate.def**
Longueur des données	**alter** ou entrée répertoire des numéros
Nom du répertoire de numéros d'appel	**directory**
Echo (activé ou non)	**modify** ou entrée répertoire des numéros
Nom du fichier de capture	**modify**
Suffixe de numérotation pour modem	**alter**
Préfixe de numérotation pour modem	**alter**
Retours de ligne	**modify** ou entrée répertoire des numéros
Nombre de tentatives de numérotation	**alter**
Nombre de bits d'arrêt	**alter** ou entrée répertoire des numéros
Parité (paire ou impaire)	**alter** ou entrée répertoire des numéros
Numéro de port (unité)	**alter**
Débit (bits/s)	**alter** ou entrée répertoire des numéros
Numéro de téléphone	entrée répertoire des numéros
Protocole de transfert (pacing ou xmodem)	**alter**
Espacement (caractère ou intervalle)	**alter**
Emulation VT100 (activée ou non)	**modify**
Délai entre deux tentatives de numérotation	**alter**
Capture des données entrantes	**modify**
Protocole Xon/Xoff (activé ou non)	**modify**

Configuration d'ATE

Cette section traite de la configuration d'ATE (Asynchronous Terminal Emulation)

Prérequis

- Le programme en option ATE (Asynchronous Terminal Emulation) doit être installé sur le système.
- Vous devez être utilisateur racine pour configurer le port de l'unité de communications.

Procédure

Effectuez les opérations suivantes :

1. Installez une carte asynchrone dans l'unité centrale si le système n'est pas équipé d'un port série intégré.
2. Branchez le câble RS–232C ou RS–422A sur la carte ou le port série intégré.
3. Déclarez une unité tty pour le port de communication. Pour ce faire, utilisez le raccourci Web-based System Manager, les **unités wsm** ou entrez :

   ```
   smit mktty
   ```

4. Sélectionnez Ajout d'un TTY.
5. Sélectionnez le type tty.
6. Sélectionnez l'unité de carte parent
7. Sélectionnez un port.
8. Désactivez l'option Activation de la CONNEXION.
9. Définissez Type de terminal sur **HFT** ou **dumb**.
10. Modifiez l'environnement en conséquence, notamment la vitesse de ligne, la parité, le nombre de bits par caractère et le mode de pilotage de la ligne (local ou distant). Indiquez `BPC 8` et `no parity` si le support de langue NLS est requis.
11. Configurez le port de l'unité.
    - Pour permettre des appels sortants via ATE, utilisez la commande **pdisable**. Par exemple, si le port est `tty1`, entrez :

      ```
      pdisable tty1
      ```

    - Pour permettre des appels entrants via ATE, utilisez la commande **penable**. Par exemple, si le port à appeler est `tty2`, entrez :

      ```
      penable tty2
      ```

12. Vérifiez que l'unité a été préalablement déclarée au système distant, puis modifiez ATE de façon à tenir compte de la configuration de l'unité : utilisez les sous-commandes **alter** et **modify**, ou éditez le fichier **ate.def** par défaut. Pour une modification temporaire limitée à une connexion téléphonique, modifiez une entrée du fichier répertoire des numéros d'appel.

Identification des incidents TTY

Cette section traite des points suivants :

- Régénération trop rapide
- Informations journalisées et identificateurs de journal tty

Incident : TTY : Régénération trop rapide

Le système enregistre le nombre de process getty générés pour un tty particulier dans un court laps de temps. Si ce nombre est supérieur à 5, l'erreur `Redémarrage trop rapide de la commande` s'affiche sur la console et le port est désactivé par le système.

Le tty reste désactivé environ 19 minutes ou jusqu'à ce que l'administrateur système le réactive. Au bout de ces 19 minutes, le système réactive automatiquement le port, générant un nouveau process getty.

Causes possibles

- La configuration du modem est incorrecte.
- Un port est défini et activé, mais aucune unité ou aucun câble ne lui est raccordé.
- Le câblage est mauvais ou la connexion desserrée.
- Il y a des bruits parasites sur la ligne de communication.
- Les fichiers **/etc/environment** ou **/etc/inittab** sont altérés.
- La configuration de tty est erronée.
- Le matériel est défectueux.

Procédures de reprise

- Rectifiez la configuration du modem :

  Vérifiez que le signal de détection de porteuse défini pour le modem *n'est* pas forcé à un niveau élevé.

  Remarque : Les instructions ci-dessous concernent les modems compatibles Hayes.

  a. Connectez le modem et examinez le profil actif.

  b. Le signal de détection de porteuse doit être positionné à **&C1** et non **&C0** (forcé à un niveau élevé). Utilisez les commandes AT ci-après pour définir ou modifier cet attribut :

  ```
  AT&C1
  AT&W
  ```

  Remarques :

  a. Reportez-vous à la section "Envoi de commandes AT (cu)", page 5-15.

  b. Reportez-vous à la documentation du modem.

- Désactivez le tty, supprimez sa définition ou raccordez une unité au port :

  – Pour désactiver la définition tty, entrez :

  ```
  chdev l nomtty –a Login=disable
  ```

  Le tty *ne sera pas* réactivé au prochain démarrage du système.

  – Pour supprimer la définition tty :

  a. Désactivez le port tty via la commande **pdisable** comme suit :

  ```
  pdisable nomtty
  ```

b. Supprimez la définition tty du système. Pour plus d'informations, reportez-vous à la section "Gestion des unités TTY", page 5-4.

- Vérifiez les câbles et les connexions :
  a. Vérifiez les câbles. Resserrez les connexions et remplacez les connecteurs endommagés ou inadéquats.
  b. Vérifiez que le câblage vraisemblablement à l'origine de la défaillance ou que les câbles répondent à la même norme. Remplacez les câbles endommagés ou inappropriés.
- Eliminez les bruits parasites sur la ligne :
  a. Vérifiez la longueur et l'impédance des câbles.
  b. Vérifiez que les bagues de serrage requises sur les câbles longs sont en place.
  c. Contrôlez le parcours des câbles, ils doivent être éloignés des lumières fluorescentes et des générateurs.
- Assurez-vous que les fichiers **/etc/environment** ou **/etc/inittab** ne sont pas altérés :
  a. Si possible, comparez ces fichiers à des copies fiables.
  b. Faites une sauvegarde de ces fichiers et modifiez-les.
  c. Dans le fichier **/etc/environment**, supprimez les lignes autres que :
     – les lignes blanches,
     – les lignes de commentaire
     – *variable*=*valeur*
  d. Vérifiez dans le fichier **/etc/inittab** les lignes relatives aux unités tty. Si le tty est positionné sur `off`, le port tty n'est sans doute pas utilisé. Supprimez sa définition ou raccordez une unité au port.
- Supprimez les éléments de configuration de tty erronés :
  a. Supprimez la définition tty. Utilisez l'application Web-based System Manager Devices ou reportez-vous à la section "Gestion des unités TTY", page 5-4.
  b. Pour effectuer une copie papier de cette définition avant de la supprimer, appuyez sur F8 ou sur Esc+8 (Image) : une capture de l'écran courant est réalisée et copiée dans le fichier **smit.log** de votre répertoire **$HOME**.

13. Examinez la définition de tty. Consultez les instructions sur l'ajout d'un TTY à la section "Gestion des unités TTY", page 5-4.

- Localisez le matériel défectueux :
  a. Exécutez les programmes de diagnostic à l'aide de la commande **diag**.
  b. Si vous décelez la moindre anomalie matérielle, suivez les procédures de résolution des incidents locaux.

Informations journalisées et identificateurs de journal TTY

Cette section présente les principaux fichiers et commandes de journalisation des erreurs ainsi que les messages d'erreur courants concernant les unités tty.

Fichiers et commandes de journalisation des erreurs

Commande **errclear**

Cette commande supprime les entrées du journal d'erreur. Vous pouvez supprimer soit la totalité du journal avec la commande `errclear 0`, soit certaines entrées seulement en spécifiant des ID, une classe ou un type de messages.

Commande **errpt**

Cette commande génère un compte rendu d'erreurs à partir des entrées du journal d'erreur du système. Le format `errpt -a | pg`, le plus utilisé, demande la génération d'un compte rendu détaillé avec, en tête, les erreurs les plus courantes.

Fichier **/var/adm/ras/errlog**

Ce fichier stocke les occurrences d'erreurs et de défaillances détectées par le système. S'il n'est pas régulièrement purgé, le fichier **errlog** peut mobiliser un espace disque important. Utilisez la commande **errclear** citée plus haut pour le purger.

Fichier **/usr/include/sys/errids.h**

Le fichier d'en-tête **errids.h** fait la corrélation entre les ID d'erreur et leurs étiquettes.

Messages d'erreurs

Message	Description	Commentaire
Core Dump	Arrêt anormal du programme	Arrêt anormal d'un programme entraînant un vidage de la mémoire : l'utilisateur n'a pas quitté proprement les applications, le système s'est arrêté en cours d'application, ou le terminal de l'utilisateur s'est bloqué et a interrompu l'application.
Errlog On	Activation du démon Err	Message consigné par le démon Err dès le lancement de la journalisation. Le système désactive automatiquement la journalisation lors de l'arrêt du système (shutdown).
Lion Box Died	Perte de communication avec concentrateur 64 ports	Message consigné par le pilote du concentrateur 64 ports. Vérifiez l'horodateur pour déterminer si un utilisateur est à l'origine de ce message. Une série de messages de ce type peut révéler une défaillance de la carte 64 ports ou du matériel associé.
Lion Buffero	Saturation du tampon : Concentrateur 64 ports	Le tampon matériel du concentrateur 64 ports est saturé. Si l'unité et le câblage le permettent, ajoutez une demande (RTS) au port et à l'unité et, si possible, réduisez le débit en bauds.
Lion Chunknumc	Décompte erroné dans une tranche de mémoire : contrôleur 64 ports	Le nombre de caractères compris dans une tranche de mémoire ne concorde pas avec les valeurs effectivement en mémoire tampon. Cette erreur peut signaler un incident matériel ; exécutez les diagnostics sur les unités.
Lion Hrdwre	Mémoire du contrôleur 64 ports inaccessible	Message consigné par le pilote du concentrateur 64 ports lorsqu'il ne parvient pas à accéder à la mémoire du contrôleur.
Lion Mem ADAP	Allocation de mémoire impossible : structure ADAP	Message consigné par le pilote du concentrateur 64 ports si la routine **malloc** pour la structure adap échoue.

Lion Mem List	Allocation de mémoire impossible : liste TTYP_T	Message consigné par le pilote du concentrateur 64 ports si la routine **malloc** pour la structure *ttyp_t* échoue.
Lion Pin ADAP	Echec de la routine pin : structure ADAP	Message consigné par le pilote du concentrateur 64 ports si la routine **pin** pour la structure adap échoue.
SRC	Erreur du programme	Message consigné par le démon SRC (System Resource Controller) en cas de défaillance des sous-systèmes, des communications ou d'autres éléments.
Lion Unkchunk	Code d'erreur inconnu issu du concentrateur 64 ports	Code d'erreur : nombre de caractère reçus dans la tranche de mémoire.
TTY Badinput	Retour ttyinput anormal	Code d'erreur : (voir **sys/errno.h**). Consigné par le pilote du tty si la routine **ttyinput** renvoie une erreur.
TTY Overrun	Surcharge en entrée côté récepteur	L'unité émettrice ignore le contrôle de flux et surcharge le tampon matériel de la carte. Survient après que le pilote ait accédé au FIFO matériel. Ajoutez une demande `rts` au port et à l'unité (si possible).
TTY TTYHOG	Saturation de TTYHOG	L'unité émettrice ignore le contrôle de flux. Survient après l'accès au FIFO matériel qui a inscrit des données dans le tampon logiciel. En d'autres termes, l'erreur ttyhog est consignée car le tampon d'entrée est saturé. Lorsque le tampon est aux 3/4 occupé, le pilote d'unité demande au matériel (ici, tty) d'envoyer à l'expéditeur le caractère XOFF pour arrêter l'envoi de données. Si des données continuent d'être envoyées sans que le tampon soit vidé, le pilote purge le tampon et consigne ce message d'erreur.
TTY Parerr	Erreur de parité/encadrement en entrée	Erreurs de parité sur les données entrantes au niveau des ports asynchrones, en mode caractère par caractère.
TTY Prog PTR	Erreur logicielle : champ T_HPTR invalide	Message consigné par le pilote tty si le pointeur *t_hptr* est nul.

Chapitre 6. Cartes Micro Channel, ISA et PCI

Ce chapitre traite de l'installation et de la configuration des cartes Micro Channel, ISA et PCI. Les différentes rubriques concernent la prise en charge et la configuration des :

- cartes Micro Channel (Multiport/2, page 6-2 et Portmaster, page 6-2)
- cartes ISA (Multiport Model 2, page 6-4)
- cartes ISA/PCI pour réseaux longue distance WAN (Multiport/2 (ISA), page 6-4, Multiprotocole 2 ports (PCI), page 6-8 et ARTIC960HX(PCI)).

Remarque : Toutes les cartes ne sont pas présentées dans ce chapitre. Veuillez vous reporter à la documentation fournie avec le système ou avec les cartes commandées séparément.

Cartes Micro Channel pour réseaux longue distance

Cette section présente la configuration requise pour les cartes Micro Channel ci-dessous :

Ce paragraphe décrit plus précisément :

Cartes Multiport/2

Cartes Multiport/2 pour Realtime Interface Co-Processor :

- Carte Multiport/2 EIA-232D 4 ports
- Carte Multiport/2 EIA-232D / EIA-422A 4 ports
- Carte Multiport/2 EIA-232D 8 ports
- Carte Multiport/2 EIA-422A 8 ports
- Carte synchrone Multiport/2 EIA-232D 6 ports

Cartes Portmaster

Appelées ici et dans SMIT sous la forme générique Web-based System Manager *Carte Portmaster/A* :

- Contrôleur de communication multiprotocole 4 ports
- Cartes Portmaster pour Realtime Interface Co-Processor :
  - Carte Portmaster/A EIA-232D 8 ports
  - Carte Portmaster/A EIA-422A 8 ports
  - Carte Portmaster/A V.35 6 ports
  - Carte Portmaster/A X.21 6 ports

Pilote d'unité

Le pilote d'unité de communication multiprotocole 4 ports est livré avec le système d'exploitation.

L'utilisation d'une carte Multiport/2 ou Portmaster pour le programme Realtime Interface Co-Processor requiert un logiciel supplémentaire pour la configuration du pilote d'unité. Vous devez disposer d'un des éléments suivants :

- Programme sous licence Realtime Interface Co-Processor

  OU

- Pilote d'unité fourni par un partenaire commercial ou écrit par un client

Procédure de configuration

La procédure ci-dessous indique comment configurer les pilotes d'unité et les ports pour un contrôleur (carte) de communication Multiport/2 ou Portmaster.

Prérequis

Le contrôleur (carte) de communication doit être installé.

Procédure de configuration	
Raccourci Web-based System Manager, (application wsm network) OU	**wsm network**
Tâche	*Raccourci SMIT*
Ajout d'un pilote d'unité	**smit commodev**[1,2]
Ajout de ports	**smit commodev**, sélectionnez une carte, **Gestion des ports**, puis **Ajout d'un port multiprotocole**
Reconfiguration des ports	**smit commodev**, sélectionnez une carte, **Gestion des ports**, puis **Modif / affich caractéristiques port multiprotocole**
Retrait d'un port	**smit commodev**, sélectionnez une carte, **Gestion des ports**, puis **Retrait d'un port**
Déclaration d'un port disponible	**smit commodev**, sélectionnez une carte, **Gestion des ports**, puis **Configuration d'un port défini**
Passage d'un pilote défini à l'état disponible	**smit commodev**, sélectionnez une carte, **Gestion des ports**, puis **Configuration d'un pilote de périphérique défini**
Retrait d'un pilote d'unité	**smit commodev**, sélectionnez une carte, **Gestion des ports**, puis **Retrait d'un pilote d'unité**

Remarques :

1. Ce menu varie en fonction du logiciel installé. Les pilotes de contrôleur de communication multiprotocole 4 ports sont compris dans le système d'exploitation de base. Pour pouvoir utiliser un autre type de carte Multiport/2 ou Portmaster/2, vous devez installer le programme sous licence Realtime Interface Co-Processor ou un pilote d'unité fourni par un partenaire commercial ou écrit par un client.
2. Si vous utilisez un autre pilote d'unité que le pilote de contrôleur multiprotocole 4 ports, reportez-vous à la documentation spécifique du pilote utilisé.

Cartes ISA/PCI pour réseaux longue distance

Cette section traite de l'installation et de la configuration des cartes Multiport/2 (ISA), Multiprotocole 2 ports (PCI) et ARTIC960HX PCI.

Cartes Multiport/2

Le pilote d'unité de la carte Multiport/2 (MM2) est un élément du sous-système d'E/S de communication. Ce pilote assure la prise en charge des opérations SDLC à travers la carte Multiport/2 à la vitesse maximale de 64 kbps. La synchronisation incombe aux modems, car seule une synchronisation externe est prise en charge.

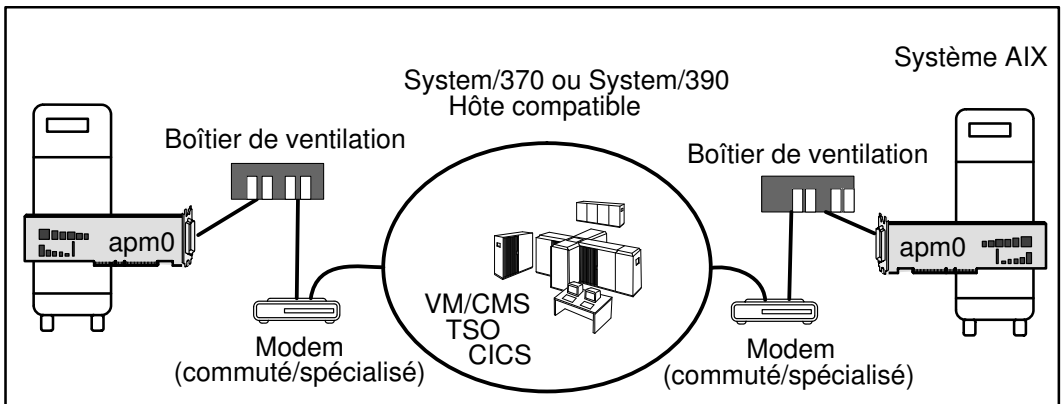
Les options donnant accès au pilote d'unité Multiport/2 sont les suivantes :

- Architecture SNA (Systems Network Architecture)
- Interface de programmation générique GDLC (Generic Data Link Control)
- Applications utilisateur compatibles avec l'API (Application Programming Interface) MPQP (Multiprotocol Quad Port).

es options requièrent l'utilisation du fichier spécial **mpq***i*, qui donne accès à la carte Multiport/2 via le pilote d'unité SDLC Multiport/2. Le fichier **mpq***i* réside dans le répertoire /**dev**.

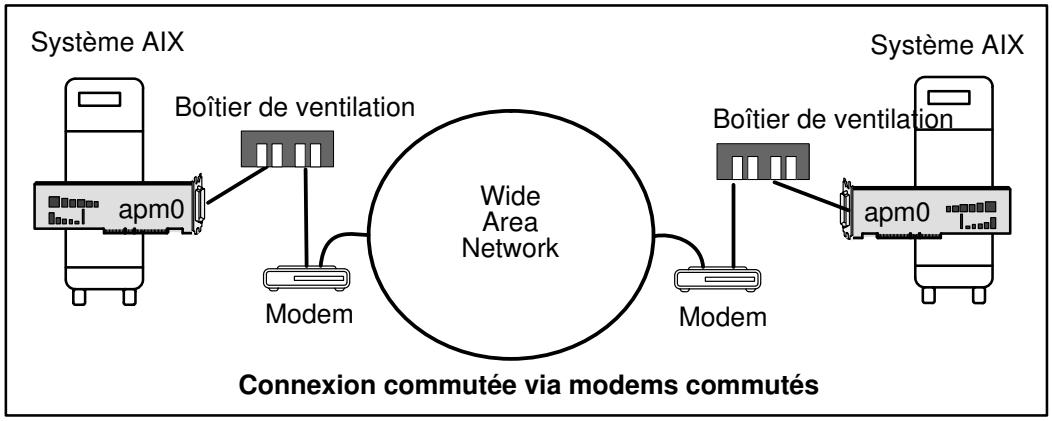
Remarque : *i* in **mpq***i* spécifie l'instance du pilote d'unité, `mpq0`, par exemple.

Le pilote d'unité SDLC Multiport/2 permet la connexion à des systèmes hôtes distants via la carte Multiport/2, soit directement par le biais d'une ligne spécialisée, soit par le biais de circuits commutés, comme illustré à la figure suivante. Le pilote d'unité peut fournir une passerelle entre les environnements de groupe de travail (work group) et les fonctions informatiques à distance.

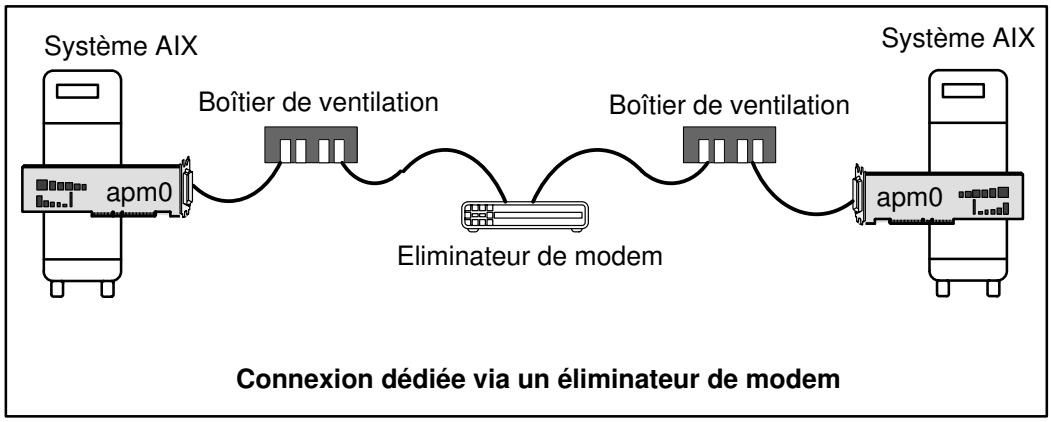


Connexions hôte sur circuits commutés

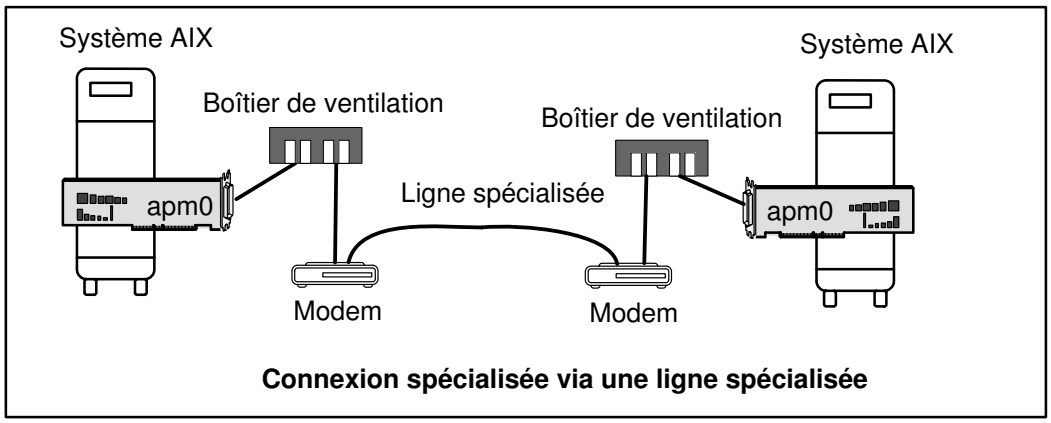
Une connexion directe à un système AIX avec carte Multiport/2 est possible via : un réseau longue distance (WAN) à l'aide de modems commutés (voir figure), un éliminateur de modem, ou des lignes spécialisées (voir figures).



Connexion commutée via modems commutés



Connexion dédiée via un éliminateur de modem



Connexion spécialisée via une ligne spécialisée

Configuration de la carte Multiport/2

Voici les procédures de configuration de la carte Multiport/2.

Configuration de la carte Multiport/2		
Raccourci Web-based System Manager, (application wsm network) OU	**wsm network**	
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Ajout d'une carte Multiport/2[1]	**smit makmm2**	**mkdev**[2]
Liste des cartes Multiport/2	**smit lsmm2**	**lsdev**[2]
Affichage/modification d'une carte Multiport/2	**smit chgmm2**	**chdev**[2]

Configuration de la carte Multiport/2		
Configuration d'une carte Multiport/2 définie	**smit cfgmm2**	**mkdev**[2]
Gestion des pilotes d'unité pour cartes Multiport/2	**smit mm2isa_dd**	
Génération d'un compte rendu d'erreur	**smit errpt**	
Suivi d'une carte Multiport/2	**smit mm2trace**	
Retrait d'une carte Multiport/2	**smit rmvmm2**	**rmdev**[2]
Gestion des services DLC	**smit mpaserv**	
Ajout d'applications utilisateur	**smit mm2apps**	

Remarques :

1. Pour plus d'informations sur l'ajout de ports, reportez-vous à la section "Configuration des cartes Multiport/2 et Portmaster", page 6-2
2. Pour plus d'informations sur les options de ligne de commande, consultez les descriptions des commandes **mkdev**, **lsdev**, **chdev** ou **rmdev** dans *AIX Commands Reference*.

Objets et attributs de la carte Multiport/2

Voici quelques informations sur les classes d'objets et les attributs de la carte Multiport/2.

Objet Predefined Device

La classe d'objets **Predefined Devices (PdDv)** contient des entrées pour tous les types d'unité pris en charge par le système. Ces informations sont modifiées exclusivement lors de l'ajout d'une nouvelle unité. Le tableau qui suit concerne la carte Multiport/2.

Device type:	portmaster
Device class:	adapter
Device subclass:	isa
Unique Type:	/adapter/isa/portmaster
Prefix name:	apm

Indicateur	**Valeur**
Base Device	no
Vital Product Data (VPD)	no
Detectable	yes
Change Status	NEW, lors de la définition d'une unité
Bus Extender	no
Field Replaceable Unit (FRU)	yes

Objet Predefined Connection

La classe d'objets **Predefined Connection (PdCn)** contient des informations sur les connexions et les dépendances des unités. Le tableau qui suit concerne la carte Multiport/2.

Connection Location:	0
Unique Type:	/adapter/isa/portmaster
Connection Key:	portmaster

Objet Predefined Attribute

La classe d'objets **Predefined Attribute (PdAt)** contient une entrée pour chaque attribut existant pour une unité, au delà de ce qui est défini dans la classe d'objets **Predefined Device.** Le tableau qui suit concerne la carte Multiport/2.

Attribut	Description	Valeurs possibles
bus_intr_lvl	ISA Interrupt Level	`3,4,7,9,10,11,12`
bus_io_addr	Bus IO Address	`0x2A0-0x3EA0 , 0x400 (pour l'ignorer)`
bus_mem_addr	Bus Memory Address	`0xC0000-0xDE0000 , 0x200 (pour l'ignorer)`
window_size	Window Size	`0x2000` (non modifiable)
intr_priority	Interrupt Priority	`2` (non modifiable)

Sous-types :

- Carte Multiport/2 sélectable 4 ports
- Carte Multiport/2
- Carte Multiport/2 6 ports (V.35)
- Carte Multiport/2 6 ports (X.21)
- Carte Multiport/2 8 ports (RS-232)
- Carte Multiport/2 8 ports (RS-422)

Remarque : A l'heure actuelle, seule la carte Multiport/2 sélectable 4 ports est prise en charge.

Carte Multiport/2-Gestion PM (Power Management)

Le pilote de la carte Multiport/2 prend en charge le support PM (Power Management). PM est une technique qui permet de minimiser la consommation électrique, tant sur le plan logiciel que matériel. PM n'est généralement important que pour les modèles d'entrée de gamme, tels qu'ordinateurs portables et systèmes sur batterie.

Lorsque Power Management est activé, le système passe en mode économie d'énergie dans les cas suivants :

- Expiration du délai d'inactivité
- Commande directe de l'utilisateur
- Batterie presque à plat
- Fermeture du couvercle de l'ordinateur portable

Les différents états de PM sont :

- **enable**
- **standby**
- **suspend**
- **hibernation**
- **shutdown**

A chaque état correspond une baisse de plus en plus sensible de l'alimentation électrique des différents éléments du système.

Pour en savoir plus sur PM, sa configuration et ses fonctions, reportez-vous à la section "Using Power Management" dans *AIX 4.3 Guide d'administration : système d'exploitation et unités*.

Impact sur les connexions externes - Accès au réseau

Amener un système à l'état **suspend**, **hibernation** ou **shutdown** entraîne la perte de l'alimentation des cartes : toutes les connexions réseau sont perdues. C'est comme si une connexion physique (câble) était débranchée : le résultat est le même, à savoir une perte du signal au niveau de la couche physique. Une erreur DSR (data set ready) est générée. Toute application pour laquelle le pilote d'unité SDLC est ouvert doit être arrêtée avant suspension, hibernation ou arrêt complet du système.

Une fois l'alimentation rétablie, tous les ports précédemment configurés sont restaurés à l'état **available**. Toutes les applications utilisant précédemment ces connexions peuvent alors être relancées.

Pilote d'unité multiprotocole HDLC 2 ports

Le pilote de carte multiprotocole HDLC (High Level Data Link Control) 2 ports est un composant du sous-système d'E/S de communication. Ce pilote d'unité prend en charge les opérations HDLC sur la carte multiprotocole 2 ports, à la vitesse de 64 Kbps au maximum.

Les options ci-dessous permettent l'accès au pilote de carte multiprotocole HDLC 2 ports :

- Architecture SNA (Systems Network Architecture)
- Version SDLC (synchronous data link control) de l'interface de programmation GDLC
- Applications utilisateur compatibles avec l'API (Application Programming Interface) SDLC MPQP (Multiprotocol Quad Port).

Remarque : Ces options requièrent l'utilisation du fichier spécial **mpq***n*, qui donne accès à la carte multiprotocole 2 ports via le sous-système d'émulation de pilote d'unité SDLC COMIO. Ce sous-système doit être installé et configuré pour chaque unité HDLC du réseau.

- Applications utilisateur compatibles avec l'API HDLC CDLI

Configuration de la carte Multiprotocole 2 ports

Le tableau ci-dessous expliquent comment configurer la carte Multiprotocole 2 ports.

Configuration de la carte Multiprotocole 2 ports	
Raccourci Web-based System Manager, (application wsm network) OU	**wsm network**
Tâche	*Raccourci SMIT*
Ajout d'un pilote d'unité	**smit mkhdlcdpmpdd**
Reconfiguration du pilote d'unité	**smit chhdlcdpmpdd**
Retrait d'un pilote d'unité	**smit rmhdlcdpmpdd**
Déclaration d'un pilote d'unité disponible	**smit cfghdlcdpmpdd**
Retrait d'un émulateur SDLC COMIO	**smit mksdlcsciedd**
Reconfiguration de l'émulateur SDLC COMIO	**smit chsdlcsciedd**

Configuration de la carte Multiprotocole 2 ports	
Retrait d'un émulateur SDLC COMIO	**smit rmsdlcsciedd**
Passage d'un émulateur SDLC COMIO défini à l'état disponible	**smit cfgsdlcsciedd**

Présentation de la carte ARTIC960HX PCI

Le pilote d'unité MPQP COMIO de la carte ARTIC960HX PCI est un élément du sous–système d'E/S de communication. Ce pilote assure la prise en charge de la carte ARTIC960HX PCI à la vitesse maximale de 2 Mbps. La synchronisation incombe aux modems, car seule une synchronisation externe est prise en charge.

Les options donnant accès au pilote d'unité Multiport/2 sont les suivantes :

- Architecture SNA (Systems Network Architecture)
- Interface de programmation générique GDLC (Generic Data Link Control)
- Applications utilisateur compatibles avec l'API (Application Programming Interface) MPQP (Multiprotocol Quad Port), par exemple les applications bisynchrones.

Ces options requièrent l'utilisation du fichier spécial **mpq***x*, qui donne accès à la carte ARTIC960HX PCI via le pilote d'unité d'émulation MPQP COMIO. Ce pilote d'unité doit être installé et configuré pour chaque port de la carte ARTIC960HX PCI. Le fichier **mpq***x* réside dans le répertoire /**dev**.

Remarque : *x* dans **mpq***x* spécifie l'instance du pilote d'unité, `mpq0`, par exemple.

Le pilote d'unité d'émulation MPQP COMIO permet de connecter des systèmes hôtes distants par le biais d'une carte ARTIC960HX PCI, soit directement, soit par l'intermédiaire d'une ligne spécialisée. Le pilote d'unité peut fournir une passerelle entre les environnements de groupe de travail (work group) et les fonctions informatiques à distance.

Configuration du pilote d'émulation MPQP COMIO sur la carte ARTIC960HX PCI

Le tableau suivant explique comment configurer le pilote d'émulation MPQP COMIO sur la carte ARTIC960HX PCI.

Configuration des tâches du pilote d'émulation MPQP COMIO	
Raccourci Web-based System Manager, (application wsm network) OU	**wsm network**
Tâche	*Raccourci SMIT*
Ajout d'un pilote d'unité	**smit mktsdd**
Reconfiguration du pilote d'émulation MPQP COMIO	**smit chtsdd**
Suppression d'un pilote d'unité	**smit rmtsdd**
Configuration d'un pilote d'unité défini	**smit cfgtsdd**
Ajout d'un port	**smit mktsdports**
Reconfiguration d'un port d'émulation MPQP COMIO	**smit chtsdports**
Suppression d'un port	**smit rmtsdports**
Configuration d'un port défini	**smit cfgtsdports**
Suivi d'un pilote d'émulation MPQP COMIO	**smit trace_link**

Chapitre 7. Protocole DLC

GDLC (Generic Data Link Control) est la définition d'une interface générique qui fournit aux utilisateurs niveau noyau et application, un jeu de commandes pour contrôler les gestionnaires d'unité DLC (Data Link Control) au sein du système d'exploitation. Cette section traite des points suivants :

Environnement GDLC – généralités

GDLC (Generic Data Link Control) est la définition d'une interface générique qui fournit aux utilisateurs niveau noyau et application, un jeu de commandes pour contrôler les gestionnaires d'unité DLC (Data Link Control) au sein du système d'exploitation.

Pour en savoir plus sur l'environnement GDLC, reportez-vous à :

- Mise en oeuvre de l'interface GDLC, page 7-5
- Installation de DLC, page 7-6
- Opérations ioctl sur l'interface GDLC, page 7-7
- Services spéciaux du noyau, page 7-10
- Identification des incidents GDLC, page 7-12

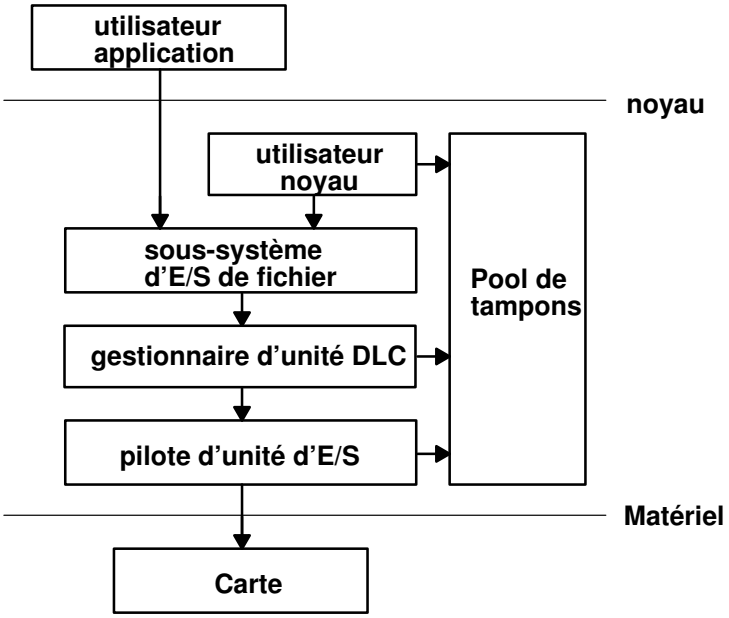
L'interface GDLC indique les contraintes de définition des points d'entrée, les fonctions fournies et les structures de données pour tous les gestionnaires d'unité DLC. On trouve parmi les normes DLC conformes à l'interface GDLC :

- 8023 (IEEE 802.3 pour Ethernet)
- ETHER (Ethernet standard)
- SDLC (Synchronous Data Link Control)
- TOKEN (anneau à jeton)
- FDDI (Fiber Distributed Data Interface)

Pour des performances optimales, les gestionnaires d'unité DLC sont implantés dans le noyau, mais ils appliquent des protocoles de la couche haute et des fonctions de portée plus étendue que celle d'un gestionnaire d'unité du noyau. Pour leurs requêtes d'E/S vers la carte, ils utilisent un gestionnaire d'unité du noyau. Quant aux utilisateurs DLC, ils se trouvent au sein ou au-dessus du noyau.

SDLC (Synchronous data link control) et IEEE 802.2 DLC sont des exemples de gestionnaires d'unité DLC. Chaque gestionnaire d'unité DLC fonctionne avec un pilote d'unité ou un groupe de pilotes d'unité spécifiques. Par exemple, SDLC fait fonctionner le pilote d'unité multiprotocole pour le produit du système et la carte associée.

La structure de base d'un environnement DLC est illustrée à la figure ci-dessous.
Les utilisateurs du noyau ont accès aux tampons de communications et appellent les points d'entrée add par les services du noyau **fp**. Les utilisateurs au dessus du noyau (niveau application) accèdent aux pilotes standard interface/noyau : le système de fichiers appelle les points d'entrée **dd**. Les données sont transférées de l'utilisateur à l'espace noyau.



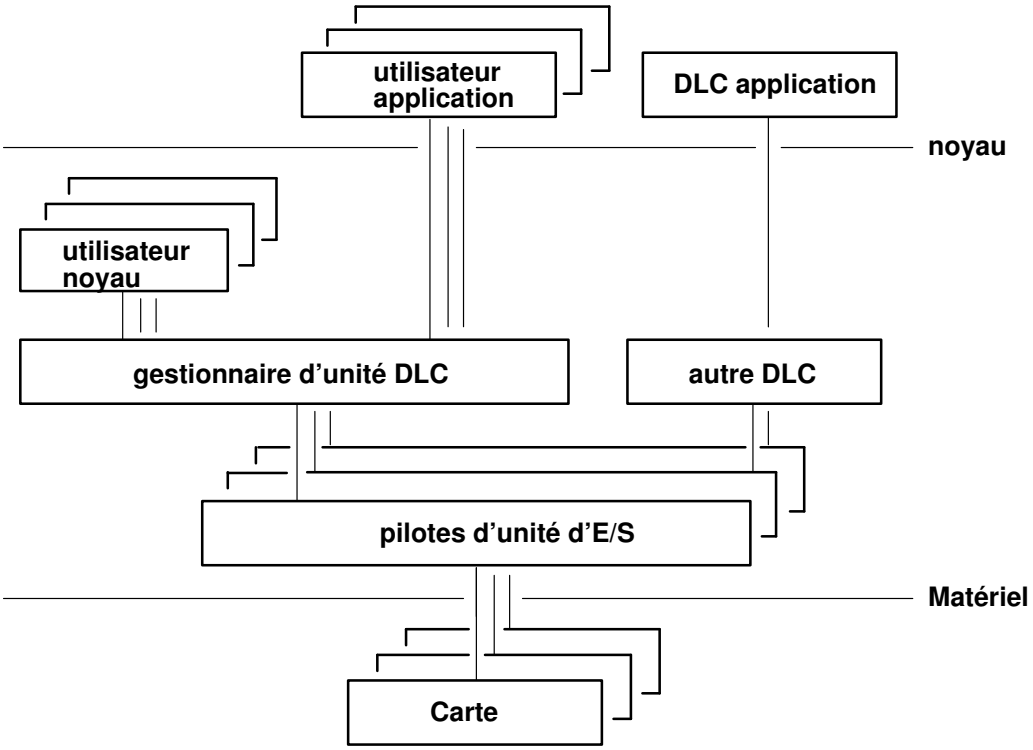
Environnement du gestionnaire d'unité DLC

Composants de l'environnement du gestionnaire d'unité DLC :

Utilisateur application	Réside au-dessus du noyau comme application ou méthode d'accès.
Utilisateur noyau	Réside dans le noyau comme process noyau ou gestionnaire d'unité.
Sous-système d'E/S de fichier	Dirige les routines de descripteur et de pointeur de fichiers vers les accès de pointeur de fichier de la table de localisation.
Pool de tampons	Fournit les services des tampons de données aux sous-systèmes de communication.
Pilote d'unité d'E/S	Contrôle les registres DMA et d'E/S de carte et achemine les paquets vers les différents DLC.
Carte	Se raccorde au support de communication.

Un gestionnaire d'unité conforme aux spécifications GDLC est compatible avec toute configuration matérielle du système d'exploitation comportant un pilote d'unité de communication et sa carte cible. Chaque gestionnaire d'unité peut prendre en charge plusieurs utilisateurs au-dessus, et plusieurs cartes et pilotes d'unité au-dessous.
En général, les utilisateurs travaillent simultanément sur une seule carte, ou individuellement sur plusieurs cartes. Les gestionnaires d'unité DLC varient en fonction de leurs contraintes de protocoles.

La figure ci-dessous illustre une configuration multi-utilisateur :



Configuration à utilisateurs et cartes multiples

Critères GDLC

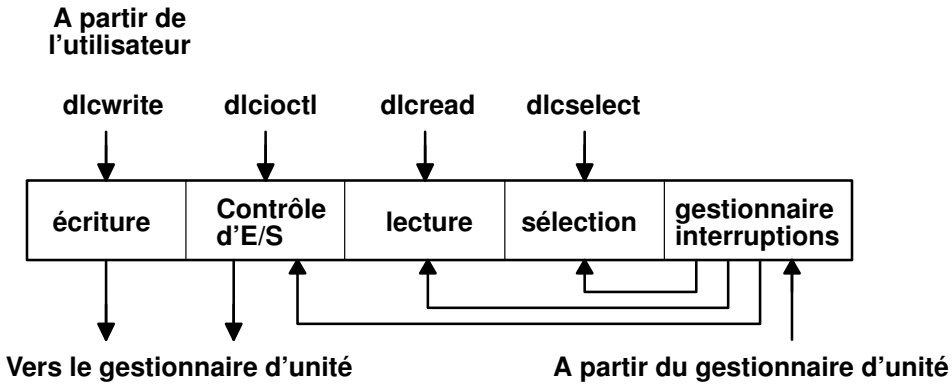
Une interface GDLC doit présenter les caractéristiques suivantes :

- souplesse et accessibilité aux utilisateurs niveau noyau et application,
- fonctions multi–utilisateurs et multicartes pour permettre aux protocoles d'exploiter les ports et sessions multiples,
- support des gestionnaires d'unité DLC orientés connexion et sans connexion,
- transfert des données transparent, dans le cas de contraintes spéciales dépassant la portée du gestionnaire d'unité DLC utilisé.

Mise en oeuvre de l’interface GDLC

Chaque gestionnaire d’unité DLC correspond à une entrée /**dev** standard qui fonctionne au niveau du noyau comme un gestionnaire de multiplexeur pour un protocole spécifique. Chaque sous-routine **open** soumise à un gestionnaire d’unité DLC pour une carte non utilisée par DLC créé un process noyau. Une sous-routine **open** est également transmise au gestionnaire d’unité de la carte cible. Au besoin, émettez des sous-routines **open** supplémentaires pour les divers ports de carte DLC du même protocole. Celles dirigées vers le même port ne créent pas de process noyau supplémentaires mais relient la sous–routine au process existant. On compte toujours un process noyau par port utilisé.

La structure interne d’un gestionnaire d’unité DLC est identique à la structure de base d’un gestionnaire d’unité du noyau, à la différence qu’un process noyau remplace le gestionnaire des interruptions pour les événements asynchrones. Le mécanisme de contrôle des E/S, l’écriture et la lecture, et les blocs de sélection sont illustrés à la figure ci-dessous :



Gestionnaire d’unité du noyau standard

Installation de DLC

Vous pouvez installer les DLC séparément ou par groupe. Un gestionnaire d'unité DLC est automatiquement ajouté au noyau et rendu disponible pour chaque type de DLC installé. Pour vérifier l'installation, lancez la commande **lslpp** :

```
lslpp -h dlctype
```

en spécifiant pour *typedlc* l'un des DLC suivants :

bos.dlc.8023	DLC IEEE Ethernet (802.3)
bos.dlc.ether	DLC Standard Ethernet
bos.dlc.fddi	DLC FDDI
bos.dlc.sdlc	DLC SDLC
bos.dlc.token	DLC anneau à jeton

Vous pouvez afficher les informations relatives à un DLC installé via Web-based System Manager, SMIT (System Management Interface Tool) ou à partir de la ligne de commande. Sur les ports de communication et systèmes très sollicités, il peut être nécessaire de modifier les attributs DLC pour optimiser les performances DLC. Si la réception est longue et que le journal des erreurs système signale une surcharge sur la file d'attente d'appels entre le DLC et son gestionnaire, augmentez sa capacité pour les données entrantes. Enfin, retirez un DLC installé à partir du noyau s'il est inutilisé pendant un certain temps : il n'est pas supprimé du système, mais des ressources noyau sont libérées. Les instructions associées figurent à la section "Gestion des pilotes d'unités DLC", page 7-15.

Opérations ioctl sur l'interface GDLC

L'interface GDLC prend en charge les opérations de sous-routines **ioctl** :

DLC_ENABLE_SAP	Active un point d'accès au service (SAP).
DLC_DISABLE_SAP	Désactive un SAP.
DLC_START_LS	Lance une station de liaison sur un SAP particulier comme appelant ou appelé.
DLC_HALT_LS	Interrompt une station de liaison.
DLC_TRACE	Suit l'activité d'une station de liaison (activités longues ou courtes).
DLC_CONTACT	Contacte une station distante pour une station de liaison locale particulière.
DLC_TEST	Teste la liaison vers une station distante pour une station de liaison locale particulière.
DLC_ALTER	Modifie les paramètres de configuration d'une station de liaison.
DLC_QUERY_SAP	Recherche les données statistiques d'un SAP.
DLC_QUERY_LS	Recherche les données statistiques d'une station de liaison.
DLC_ENTER_LBUSY	Passe en mode local-busy sur une station de liaison.
DLC_EXIT_LBUSY	Sort du mode local-busy sur une station de liaison.
DLC_ENTER_SHOLD	Passe en mode short- hold sur une station de liaison.
DLC_EXIT_SHOLD	Sort du mode short- hold sur une station de liaison.
DLC_GET_EXCEP	Renvoie des notifications d'exceptions asynchrones à l'utilisateur niveau application. **Remarque :** Cette opération de sous-routine **ioctl** n'est pas utilisée par l'utilisateur niveau noyau puisque toutes les conditions d'exception ont préalablement été filtrées par le gestionnaire d'exception.
DLC_ADD_GRP	Ajoute à un port un groupe ou une adresse de réception multi-destinataire.
DLC_ADD_FUNC_ADDR	Ajoute à un port un groupe ou une adresse de réception multi-destinataire.
DLC_DEL_FUNC_ADDR	Supprime d'un port un groupe ou une adresse de réception multi-destinataire.
IOCINFO	Renvoie une structure décrivant le gestionnaire d'unité GDLC. Pour en savoir plus, reportez-vous au format de fichier **/usr/include/sys/devinfo.h**.

Point d'accès au service

Un point d'accès au service (SAP) identifie un service utilisateur chargé d'envoyer et de recevoir une certaine classe de données. Ainsi, différentes classes de données peuvent être acheminées séparément vers leurs gestionnaires de service respectifs. Les DLC qui prennent en charge plusieurs SAP simultanément portent dans leur en-tête de paquet des adresses SAP source et destination. Ceux qui n'acceptent qu'un seul SAP n'ont pas besoin d'adressage SAP, mais l'activation du SAP est toujours requise. On compte généralement sur chaque port un SAP activé par utilisateur DLC.

La plupart des adresses SAP sont définies par les organismes de gestion de réseaux normalisés IEEE ou par les utilisateurs comme indiqué dans le manuel *Token–Ring Network Architecture Reference*. Voici quelques adresses SAP courantes :

Null SAP (0x00)	Permet de répondre à des noeuds distants même si aucun SAP n'est activé. Le SAP nul ne prend en charge que le service sans connexion et ne répond qu'aux LPDU (Link Protocol Data Unit) XID et TEST.
SNA Path Control (0x04)	Adresse SAP individuelle par défaut utilisée par les noeuds SNA.
PC Network NETBIOS (0xF0)	Utilisé pour toute communication DLC pilotée par émulation NETBIOS.
Discovery SAP (0xFC)	Utilisés par les services de noms LAN.
Global SAP (0xFF)	Identifie tous les SAP actifs.

Station de liaison

Une station de liaison (LS) identifie un raccordement entre deux noeuds pour une paire SAP. Cette liaison peut fonctionner comme service sans connexion (datagramme) ou orienté connexion (transfert intégralement suivi des données avec recouvrement des erreurs). Généralement, une station de liaison est lancée pour chaque téléraccordement.

Mode Local-Busy

En exploitation orientée connexion, une station de liaison doit arrêter l'émission des paquets en provenance de la station distante, en cas d'indisponibilité des ressources, par exemple. Il est alors possible d'avertir la station distante de faire passer la station locale en mode local–busy. Dès que les ressources sont de nouveau disponibles, la station locale en avertit la station distante qui peut reprendre l'émission des paquets. En mode local-busy, seuls les paquets d'informations séquencés sont arrêtés. Les autres types de données ne sont pas concernés.

Mode Short-Hold

Ce mode est particulièrement adapté aux réseaux de données pour lesquels :

- le délai d'établissement d'une connexion est court,
- le coût d'établissement de la connexion est faible par rapport à son coût d'utilisation.

En mode short-hold, la liaison entre deux stations est maintenue tant qu'il y a des données à transférer. Dès lors qu'il n'y a plus de données à envoyer, la liaison est interrompue (à l'expiration d'un délai défini) et n'est rétablie que lorsque des données sont de nouveau disponibles pour le transfert.

Test et suivi d'une liaison

Pour tester le raccordement de deux stations, demandez à une station de liaison d'émettre un paquet test à partir de la station locale. Ce paquet est renvoyé par la station distante si la liaison fonctionne correctement.

Certaines liaisons de données sont limitées par des contraintes de protocoles dans l'application de cette fonction. SDLC, par exemple, ne peut générer le paquet test qu'à partir de la station hôte ou principale. Néanmoins, la plupart des protocoles laissent toute latitude pour le choix de la station d'origine.

Pour suivre une liaison, il est possible de consigner les données de la ligne et les événements spéciaux (activation et fermeture d'une station, écoulement des délais, etc.), dans le dispositif de suivi générique de chaque station de liaison. Cette fonction permet de déterminer l'origine de certains incidents de raccordement. L'utilisateur de GDLC indique si le suivi doit porter sur des entrées longues ou courtes.

Les entrées courtes sont constituées au maximum de 80 octets de données alors que les entrées longues autorisent le suivi des paquets de données complets.

Le suivi peut être activé au lancement de la station de liaison, ou activé/désactivé de façon dynamique ultérieurement.

Statistiques

L'utilisateur GDLC dispose de deux services statistiques : les statistiques SAP, qui fournissent les informations et l'état SAP courants du gestionnaire d'unité ; et les statistiques LS, qui indiquent l'état courant de la station et des compteurs de fiabilité/disponibilité/maintenabilité (contrôlant l'activité de la station dès son lancement).

Services spéciaux du noyau

GDLC (Generic Data Link Control) met à la disposition de l'utilisateur noyau des services spéciaux. Le noyau doit cependant être doté d'un environnement sécurisé. A la différence du gestionnaire d'unité DLC qui copie les données des événements asynchrones dans un espace utilisateur, l'utilisateur noyau doit spécifier des pointeurs de fonction vers des routines spéciales appelées gestionnaires de fonction. Ces derniers sont appelés par le DLC lors de l'exécution, ce qui assure des performances maximales entre l'utilisateur noyau et les couches DLC. Il est demandé à chaque utilisateur noyau de limiter le nombre de gestionnaires de fonction à une longueur de chemin minimale et de suivre le schéma des tampons de mémoire de communication (mbuf).

Un gestionnaire de fonction ne doit jamais appeler une autre entrée DLC directement. En effet, les appels directs sont verrouillés, entraînant une mise en veille bloquante. Une seule exception à cette règle : l'utilisateur noyau peut appeler le point d'entrée **dlcwritex** pendant que ce dernier assure le service d'une des quatre fonctions de données de réception. Cet appel permet de générer immédiatement les réponses sans passer par un commutateur de tâche. Une logique spéciale est nécessaire dans le gestionnaire d'unité DLC pour contrôler l'identification de l'utilisateur sollicitant une opération en écriture. S'il s'agit d'un process DLC et que la capacité interne d'accueil en file d'attente DLC a été dépassée, l'écriture est renvoyée avec un code d'erreur (valeur retour **EAGAIN**) au lieu de mettre en veille le process appelant. La sous-routine du demandeur doit alors renvoyer une notification au DLC pour prévoir une nouvelle tentative du tampon récepteur.

Les gestionnaires de fonction disponibles sont les suivants :

Datagram Data Received Routine

Appelée chaque fois qu'un paquet datagramme arrive pour l'utilisateur noyau.

Exception Condition Routine

Appelée chaque fois qu'un événement asynchrone à signaler à l'utilisateur noyau se produit (SAP Closed ou Station Contacted, par exemple).

I–Frame Data Received Routine

Appelée chaque fois qu'un paquet normal de données séquencées arrive pour l'utilisateur noyau.

Network Data Received Routine

Appelée chaque fois qu'un paquet réseau spécifique arrive pour l'utilisateur noyau.

XID Data Received Routine

Appelée chaque fois qu'un paquet XID (exchange identification) arrive pour l'utilisateur noyau.

Les points d'entrée **dlcread** et **dlcselect** de DLC ne sont pas appelés par l'utilisateur noyau : les entrées asynchrones fonctionnelles sont appelées directement par le gestionnaire d'unité DLC. Normalement, la mise en file d'attente de ces événements doit intervenir dans le gestionnaire de fonction de l'utilisateur. Toutefois, si l'utilisateur noyau ne peut pas traiter un paquet, le gestionnaire d'unité DLC peut bloquer le dernier tampon reçu et passer dans l'un des deux modes user-busy :

User–Terminated Busy Mode (I–frame exclusivement)

Si l'utilisateur noyau ne peut pas traiter une trame-I reçue (suite à un incident tel un blocage au niveau de la file d'attente), un code DLC_FUNC_BUSY est renvoyé, et DLC bloque le pointeur de tampon et passe en mode local-busy pour interrompre l'émission des trames-I par la station distante. L'utilisateur noyau doit alors appeler la fonction Exit Local Busy pour réinitialiser le mode local-busy et reprendre la réception des trames-I. Seules les trames-I séquencées normales peuvent être interrompues : le mode local-busy n'a aucune incidence sur les données XID, datagramme et réseau.

Timer–Terminated Busy Mode (tous types de trames)

Si l'utilisateur noyau ne peut pas traiter un paquet reçu et souhaite que DLC bloque un court instant le tampon de réception, puis rappelle la fonction de réception utilisateur, un code DLC_FUNC_RETRY est renvoyé au DLC. Si le paquet est une trame-I séquencée, la station passe en mode local-busy pendant ce délai. Dans tous les cas, un compte à rebours est lancé : à expiration, l'entrée fonctionnelle de données de réception est rappelée.

Identification des incidents GDLC

Chaque GDLC fournit des données d'identification d'incident, qui permettent d'isoler les incidents réseau. Quatre types de données sont fournies :

- Informations d'état DLC
- Consignation des erreurs DLC, page 7-13
- Suivi d'une station de liaison, page 7-13
- Suivi du moniteur LAN., page 7-14

Informations d'état DLC

Les informations d'état sur un point d'accès au service (SAP) ou une station de liaison (LS) peuvent être obtenues via les sous-routines ioctl **DLC_QUERY_SAP** et **DLC_QUERY_LS**, pour appeler le gestionnaire d'unité du noyau DLC spécifique en cours.

La sous-routine ioctl **DLC_QUERY_SAP** permet d'accéder aux statistiques individuelles de plusieurs types d'unité :

- Anneau à jeton
- Ethernet
- Multiprotocole

La sous-routine ioctl **DLC_QUERY_SAP** permet d'accéder aux statistiques LS de plusieurs DLC, dont les statistiques concernant les compteurs des protocoles de liaison de données. Chaque compteur est réinitialisé par le DLC pendant la sous-routine ioctl **DLC_START_LS,** et est normalement actif jusqu'à ce que la station de liaison soit arrêtée et son espace de stockage libéré. Si le compteur atteint son maximum, le décompte est gelé (il ne repart pas à zéro).

Les compteurs qu'il est conseillé d'associer à un gestionnaire d'unité DLC sont indiqués ci-après. Certains DLC peuvent modifier cet ensemble, sur la base du protocole spécifique pris en charge (le nombre de rejets ou de paquets RNR (non prêt à recevoir) reçus peut ainsi être significatif).

Test Commands Sent	Décompte (binaire) des commandes **test** envoyées par GDLC à la station distante, en réponse aux commandes **test** émises par l'utilisateur.
Test Command Failures	Décompte (binaire) des commandes **test** dont l'exécution n'a pas abouti, pour cause de problèmes tels que : • réponse non valide, • discordance de données, • inactivité.
Test Commands Received	Décompte (binaire) des commandes **test** valides reçues, que la réponse ait abouti ou non.
Sequenced Data Packets Transmitted	Décompte (binaire) du nombre total de paquets normaux de données séquencées transmis au LS distant.
Sequenced Data Packets Transmitted	Décompte (binaire) du nombre total de paquets normaux de données séquencées transmis au LS distant.
Maximum Contiguous Retransmissions	Décompte (binaire) du nombre maximal de fois qu'un paquet de données a été transmis à la station LS distante avant acquittement. Le compteur est remis à zéro chaque fois qu'un acquittement valide est reçu.

Sequenced Data Packets Received	Décompte (binaire) du nombre total de paquets normaux de données séquencées correctement reçus.
Invalid Packets Received	Décompte (binaire) du nombre de commandes ou de réponses non valides reçues - octets de contrôle non valides, champs-I non valides et champs-I saturés compris.
Adapter Detected Receive Errors	Décompte (binaire) du nombre d'erreurs de réception signalées par le pilote d'unité.
Adapter Detected Transmit Errors	Décompte (binaire) du nombre d'erreurs de réception signalées par le pilote d'unité.
Receive Inactivity Time–outs	Décompte (binaire) du nombre de dépassements de délai en réception.
Command Polls Sent	Décompte (binaire) du nombre de paquets de commandes envoyées, nécessitant une réponse de la station LS distante.
Command Repolls Sent	Décompte (binaire) du nombre total de paquets de commandes retransmis à la station LS distante, faute de réponse.
Command Contiguous Repolls	Décompte (binaire) du nombre de fois qu'un paquet de commandes a dû être retransmis à la station LS distante, faute de réponse. Le compteur est remis à zéro chaque fois qu'une réponse valide est reçue.

Consignation des erreurs DLC

Lorsque chaque DLC rencontre une erreur, il crée une entrée dans le journal des erreurs système.

Vous pouvez obtenir les données formatées de ce journal via la commande **errpt**. Assortie de l'indicateur **–N** *NomDLC*, cette commande génère un récapitulatif de toutes les erreurs consignées pour la ressource spécifiée par le paramètre *NomDLC*, ce paramètre pouvant prendre l'une des valeurs suivantes-:

SYSXDLCE	liaison de données Ethernet standard
SYSXDLCI	liaison de données Ethernet IEEE 802.3
SYSXDLCT	liaison de données en anneau à jeton
SYSXDLCS	liaison de données SDLC

Pour des précisions sur le format des vecteurs requis, reportez-vous au manuel *SNA Format and Protocol Reference Manual: Management Services.*

Pour en savoir plus sur la fonction de consignation des erreurs, reportez-vous à "Journalisation des erreurs : présentation" dans *AIX Version 4.3 - Guide de résolution des incidents*.

Suivi d'une station de liaison

GDLC offre un accès en option à un canal de suivi système générique, comme requis par la norme fiabilité/disponibilité/maintenabilité. Par défaut, le suivi est désactivé : les performances en sont meilleures, et le nombre de ressources système utilisées, moindre. Pour en savoir plus sur les fonctions de suivi complémentaires, reportez-vous à "Gestion des pilotes d'unités DLC", page 7-15.

Canaux de suivi

Le système d'exploitation prend en charge jusqu'à sept canaux de suivi génériques simultanément. Avant de démarrer le suivi d'une LS, l'utilisateur doit affecter un canal, via l'opération ioctl **DLC_START_LS** ou **DLC_TRACE**, par le biais des sous-routines **trcstart** et **trcon**.

Pour arrêter le suivi d'une LS, vous avez le choix entre arrêter la LS ou exécuter une opération ioctl (**DLC_TRACE**, indicateurs=0) sur la station. Une fois le suivi interrompu, le canal est désactivé via la sous-routine **trcoff** et revient au système via la sous-routine **trcstop**.

Rapports de suivi

Pour obtenir les données de suivi consignées, formatées, lancez la commande **trcrpt** avec le nom du fichier concerné. Par exemple :

```
trcrpt /tmp/link1.log
```

Cette commande génère un état détaillé de toutes les entrées de suivi du fichier **/tmp/link1.log**, *sous réserve* qu'une sous-routine **trcstart** préalable ait désigné le fichier **/tmp/link1.log** comme nom **o** du journal de suivi.

Entrées de suivi

Pour chaque entrée de suivi, GDLC génère le service de noyau **trcgenkt** dans le suivi générique de noyau.

Suivi du moniteur LAN

Chacun des DLC associés au réseau local (DLCETHER, DLC8023, DLCFDDI et DLCTOKEN) offre une fonction de suivi de moniteur interne, permettant d'identifier la séquence de points d'entrée pertinents à l'intérieur de ce code. Cette fonction est particulièrement utile si le réseau présente des problèmes indiquant que la liaison de données est mal exécutée : la séquence d'événements peut aider à identifier la cause des problèmes. Ce suivi, commun à tous les DLC du réseau LAN, est désactivé par défaut.

Pour activer le suivi du moniteur LAN, lancez la commande :

```
trace -j 246
```

`246` étant l'ID du point d'ancrage pour lequel un suivi est demandé.

La commande **trcstop** interrompt le suivi, un état pouvant être obtenu via la commande :

```
trcrpt -d 246
```

`246` étant l'ID du point d'ancrage pour lequel un état est demandé.

> **Remarque :** Soyez prudent si vous activez le suivi moniteur : cette fonction affecte directement les performances des DLC et unités associées.

Pour en savoir plus sur les fonctions de suivi complémentaires, reportez-vous à "Gestion des pilotes d'unités DLC", page 7-15.

Gestion des pilotes d'unités DLC

Un DLC doit être installé pour pouvoir être ajouté au système. Chaque DLC installé est automatiquement ajouté après l'installation et à chaque réinitialisation du système. Si un DLC a été supprimé sans être suivi d'une réinitialisation, il peut être ajouté de nouveau, selon la procédure suivante :

Gestion des opérations des pilotes d'unités DLC		
Web-based System Manager: raccourci **unités wsm** (application Devices) OU		
Restrictions d'accès FTP	*Raccourci SMIT*	*Commande ou fichier*
Ajout d'un DLC installé	Choix possibles (par nom de pilote d'unité) : **smit cmddlc_sdlc** **smit cmddlc_token** **smit cmddlc_qllc** **smit cmddlc_ether**[1] **smit cmddlc_fddi** puis sélectionnez l'option **Add**	**mkdev**[2]
Modification des attributs DLC[3,4]	Choix possibles (par nom de pilote d'unité) : **smit cmddlc_sdlc_ls** **smit cmddlc_token_ls** **smit cmddlc_qllc_ls** **smit cmddlc_ether_ls**[1] **smit cmddlc_fddi_ls**	**chdev**[2]
Démarrage du suivi du moniteur LAN DLC[5]	**smit trace**	**trace –j *nnn***, *nnn* étant l'ID du point d'ancrage pour lequel un suivi est demandé.
Arrêt du suivi du moniteur LAN DLC	**smit trcstop**	**trcstop**[2]
Génération d'états sur le suivi du moniteur LAN DLC	**smit trcrpt**	**trcrpt –d *nnn***, *nnn* étant l'ID du point d'ancrage pour lequel un état est demandé.
Affichage d'informations sur le DLC courant[3]	Choix possibles (par nom de pilote d'unité) : **smit cmddlc_sdlc_ls** **smit cmddlc_token_ls** **smit cmddlc_qllc_ls** **smit cmddlc_ether_ls**[1] **smit cmddlc_fddi_ls**	**lsdev**[2] ou **lsattr**[2]
Suppression d'un DLC[3,6]	Choix possibles (par nom de pilote d'unité) : **smit cmddlc_sdlc_rm** **smit cmddlc_token_rm** **smit cmddlc_qllc_rm** **smit cmddlc_ether_rm**[1] **smit cmddlc_fddi_rm**	**rmdev**[2]

Remarques :

1. La commande SMIT d'ajout d'un gestionnaire d'unité Ethernet concerne aussi bien le gestionnaire standard que le gestionnaire IEEE 802.3.
2. Pour plus d'informations sur les options de ligne de commande, consultez les descriptions des commandes **mkdev**, **chdev**, **trace**, **trcstop**, **trcrpt**, **lsdev**, **lsattr** ou **rmdev** dans *AIX Commands Reference*.
3. Un DLC doit être installé et ajouté pour que vous puissiez afficher, modifier ou supprimez ses attributs. Modifier un attribut n'aboutit que si le DLC cible ne fait l'objet d'aucune ouverture active. Avant toute modification, il convient d'interdire à tous les services, tels que SNA, OSI ou NetBIOS, l'accès au DLC.
4. Modifier la taille de la file d'attente de réception a une incidence directe sur les ressources système. N'effectuez ce changement que si le DLC présente des failles au niveau de cette file d'attente (dégradation des performances ou surcharge entre le DLC et son gestionnaire, par exemple).
5. Soyez prudent si vous activez le suivi moniteur : cette fonction affecte directement les performances des DLC et unités associées.
6. Supprimer un DLC n'aboutit que si le DLC cible ne fait l'objet d'aucune ouverture active. Avant toute suppression, il convient d'interdire à tous les services, tels que SNA, OSI ou NetBIOS, l'accès au DLC.

Chapitre 8. Utilitaires réseau (BNU)

Ce chapitre traite de l'installation, la configuration et la maintenance des utilitaires réseau (BNU). Cette section traite des points suivants :

Présentation de BNU

Les utilitaires BNU (Basic Networking Utilities) sont constitués d'un groupe de programmes, répertoires et fichiers, exploitables pour établir une communication avec un système UNIX sur lequel une version du programme UUCP (UNIXtoUNIX Copy Program) est active. Il s'agit de l'un des programmes de services étendus pouvant être installés avec le système d'exploitation de base.

BNU contient un groupe de commandes liées à UUCP, programme de communication UNIX vers UNIX développé par AT&T et modifié dans le cadre de la distribution Berkeley Software (BSD). BNU fournit des commandes, des processus et une base de données de support pour les connexions aux systèmes locaux et distants. Les réseaux de communication (tels TokenRing et Ethernet) servent à connecter des systèmes sur des réseaux locaux.
Un réseau local peut être connecté à un système distant par un modem téléphonique ou un câble. Commandes et fichiers peuvent alors être échangés entre le réseau local et le système distant.

Cette section traite des points suivants :

- Fonctionnement de BNU
- Structure de répertoires et de fichiers BNU
- Sécurité de BNU
- Démons BNU

Les programmes BNU ne peuvent être exploités qu'une fois BNU installé et configuré.

BNU est contrôlé par un jeu de fichiers de configuration qui détermine si les systèmes distants peuvent se connecter au système local et ce qu'ils sont habilités à exécuter une fois la connexion établie. Ces fichiers de configuration doivent être configurés en fonction des impératifs et des ressources de votre système.

Pour la maintenance de BNU, vous devez lire et supprimer régulièrement les fichiers journaux, et vérifier les files d'attente BNU pour vous assurer que le transfert des travaux aux systèmes distants s'effectue correctement. Vous devez également mettre régulièrement à jour les fichiers de configuration pour y répercuter les modifications de votre système ou des systèmes distants.

Pour en savoir plus, reportez–vous à :

- Configuration de BNU
  - Informations préalables
- Maintenance de BNU
  - Fichiers journaux BNU
  - Commandes de maintenance BNU

Fonctionnement de BNU

BNU assure la communication entre systèmes via un ensemble de connexions matérielles et de logiciels. Une structure de répertoires et de fichiers suit à la trace les activités BNU. Cette structure intègre un jeu de répertoires publics, un groupe de répertoires et de fichiers administratifs, des fichiers de configuration et des fichiers de verrouillage. La plupart des répertoires BNU sont créés au cours de l'installation. Certains répertoires et fichiers administratifs sont créés par les différents programmes BNU.

A l'exception des commandes de connexion à distance, BNU fonctionne comme un système de traitement par lots. Lorsqu'un utilisateur demande qu'un travail soit envoyé à un système distant, BNU stocke les informations nécessaires. Cette opération s'appelle *mise en file d'attente* du travail. A des moments planifiés, ou à la demande d'un utilisateur, BNU contacte différents systèmes distants, transfère le travail en file d'attente et accepte d'autres travaux. Ces transferts sont contrôlés par les fichiers de configuration de votre système et par ceux du système distant.

Support NLS (National Language Support) pour les commandes BNU

Toutes les commandes BNU, sauf **uucpadm**, sont prises en charge par NLS (langue nationale). Les noms utilisateur ne doivent pas être forcément en caractères ASCII. Mais tous les noms de système doivent être en caractères ASCII. Si un utilisateur tente de planifier un transfert ou une exécution de commande à distance impliquant des noms système non ASCII, BNU renvoie un message d'erreur.

Structure de répertoires et de fichiers BNU

BNU a recours à une structure de répertoires et de fichiers pour garder trace de ses activités. Cette structure comporte :

- Répertoires publics
- Fichiers de configuration
- Répertoires et fichiers administratifs
- Fichiers de verrouillage.

La plupart des répertoires BNU sont créés au cours de l'installation. Certains répertoires et fichiers administratifs sont créés au cours de l'exécution des différents programmes BNU.

Répertoires publics BNU

Le répertoire public BNU, /**var**/**spool**/**uucppublic**, stocke les fichiers transférés sur le système local par d'autres systèmes. Ces fichiers restent en attente jusqu'à ce que des utilisateurs viennent les chercher via la commande **uupick**. Le répertoire public est créé au cours de l'installation de BNU. Dans le répertoire public, BNU crée autant de sousrépertoires que de systèmes distants envoyant des fichiers au système local.

Fichiers de configuration BNU

Les fichiers de configuration BNU, ou base de données de support BNU, se trouvent dans le répertoire /**etc**/**uucp**. Les fichiers doivent être configurés spécifiquement pour votre système. Ils sont propriété de l'ID de connexion uucp et ne peuvent être édités que par l'utilisateur racine. Les fichiers de configuration contiennent des informations sur :

- les systèmes distants accessibles,
- les unités permettant le contact avec les systèmes distants,
- les horaires d'accès aux systèmes distants,
- les actions autorisées aux systèmes distants sur votre système.

Certains fichiers de configuration spécifient également des limites aux activités de BNU pour éviter une surcharge de votre système.

Liste des fichiers de configuration :

Devices	Contient des informations sur les unités disponibles, notamment les modems et les connexions directes.
Dialcodes	Contient des codes de numérotation abrégés, permettant de raccourcir les numéros de téléphone dans le fichier **Systems**.
Dialers	Spécifie la syntaxe de commande d'appels pour un type de modem spécifique ("dialer").
Maxuuscheds	Limite les travaux programmés simultanément.
Maxuuxqts	Limite les exécutions simultanées de commandes à distance.
Permissions	Contient les codes d'autorisation d'accès. Il s'agit du fichier de sécurité principal de BNU.
Poll	Définit les moments où le programme BNU doit demander aux systèmes distants de lancer les tâches.

Sysfiles	Répertorie les fichiers qui servent de fichiers **Systems**, **Devices** et **Dialers** pour la configuration BNU. Les fichiers par défaut sont **/etc/uucp/Systems**, **/etc/uucp/Devices** et **/etc/uucp/Dialers**.
Systems	Donne la liste des systèmes accessibles et des informations requises pour les contacter : unité à utiliser, combinaisons nom et mot de passe utilisateur requises pour la connexion, etc. Spécifie également les créneaux horaires pendant lesquels les systèmes peuvent être contactés.

Les fichiers de configuration se font mutuellement référence. Par exemple :

- Le fichier **Devices** contient un champ *Token* se rapportant aux entrées du fichier **Dialers**.
- Le fichier **Systems** contient une entrée par classe (Class) d'unité. Une unité de chaque *Class* mentionnée dans le fichier **Systems** doit être définie dans le fichier **Devices**.
- Le fichier **Poll** contient des entrées pour les systèmes appelés par le vôtre. Chaque système mentionné doit être défini dans le fichier **Systems**.

Les entrées des fichiers de configuration BNU dépendent du type des connexions entre votre système et chaque système distant. Par exemple, des entrées spéciales doivent être établies pour des connexions directes ou TCP/IP (Transmission Control Protocol/Internet Protocol). Si la connexion passe par des modems, ils doivent être définis dans le fichier **Dialers**.

Les fichiers **Systems**, **Devices** et **Permissions** doivent être configurés sur votre système pour que vous puissiez contacter des systèmes distants via BNU. D'autres fichiers de configuration donnent accès aux fonctions BNU telle l'interrogation automatique. La plupart de ces fichiers doivent être périodiquement modifiés pour refléter les changements opérés sur votre système ou sur les systèmes contactés. Le fichier **Sysfiles** peut servir à attribuer à d'autres fichiers le rôle des fichiers **Systems**, **Devices** et **Dialers**.

Répertoires et fichiers administratifs BNU

Les répertoires et fichiers administratifs BNU se trouvent dans des sousrépertoires de **/var/spool/uucp**. Ils contiennent deux types d'informations :

- les données en attente de transfert vers d'autres systèmes,
- les informations de journalisation et d'erreur sur les activités BNU.

Dans le répertoire **/var/spool/uucp**, BNU crée les répertoires suivants :

.Admin	Contient quatre fichiers administratifs. • **audit** • **Foreign** • **errors** • **xferstats** Ces fichiers contiennent des informations de journalisation et d'erreur relatives aux activités BNU.
.Corrupt	Contient la copie des fichiers que le programme BNU ne peut pas traiter.
.Log et **.Old**	Contient les fichiers journaux issus des anciennes transactions BNU.
.Status	Prend date de la dernière tentative du démon **uucico** de communiquer avec les systèmes distants.
.Workspace	Contient les fichiers temporaires utilisés en interne par les programmes de transport de fichier.

.Xqtdir	Contient les fichiers exécutables avec les listes des commandes exécutables par les systèmes distants.
SystemName	Contient les fichiers utilisés par les programmes de transport de fichier. Ces fichiers sont : • Command (**C.***) • Data (**D.***) • Execute (**X.***) • Temporary (**TM.***) BNU crée un répertoire *SystemName* pour chaque système distant qu'il contacte.

Les répertoires dont le nom commence par un point sont *cachés*. Ils ne sont pas affichés par les commandes **ls** ou **li** sauf si elles sont assorties de l'indicateur **–a**. A son lancement, le démon **uucico** recherche dans le répertoire /**var**/**spool**/**uucp** les fichiers de travail et transfère les fichiers de tout répertoire non caché. Le démon **uucico** ne voit que les répertoires *SystemName*, à l'exclusion des autres répertoires administratifs.

Les fichiers des répertoires cachés sont propriété de l'ID de connexion uucp. Ils ne sont accessibles que par l'utilisateur racine ou via un ID de connexion dont l'UID est de 5.

Pour en savoir plus sur la maintenance des répertoires administratifs BNU, reportez-vous à "Maintenance de BNU", page 8-18.

Fichiers de verrouillage BNU

Ils sont stockés dans le répertoire /**etc**/**locks**. Lorsque BNU utilise une unité pour se connecter à un ordinateur distant, il place un fichier de verrouillage pour cette unité dans le répertoire /**etc**/**locks**. Lorsqu'un autre programme (BNU ou non) a besoin de l'unité, il vérifie s'il existe un fichier de verrouillage dans /**etc**/**locks**. Dans l'affirmative, le programme attend que l'unité soit disponible ou utilise une autre unité pour la communication.

En outre, le démon **uucico** place des fichiers de verrouillage dans le répertoire /**etc**/**locks** pour les systèmes distants. Avant de contacter un système distant, le démon **uucico** vérifie la présence d'un fichier de verrouillage pour ce système dans /**etc**/**locks**. Ces fichiers empêchent d'autres instances du démon **uucico** d'établir des connexions en double au même système distant.

Remarque : Outre BNU, d'autres logiciels, comme ATE (Asynchronous Terminal Emulation) et TCP/IP, utilisent le répertoire /**etc**/**locks**.

Sécurité de BNU

D'autres systèmes prenant contact avec le vôtre pour se connecter, transférer des fichiers et lancer des commandes, BNU fournit des moyens d'assurer la sécurité. Les fonctions de sécurité BNU permettent de limiter les actions exécutables par les systèmes distants sur le système local (les utilisateurs des systèmes distants peuvent également limiter les actions que vous êtes habilité à effectuer). Pour ce faire, BNU exécute plusieurs démons et utilise les répertoires administratifs pour y stocker les fichiers dont il a besoin. Il conserve également un journal de ses propres activités.

La sécurité de BNU fonctionne à plusieurs niveaux. Lorsque vous configurez BNU, vous pouvez déterminer :

- les utilisateurs de votre système habilités à accéder aux fichiers BNU ;
- les systèmes distants accessibles par votre système ;
- le mode de connexion des utilisateurs distants à votre système ;
- les actions accessibles aux utilisateurs connectés à votre système.

ID de connexion uucp

A l'installation de BNU, tous les fichiers de configuration, les démons et nombre de commandes et de procédures shell appartiennent à l'ID de connexion uucp. L'ID de connexion uucp a un ID utilisateur (UID) de 5 et un ID de groupe (GID) de 5. Le démon **cron** lit le fichier **/var/spool/cron/crontabs/uucp** pour planifier les travaux automatiques pour BNU.

Il est en général interdit de se connecter comme utilisateur uucp. Pour modifier des fichiers appartenant à l'ID de connexion uucp, connectezvous en tant qu'utilisateur racine.

Attention : Autoriser la connexion de systèmes distants au système local avec un ID de connexion uucp nuit gravement à la sécurité de votre système. En effet, les systèmes distants ainsi connectés peuvent afficher voire modifier (selon les droits d'accès définis dans l'entrée LOGNAME) les fichiers locaux **Systems** et **Permissions**. Il est donc vivement recommandé d'attribuer d'autres ID de connexion BNU aux systèmes distants et de réserver les ID UUCP aux administrateurs BNU du système local. Pour une sécurité maximale, définissez pour chaque système distant appelé à communiquer avec le système local un ID de connexion unique avec un UID (ID utilisateur) et un GID (ID de groupe) uniques.

ID de connexion BNU

Le shell de lancement pour les ID de connexion BNU est le démon **uucico** (**/usr/sbin/uucp/uucico**). Lorsque des systèmes distants appellent votre système, ils lancent automatiquement le démon **uucico** sur votre système. Les ID de connexion pour BNU ont un ID de groupe uucp de5.

Les ID de connexion utilisés par les systèmes distants ont besoin de mots de passe. Pour éviter que, dans le cadre de la sécurité, un nouveau mot de passe soit demandé au nouvel ID de connexion BNU lorsque le système distant se connecte, vous devez définir ce mot de passe dès la création du compte. Pour ce faire, utilisez la commande **passwd** suivie de la commande **pwdadm**. Par exemple, pour définir un mot de passe pour l'ID de connexion `nuucp`, connectezvous en tant qu'utilisateur racine et entrez les commandes :

```
passwd nuucp

pwadm -f NOCHECK
nuucp
```

Le système vous invite à indiquer un mot de passe pour l'ID de connexion `nuucp`. Mener à bien ces étapes permet au système distant de se connecter sans être immédiatement invité à entrer un nouveau mot de passe (que l'ID de connexion orientée traitement par lots `nuucp` ne peut fournir).

Après création de l'ID de connexion pour un système distant, communiquezle à l'administrateur de ce système et indiquezlui le mot de passe.

Création d'un ID de connexion administratif BNU

Un utilisateur racine peut définir un ID de connexion administratif BNU. Cette opération permet de déléguer des tâches d'administration BNU à un utilisateur ne détenant pas les droits racine. L'ID de connexion administratif BNU doit être sécurisé par mot de passe, doté d'un UID de5 et d'un GID (ID de groupe) uucp de5. Le shell de connexion administrative doit être le programme **/usr/bin/sh** (et non le démon **uucico**). Affecter à la connexion administrative BNU un UID de 5 lui confère les mêmes droits que l'ID de connexion uucp. C'est pourquoi il convient de ne pas accorder aux systèmes distants le droit de se connecter comme administrateur BNU.

Ajout de shells de connexion BNU au fichier login.cfg

Les strophes de configuration utilisateur dans les fichiers **login.cfg** et utilisateur fournissent des informations de configuration aux programmes qui modifient les attributs utilisateur ou ajoutent de nouveaux utilisateurs. La strophe du fichier **login.cfg** est libellée usw. Les strophes du fichier utilisateur sont libellées par les noms utilisateur individuels.

L'attribut shells de la strophe usw définit les shells valides sur le système. Sa valeur est une liste de chemins d'accès complets séparés par des virgules. Valeur par défaut :

```
/usr/bin/sh,/usr/bin/bsh,/usr/bin/csh,/usr/bin/ksh
```

Web-based System ManagerAvant de faire appel à ou à SMIT (System Management Interface Tool) pour ajouter un nouvel utilisateur BNU, ajoutez le nom du programme `/usr/sbin/uucp/uucico` à la strophe shells usw. Le nouveau nom du programme doit être séparé de la dernière entrée par une virgule et non par des espaces; par exemple :

```
/usr/bin/sh,/usr/bin/bsh,/usr/bin/csh,/usr/bin/ksh,/usr/sbin/uucp/uucico
```

Attention : Si le nom du programme **login.cfg** n'est pas ajouté au fichier, WBSN ou SMIT échouent lorsque **/usr/sbin/uucp/uucico** est spécifié comme shell de connexion utilisateur.

Sécurité et fichiers Systems et remote.unknown

Sur la plupart des systèmes BNU, seuls les systèmes distants répertoriés dans le fichier **/etc/uucp/Systems** ou un de ses substituts (spécifié dans le fichier **Sysfiles**) peuvent se connecter au système local. Le script **/usr/sbin/uucp/remote.unknown** est exécuté chaque fois qu'un système inconnu tente d'appeler le système local. Ce script refuse la connexion du système inconnu et consigne l'heure de la tentative dans le fichier **/var/spool/uucp/.Admin/Foreign**.

Avec un privilège racine, ou en tant qu'administrateur BNU, vous pouvez modifier la procédure shell **remote.unknown** de façon à enregistrer plus d'informations sur le système distant ou à stocker les informations dans un fichier différent. Vous pouvez ainsi décider d'envoyer un courrier à l'administrateur BNU dès qu'un système inconnu essaie de se connecter.

En éliminant les droits d'exécution de la procédure shell **remote.unknown**, vous autorisez les machines inconnues à se connecter. Dans ce cas, ajoutez une entrée MACHINE=OTHER dans le fichier **/etc/uucp/Permissions** pour établir les droits des machines inconnues.

Votre système ne peut contacter que les systèmes distants figurant dans le fichier **Systems**. Ceci interdit aux utilisateurs de votre système de contacter des systèmes inconnus.

Sécurité et fichier Permissions

Le fichier **/etc/uucp/Permissions** détermine :

- les noms de connexion des utilisateurs distants pour la connexion au système local ;
- les commandes et les privilèges accordés aux systèmes distants se connectant au système local.

Le fichier **/etc/uucp/Permissions** contient deux types d'entrée :

LOGNAME	Définit les noms de connexion et les privilèges associés. Les entrées LOGNAME prennent effet lorsqu'un système distant appelle le système local et essaie de se connecter.
MACHINE	Définit les noms des machines et les privilèges associés. Les entrées MACHINE prennent effet lorsque le système distant essaie d'exécuter des commandes sur le système local.

Les options du fichier **Permissions** permettent d'établir différents niveaux de sécurité pour chaque système distant. Par exemple, si plusieurs systèmes distants partagent un même ID de connexion sur le système local, utilisez l'option VALIDATE pour obliger chaque système distant à utiliser un ID de connexion unique. Les options SENDFILES, REQUEST et CALLBACK spécifient le système qui détient le contrôle, en conservant au besoin le contrôle des transactions au système local.

Les options READ, WRITE, NOREAD et NOWRITE définissent l'accès à des répertoires spécifiques du système local. Ce sont elles également qui contrôlent l'endroit de votre système où les utilisateurs distants peuvent stocker les données. L'option COMMANDS limite le nombre de commandes exécutables sur le système local par les utilisateurs distants. L'option COMMANDS=ALL accorde tous les privilèges aux systèmes étroitement associés au vôtre.

Attention : L'option COMMANDS=ALL peut sérieusement menacer la sécurité de votre système.

Démons BNU

Le logiciel BNU comprend quatre démons, stockés dans le répertoire **/usr/sbin/uucp** :

uucico	Facilite le transfert de fichiers.
uusched	Facilite la planification des demandes de traitement des fichiers en file d'attente dans le répertoire de spoulage local.
uuxqt	Facilite les exécutions des commandes à distance.
uucpd	Facilite les communications via TCP/IP.

Les démons **uucico**, **uusched** et **uuxqt** sont lancés par le démon cron, suivant la planification décidée par l'administrateur BNU. Avec un privilège d'utilisateur racine, vous pouvez également lancer ces démons manuellement. Dans ce cas, le démon **uucpd** doit être lancé par le démon **inetd** de TCP/IP.

Démon uucico

Le démon **uucico** transporte les fichiers nécessaires au transfert des données entre deux systèmes. Les commandes **uucp** et **uux** lancent le démon **uucico**, pour qu'il transfère les fichiers de commandes et de données, et qu'il exécute les fichiers sur le système désigné. Le démon **uucico** est également régulièrement lancé par le programmateur BNU, le démon **uusched**. Lorsqu'il est lancé par le démon **uusched**, **uucico** essaie de contacter d'autres systèmes et d'exécuter les instructions des fichiers de commandes.

Lancement du processus du démon

Pour exécuter les instructions des fichiers de commandes, le démon uucico recherche d'abord dans le fichier **/etc/uucp/Systems** (ou dans le(s) fichier(s) spécifié(s) dans **/etc/uucp/Sysfiles**) le système à appeler. Il consulte ensuite le fichier **Systems** pour connaître le créneau horaire défini. S'il se trouve dans un créneau horaire admis, le démon **uucico** vérifie les champs *Type* et *Class*, puis recherche dans le fichier **/etc/uucp/Devices** (ou le(s) fichier(s) spécifié(s) dans **/etc/uucp/Sysfiles**) une unité correspondante.

Une fois l'unité trouvée, le démon **uucico** explore le répertoire **/etc/locks** à la recherche d'un fichier de verrouillage pour l'unité. S'il en trouve un, le démon recherche une autre unité du type et du débit requis.

Si aucune unité n'est disponible, le démon revient au fichier **Systems** pour trouver une autre entrée relative au système distant. S'il en existe une, le démon réitère le processus de recherche. Dans le cas contraire, il crée une entrée pour ce système dans le fichier **/var/spool/uucp/.Status/***SystemName*, puis passe à la requête suivante. Le fichier de commande reste dans la file d'attente. Le démon **uucico** tente à nouveau le transfert ultérieurement. Cette nouvelle tentative est appelée réessai.

Contact avec le système distant

Lorsque le démon **uucico** accède au système distant, il se sert des instructions des fichiers Systems pour établir la connexion. Ceci entraîne l'appel d'une instance du démon **uucico** sur le système distant également.

Les deux démons **uucico**, chacun sur un système, coopèrent pour effectuer le transfert. Le démon **uucico** du système appelant contrôle la liaison, en spécifiant les requêtes à effectuer. Le démon **uucico** du système distant vérifie si les autorisations en local permettent l'exécution de la requête. Si tel est le cas, le transfert de fichiers démarre.

Lorsque le premier démon **uucico** a fini de transférer toutes les requêtes pour le système distant, il envoie une demande de raccrochage. Si le deuxième démon **uucico** a des transactions à lui envoyer, il ignore cette demande, et inverse les rôles.

Remarque : Le fichier /**etc**/**uucp**/**Permissions** du système local ou le fichier /**etc**/**uucp**/**Permissions** du système distant peut interdire aux démons d'inverser leurs rôles. Dans ce cas, le système distant doit attendre, pour transférer ses fichiers, d'appeler le système local.

Lorsqu'il ne reste plus rien à transférer d'un côté ou de l'autre, les deux démons **uucico** raccrochent. A ce stade, le démon **uuxqt** est appelé pour exécuter les demandes de commande à distance.

Pendant toute la durée du transfert, les démons **uucico** des deux systèmes enregistrent des messages dans les fichiers d'erreur et le fichier journal de BNU.

Démon uusched

Le démon **uusched** programme le transfert des fichiers en file d'attente dans le répertoire de spoulage du système local. Le répertoire de spoulage est /**var**/**spool**/**uucppublic**. Lorsque le démon **uusched** est appelé, il recherche dans ce répertoire les fichiers de commandes, puis les "randomise" et lance le démon **uucico**. Le démon **uucico** transfère les fichiers.

Démon uuxqt

Lorsqu'un utilisateur émet la commande **uux** pour exécuter une commande sur un système désigné, c'est le démon **uuxqt** qui exécute la commande. Après création des fichiers nécessaires, la commande **uux** lance le démon **uucico**, qui transfère ces fichiers dans le répertoire de spoulage public sur le système spécifié.

Le démon **uuxqt** explore régulièrement le répertoire de spoulage de chaque système connecté : Lorsqu'il trouve une requête, le démon **uuxqt** vérifie l'existence des droits et des fichiers requis. Puis, si l'action est autorisée, le démon exécute la commande spécifiée.

Démon uucpd

Le démon **uucpd** doit être actif sur le système distant pour que BNU puisse établir des communications avec l'ordinateur distant via TCP/IP (Transmission Control Protocol/Internet Protocol). Le démon **uucpd**, sous serveur du démon TCP/IP **inetd**, est lancé par le démon **inetd**.

Par défaut, le démon **inetd** est configuré pour lancer le démon **uucpd**. Si toutefois, cette configuration a été modifiée sur votre système, il vous faudra reconfigurer le démon **inetd** en conséquence pour lancer le démon **uucpd**.

Configuration de BNU

Les procédures suivantes traitent de la configuration de BNU (Basic Network Utilities) pour les différents types de connexion : connexions par câble, par modem, via TCP/IP (Transmission Control Protocol/Internet Protocol), etc.

Prérequis

- BNU doit être installé sur votre système.
- Vous devez être utilisateur racine pour éditer les fichiers de configuration BNU.
- Si vous utilisez des connexions directes, les câbles appropriés entre votre système et les systèmes distants doivent être installés.
- Si vous utilisez des modems pour vos communications BNU, vous devez avoir installé et configuré chaque modem.
- Si une ou plusieurs de vos connexions utilisent le protocole TCP/IP, ce dernier doit être opérationnel entre votre système et les systèmes distants appropriés.
- Rassemblez les informations requises pour configurer BNU. Doivent y figurer la liste des systèmes distants ainsi que celle des unités et des modems à utiliser pour la connexion aux systèmes.

Collecte des informations

Avant de configurer BNU, rassemblez les informations ci-dessous :

- Pour chaque système distant que votre système appellera :
  - le nom du système,
  - le nom de connexion que votre système doit utiliser sur le système distant,
  - le mot de passe pour le nom de connexion,
  - les invites de connexion et de mot de passe sur le système distant,
  - le type de connexion que vous utiliserez pour atteindre le système distant (TCP/IP, direct ou par téléphone).
- Si la connexion est directe :
  - le débit (en bits) de la connexion,
  - le port du système local auquel est rattachée la connexion.
- Si la connexion est téléphonique :
  - le numéro de téléphone du système distant,
  - la vitesse de votre modem, compatible avec celle du système distant.

  Remarque : Si l'un des systèmes distants appelle votre système, assurez-vous que l'administrateur BNU sur chacun des systèmes distants possède, à propos de votre système, toutes les informations citées ci-dessus.
- Pour chaque modem local utilisé :
  - le script `chat` pour le modem (consultez la documentation du modem),

    Remarque : Pour certains modems, le script chat se trouve déjà dans le fichier **/etc/uucp/Dialers**.
  - le port local pour le modem.

A l'aide de ces informations, dressez une liste pour chaque unité à connecter au système distant. Voici un exemple de liste pour le système local `morgan` :

```
direct:
hera 9600 tty5
zeus 2400 tty2
ariadne 2400 tty1
hayes modem (tty3):  apollo, athena
TCP/IP:  merlin, arthur, percy
```

La connexion au système `hera` est de type `direct`, effectuée à la vitesse de `9600` à partir du port `tty5`. La connexion au système `apollo` passe par le modem `hayes` connecté au port `tty3`. La connexion aux systèmes `merlin`, `arthur` et `percy` fait appel à TCP/IP.

Procédure

Pour que BNU fonctionne correctement sur votre site, vous devez configurer les fonctions de communication à distance pour qu'elles :

- dressent la liste des unités utilisées pour établir une liaison par câble, téléphone ou modem ;
- dressent la liste des modems utilisés pour contacter les systèmes distants via le réseau téléphonique ;
- dressent la liste des systèmes distants accessibles ;
- dressent la liste des abréviations alphabétiques représentant les préfixes des numéros de téléphone utilisés pour contacter les systèmes distants spécifiés (en option) ;
- définissent les autorisations d'accès, spécifiant les modes de communication possibles entre les systèmes local et distants ;
- programment la surveillance des systèmes distants en réseau (en option).

Pour créer ces listes, autorisations, programmations et procédures :

- modifiez les fichiers de configuration BNU ;
- éditez le fichier **/var/spool/cron/crontabs/uucp** pour annuler la mise en commentaire (par #) des lignes planifiant les routines de maintenance automatique.

Vous devez également configurer les fichiers **Systems**, **Devices** et **Permissions**. Il n'est pas nécessaire de modifier les fichiers de configuration BNU dans un ordre particulier.

Pour configurer BNU sur votre système :

1. Assurez-vous que BNU est installé sur votre système :

   ```
   lslpp -h bos.net.uucp
   ```

   Si BNU est installé, `bos.net.uucp` apparaît sur la sortie. Sinon, installez `bosext1` à partir de la bande d'installation.

2. Définissez les ID de connexion et mots de passe pour les systèmes distants qui doivent communiquer avec votre système et indiquez-les à l'administrateur BNU ou UUCP (UNIX–to–UNIX Copy Program) de chaque système distant. Pour ce faire, éditez les fichiers **/etc/passwd**, **/etc/group**, **/etc/security/login.cfg** et **/etc/security/passwd**. **Attention :** Autoriser la connexion de systèmes distants au système local avec l'ID de connexion uucp nuit gravement à la sécurité de votre système. En effet, les systèmes distants ainsi connectés peuvent afficher voire modifier (selon les droits définis dans l'entrée LOGNAME du fichier **Permissions**) les fichiers locaux **Systems** et **Permissions**. Il est donc vivement recommandé d'attribuer d'autres ID de connexion BNU aux systèmes distants et de réserver les ID uucp aux administrateurs BNU du système local. Pour une sécurité maximale, définissez pour chaque système distant appelé à communiquer avec le système local un ID de connexion unique avec un UID (ID utilisateur) unique. Ces ID de connexion doivent avoir un GID (ID de groupe) de 5.

Remarque : Les strophes de configuration utilisateur dans **login.cfg** et dans les fichiers utilisateur fournissent des données de configuration pour Web-based System Manager et pour SMIT (System Management Interface Tool). La strophe du fichier **login.cfg** est libellée `usw`. Les strophes du fichier utilisateur sont libellées par les noms utilisateur individuels.

Avant d'exploiter Web-based System Manager ou SMIT pour ajouter un nouvel utilisateur BNU, ajoutez le nom du programme `/usr/sbin/uucp/uucico` à la strophe `usw` des shells. Le nouveau nom du programme doit être séparé de la dernière entrée par un virgule et non par des espaces ; par exemple :

```
/usr/bin/sh,/usr/bin/bsh,/usr/bin/csh,/usr/bin/ksh,
/usr/sbin/uucp/uucico
```

Attention : Si le nom du programme **login.cfg** n'est pas ajouté au fichier, Web-based System Manager ou SMIT échouent lorsque `/usr/sbin/uucp/uucico` est spécifié comme shell de connexion utilisateur.

a. Dans le fichier `/etc/passwd`, attribuez au système un utilisateur `uucpadm` assorti des mêmes ID utilisateur et groupe que uucp. Cet ID utilisateur sera utile pour l'administration et la mise au point du système. Veillez à ce que le shell uucpadm soit différent de `/usr/sbin/uucp/uucico` et définissez `/usr/sbin/uucp` comme répertoire personnel. L'entrée conseillées dans `/etc/passwd` est :

   ```
   uucpadm:!:5:5::/usr/sbin/uucp:/bin/ksh
   ```

b. Vous avez la possibilité d'utiliser, pour l'ensemble des connexions, un ou plusieurs ID de connexion. La première option est conseillée si vous souhaitez contrôler parfaitement l'accès à chaque machine. Dans ce cas, créez les différents ID et associez les entrées MACHINE et LOGNAME dans le fichier **Permissions**. Voici quelques exemples d'entrées /**etc**/**passwd** :

   ```
   Umicrtk:!:105:5:micrtk
   uucp:/usr/spool/uucppublic:/usr/sbin/uucp/uucico
   Ufloydl:!:106:5:floydl
   uucp:/usr/spool/uucppublic:/usr/sbin/uucp/uucico
   Uicus:!:107:5:icus
   uucp:/usr/spool/uucppublic:/usr/sbin/uucp/uucico
   Urisctkr:!:108:5::/usr/spool/uucppublic:/usr/sbin/uucp/uucico
   ```

c. Si vous souhaitez disposer d'un seul jeu de droits d'accès au lieu de contrôler séparément chacune de vos connexions UUCP, définissez un seul ID de connexion pour l'ensemble des machines :

   ```
   nuucp:!:6:5::/usr/spool/uucppublic:/usr/sbin/uucp/uucico
   ```

d. L'ID utilisateur (champ de la troisième colonne) doit être unique pour garantir la sécurité de système. L'ID de groupe (quatrième champ) doit être égal à 5, le même groupe qu'uucp. Vous pouvez définir comme répertoire personnel (sixième champ) n'importe quel répertoire valide, mais le shell de connexion (septième champ) doit être `/usr/sbin/uucp/uucico`.

e. Vérifiez que le fichier /**etc**/**group** contient les nouveaux utilisateurs. Voici un exemple d'entrée de ce type :

   ```
   uucp:!:5:uucp,uucpadm,nuucp,Umicrtk,Uicus,Urisctakr
   ```

f. Vous pouvez ajouter des utilisateurs à un groupe uucp appelé à utiliser des modems avec d'autres programmes que **cu.**

g. Editez ces fichiers en tant qu'utilisateur racine et attribuez un mot de passe aux nouveaux utilisateurs à l'aide de la commande `passwd nom_utilisateur`.

h. Le shell de connexion de vos ID de connexion BNU (`usr/sbin/uucp/uucico`) doit figurer dans la liste des shells spécifiée dans **login.cfg**. Recherchez la strophe `shells =` et ajoutez en fin de liste `/usr/sbin/uucp/uucico`.

i. Il peut arriver que la strophe par défaut herald avec tous ses Ctrl-J interrompe le processus de connexion uucico. (Il se peut que le message `Enough already` s'affiche.) Pour l'éviter, placez la strophe par défaut en commentaire (avec des astérisques) et définissez une strophe pour votre tty, de la forme :

```
dev/tty0:
             herald = "\nrisc001 login:"
```

j. Si vous modifiez un mot de passe à partir d'une connexion racine, les entrées d'indicateurs de la strophe utilisateur dans `/etc/security/passwd` doivent se présenter comme suit :

```
flags = ADMCHG
```

Indiquez à la place :

```
flags=Faute de quoi, à la connexion du uucico distant, un
nouveau mot de passe est demandé, qu'il ne peut fournir. Et la
connexion échoue.
```

k. Une fois connecté en tant qu'administrateur `uucpadm`, exécutez la commande ci-dessous pour lire le crontab courant du BNU vers un fichier temporaire :

```
crontab -l > /tmp/cron.uucp
```

l. Editez ensuite `/tmp/cron.uucp` pour activer les entrées (enlever les marques de commentaire). Elles doivent être semblables à :

```
20,50 * * * * /bin/bsh -c "/usr/sbin/uucp/uudemon.poll > /dev/null"
25,55 * * * * /bin/bsh -c "/usr/sbin/uucp/uudemon.hour > /dev/null"
45 23 * * * /bin/bsh -c "/usr/sbin/uucp/uudemon.cleanu > /dev/null"
48 8,12,16 * * * /bin/bsh -c "/usr/sbin/uucp/uudemon.admin >
/dev/null"
```

Vous pouvez modifier ces entrées à votre gré. Vérifiez la version éditée dans le crontab de BNU, via la commande :

```
crontab /tmp/cron.uucp
```

m. Vérifiez que les modifications sont prises en compte, via la commande :

```
crontab -l
```

n. Configurez les fichiers de données de BNU : Systems, Permissions, Devices, Dialers et Sysfiles. Pour une définition initiale, utilisez la commande **/usr/sbin/uucp/uucpadm** et modifiez-les ensuite selon vos besoins. Notez que Sysfiles permet de spécifier des fichiers de configuration BNU autres que **/etc/uucp/Systems**, **/etc/uucp/Devices** et **/etc/uucp/Dialers**. Pour en savoir plus, reportez-vous à **Sysfiles**.

3. Décidez si vous souhaitez des abréviations pour les numéros de téléphone (voir le format du fichier **Dialcodes**). Si vous décidez d'utiliser des abréviations dans les fichiers **Systems**, définissez l'entrée **Dialcodes** pour chaque abréviation. Pour en savoir plus, reportez–vous à Dialcodes File Format for BNU dans le manuel *AIX Files Reference*.

   Si vous utilisez TCP/IP pour vos connexions BNU, vérifiez à l'aide de la commande **netstat** que le démon **uucpd** est exécutable :

   ```
   netstat -a
   ```

   Le démon **uucpd** est lancé par **inetd**. Si le démon **uucpd** ne peut être exécuté, reconfigurez le démon **inetd** pour lancer le démon **uucpd**.

4. A l'aide de votre liste d'unités, modifiez le fichier **Devices** sur votre système. Créez une entrée pour chaque modem et chaque connexion directe. Si vous utilisez TCP/IP, vérifiez que l'entrée TCP/IP n'est plus en commentaire dans le fichier **Devices**. Vous pouvez configurer le fichier /**etc**/**uucp**/**Sysfiles** pour spécifier d'autres fichiers de configuration de Devices. Pour en savoir plus sur le fichier Devices, reportez–vous à Devices File Format for BNU dans le manuel *AIX Files Reference*. Pour en savoir plus sur le fichier Sysfiles, reportez–vous à Sysfiles File Format for BNU dans le manuel *AIX Files Reference*.

   De plus, si vous utilisez TCP/IP, vérifiez que le fichier /**etc**/**services** contient la ligne :

   ```
   uucp        540/tcp          uucpd
   ```

   Sinon, ajoutez-la.

5. Utilisez les informations concernant chaque système distant pour modifier le fichier **Systems** sur votre système. Aidez-vous des exemples commentés dans le fichier **Systems** pour effectuer votre configuration. Pour en savoir plus, reportez–vous à "BNU Systems File Format" dans le manuel *AIX Files Reference*. Si vous utilisez TCP/IP, assurez-vous que la table des noms d'hôte dans le fichier /**etc**/**hosts** comprend le nom de la machine distante à laquelle vous souhaitez vous connecter. Vous pouvez configurer le fichier /**etc**/**uucp**/**Sysfiles** pour spécifier d'autres fichiers de configuration de Systems. Pour en savoir plus, reportez–vous à Sysfiles File Format for BNU dans le manuel *AIX Files Reference*.

6. A partir des informations relatives aux unités et modems, vérifiez que le fichier **Dialers** de votre système contient une entrée pour chaque modem. Si vous utilisez des connexions TCP/IP et directes, vérifiez que les entrées correspondantes figurent dans le fichier. Pour en savoir plus, reportez–vous à Dialers File Format for BNU dans le manuel *AIX Files Reference*. Vous pouvez configurer le fichier /**etc**/**uucp**/**Sysfiles** pour spécifier d'autres fichiers de configuration de Dialers. Pour en savoir plus, reportez–vous à Sysfiles File Format for BNU dans le manuel *AIX Files Reference*.

7. Déterminez l'accessibilité de votre système pour chaque système distant appelé à communiquer avec vous. Définissez les entrées correspondantes pour chaque système et nom de connexion dans le fichier **Permissions**. Pour en savoir plus, reportez–vous à Permissions File Format for BNU dans le manuel *AIX Files Reference*.

8. Exécutez la commande **uucheck** pour vérifier que tout est en place :

   ```
   /usr/sbin/uucp/uucheck -v
   ```

   La commande **uucheck** vérifie que les répertoires, programmes et fichiers de support sont correctement définis et que les entrées du fichier **Permissions** sont cohérentes. Si la commande **uucheck** signale une erreur, corrigez–la.

9. Vous pouvez demander le contrôle automatique des opérations BNU et l'appel automatique des systèmes distants.

Contrôle automatique de BNU

Prérequis

- Exécutez les étapes décrites à la section "Configuration de BNU", page 8-10.
- Vous devez être utilisateur racine pour éditer le fichier /**var**/**spool**/**cron**/**crontabs**/**uucp**.

Procédure

BNU fait appel au démon **cron** pour lancer les démons BNU et contrôler l'activité BNU. Le démon **cron** lit les instructions du fichier /**var**/**spool**/**cron**/**crontabs**/**uucp** sur le lancement des procédures BNU.

1. Connectez-vous en tant qu'utilisateur racine.
2. Modifiez le fichier /**var**/**spool**/**cron**/**crontabs**/**uucp** à l'aide d'un éditeur de texte ASCII.

3. Enlevez les marques de commentaire des lignes sur les procédures de maintenance BNU, **uudemon.admin** et **uudemon.cleanup**. Vous pouvez modifier à votre guise la fréquence d'exécution de ces procédures sur votre système. Toutefois, il est conseillé d'exécuter **uudemon.admin** au moins une fois par jour et **uudemon.cleanup** au moins une fois par semaine.
4. Vous disposez du fichier **crontabs**/**uucp** pour programmer d'autres commandes de maintenance BNU, telles que **uulog**, `uuclean` ou **uucleanup**. Le fichier **crontabs**/**uucp** vous permet également d'indiquer au démon **cron** de planifier le lancement des démons **uucico**, **uuxqt** ou **uusched** par `cron`.

Appel automatique BNU des systèmes distants

Prérequis

1. Exécutez les étapes décrites à la section "Configuration de BNU", page 8-10.
2. Vous devez être utilisateur racine pour éditer les fichiers **/var/spool/cron/crontabs/uucp** et **/etc/uucp/Poll**.

Procédure

Pour permettre à BNU de solliciter des systèmes distants pour des travaux, dressez la liste de ces systèmes dans le fichier **/etc/uucp/Poll**. Exécutez en outre périodiquement les commandes **uudemon.hour** et **uudemon.poll**.

1. Décidez des systèmes distants à solliciter automatiquement. Décidez de la fréquence de leur sollicitation. Indiquez chaque fréquence (au moins une fois par jour) dans le fichier **Poll**.
2. Connectez-vous en tant qu'utilisateur racine.
3. Modifiez le fichier **Poll** à l'aide d'un éditeur de texte ASCII ou de la commande **uucpadm**. Ajoutez une entrée pour chaque système à solliciter.

   Remarque : Les systèmes répertoriés dans le fichier **Poll** doivent également figurer dans le fichier **/etc/uucp/Systems**.
4. Modifiez le fichier **/var/spool/cron/crontabs/uucp** à l'aide d'un éditeur de texte ASCII. Enlevez les marques de commentaire (#) des lignes qui exécutent les commandes **uudemon.hour** et **uudemon.poll**. Vous pouvez modifier le moment d'exécution de ces commandes. Veillez toutefois à programmer la commande **uudemon.poll** environ cinq minutes *avant* la commande **uudemon.hour**.

BNU sollicitera automatiquement les systèmes répertoriés dans le fichier **Poll** aux moments spécifiés.

Fichier /etc/uucp/Systems

Les systèmes distants accessibles via les commandes BNU sont identifiés à l'installation du programme BNU. Il figurent dans les fichiers **/etc/uucp/Systems**. Le fichier **/etc/uucp/Systems** est le fichier **Systems** par défaut. L'administrateur système peut en définir d'autres dans le fichier **/etc/uucp/Sysfiles**.

Chaque entrée de fichier **Systems** comprend :

- le nom du système distant,
- les créneaux horaires pendant lesquels le système distant est accessible,
- le type de liaison (directe ou par modem),
- la vitesse de transmission par liaison,
- les informations requises pour la connexion au système distant.

Chaque entrée d'un fichier **Systems** représente un système distant. Pour établir la communication, le système distant doit être répertorié dans le fichier **Systems** local. Un fichier **Systems** doit être installé sur chaque système exploitant BNU. Normalement, seul l'utilisateur racine est habilité à lire les fichiers **Systems**. Tout utilisateur peut toutefois afficher la liste des systèmes BNU distants, via la commande **uuname**.

Édition du fichier Devices pour connexion câblée

Prérequis

Vous devez être utilisateur racine pour éditer le fichier /**etc**/**uucp**/**Devices** ou tout autre fichier déclaré comme fichier **Devices** dans /**etc**/**uucp**/**Sysfiles**.

Création d'une entrée de nom de système

Pour définir une connexion câblée, avec un port et un système distant, créez une entrée comme suit :

1. Spécifiez, dans le champ *Type* (seconde ligne), le nom du système distant auquel connecter la machine locale via la ligne câblée.
2. Spécifiez, dans le champ *Line* des deux lignes de l'entrée, le nom de l'unité pour la connexion câblée utilisée sur votre site.
3. Insérez un tiret (`-`) de réserve dans le champ *Line2* sur les deux lignes de l'entrée.
4. Indiquez dans le champ *Class,* sur les deux lignes de l'entrée, le débit de transmission pour la connexion câblée utilisée sur votre site.
5. Entrez `direct` (en minuscules) dans le champ *Dialer-Token Pairs* sur les deux lignes de l'entrée.

Complétez ainsi le fichier **Devices** jusqu'à ce que toutes les unités câblées reliant le système local à un système distant soient répertoriées.

Création d'une entrée directe

Pour définir une connexion câblée entre deux systèmes utilisant une connexion série asynchrone permanente, créez une entrée d'une ligne comme suit :

1. Entrez le nom du système dans le premier champ (*Type*).
2. Entrez le nom de l'unité tty dans le second champ (*Line*).
3. Insérez un tiret (`-`) de réserve dans le troisième champ (*Line2*).
4. Indiquez dans le quatrième champ (*Class*), le débit de transmission pour la connexion câblée utilisée sur votre site.
5. Entrez `direct` (en minuscules) dans le cinquième champ (*Dialer–Token Pairs*).

Complétez ainsi le fichier **Devices** jusqu'à ce que toutes les unités câblées reliant le système local à un système distant soient répertoriées.

Édition du fichier Devices pour connexion automatique

Prérequis

Vous devez être utilisateur racine pour éditer le fichier /**etc**/**uucp**/**Devices** ou tout autre fichier déclaré comme fichier **Devices** dans /**etc**/**uucp**/**Sysfiles**.

Procédure

Dans les entrées de connexion téléphonique, le champ *Type* est spécifié comme une unité ACU (automatic calling unit). Indiquez ACU dans le champ *Type* dans toutes les connexions à distance établie via une ligne téléphonique. Pour définir les entrées du fichier **Device** pour connexions automatiques, créez une entrée d'une ligne pour chaque modem, comme suit :

1. Entrez `ACU` dans le premier champ (*Type*).

2. Le deuxième champ (*Line*) contient le nom de l'unité raccordée au modem. Entrez le nom qui convient pour votre site.
3. Entrez un `-` (tiret) de réserve dans le troisième champ (*Line2*), sauf si le numéroteur automatique est un numéroteur 801 standard. Si le numéroteur est un 801 standard, entrez `801`.
4. Indiquez dans le quatrième champ (*Class*), le débit en bauds correspondant à votre modem et votre ligne (300, 1200, 2400 ou plus, selon le modem) ou la classe du modem utilisé (par exemple, D2400).

   Remarque : Si le modem est exploitable à plusieurs débits, créez une entrée distincte pour chaque débit dans le fichier **Devices**. Si le modem peut être utilisé à n'importe quel débit, indiquez `Any` dans le champ *Class.*
5. Entrez le nom du modem dans la partie *Dialer* du cinquième champ (*Dialer Token Pair*). Si vous envisagez d'inclure des numéros d'appel complets dans le fichier **/etc/uucp/Systems** ou un fichier **Systems** spécifié dans **/etc/uucpSysfiles**, laissez la partie *Token* en blanc. (Un blanc indique au programme BNU d'utiliser l'option par défaut `\D`.) Si vous souhaitez utiliser les codes d'accès directs spécifiés dans le fichier **/etc/uucp/Dialcodes**, entrez l'option `\T`.

Complétez ainsi le fichier **Devices** jusqu'à répertorier toutes les unités câblées reliant le système local à un système distant via une ligne téléphonique ou un modem.

Édition du fichier Devices pour TCP/IP

Prérequis

Vous devez être utilisateur racine pour éditer le fichier **/etc/uucp/Devices** ou tout autre fichier déclaré comme fichier **Devices** dans **/etc/uucp/Sysfiles**.

Procédure

Si vous utilisez TCP/IP, insérez l'entrée TCP/IP correspondante dans le fichier **Devices**. Pour configurer le fichier pour l'utiliser avec le système TCP/IP, insérez la ligne suivante dans le fichier **Devices** :

```
TCP - - - TCP
```

Maintenance de BNU

Pour que BNU fonctionne correctement, vous devez effectuer un certain nombre de tâches de maintenance. Pour maintenir BNU :

- Consultez et supprimez régulièrement les fichiers journaux.
- Utilisez les commandes **uuq** et **uustat** pour contrôler les files d'attente BNU et vous assurer que les travaux sont correctement transférés aux systèmes distants.
- Planifiez les commandes automatiques qui sollicitent les systèmes distants pour les travaux, qui réexpédient les fichiers non envoyés aux utilisateurs et qui vous informent périodiquement de l'état de BNU.
- Effectuez régulièrement une mise à jour des fichiers de configuration pour intégrer les modifications apportées à votre système.

Par ailleurs, tenez-vous informé, auprès des administrateurs de systèmes distants, des modifications apportées à leurs systèmes, susceptibles d'influer sur votre configuration. Par exemple, si le superviseur de `venus` modifie votre mot de passe système, vous devez le déclarer dans le fichier **/etc/uucp/Systems** (ou dans le fichier Systems correspondant spécifié par **/etc/uucp/Sysfiles**) avant de vous connecter à `venus`.

Reportez-vous à Fichiers, commandes et répertoires BNU, page 8-39, pour connaître les commandes de maintenance de BNU.

Fichiers journaux BNU

BNU crée des fichiers journaux et des fichiers d'erreurs pour le suivi de vos activités. Veillez à consulter et supprimer ces fichiers régulièrement afin d'éviter tout encombrement de l'espace système. BNU offre plusieurs commandes pour le vidage des journaux :

- **uulog**
- **uuclean**
- **uucleanup**
- **uudemon.cleanu**

Exécutez ces commandes manuellement ou déclarez-les dans le fichier **/var/spool/cron/crontabs/uucp** pour que le démon **cron** les exécute automatiquement.

Fichiers journaux des répertoires .Log et .Old

BNU crée des fichiers journaux individuels dans le répertoire **/var/spool/uucp/.Log**. BNU crée ces journaux pour chaque système distant accessible, via la commande **uucp**, **uuto** ou **uux**. BNU consigne dans le fichier journal correspondant l'état de chaque transaction, chaque fois qu'un utilisateur du système fait appel à BNU. Lorsque plusieurs processus BNU sont exécutés, le système ne peut accéder au fichier journal. L'état est alors consigné dans un fichier séparé et suffixé par **.LOG**.

La commande **uulog** fournit un récapitulatif, par utilisateur ou par système, des requêtes **uucp** ou **uux**. La commande **uulog** affiche les fichiers. Mais vous pouvez également demander à BNU de fusionner automatiquement les fichiers journaux dans un fichier principal. L'opération, appelée *compactage*, exécutée par la commande **uudemon.cleanu**, est généralement lancée par le démon **cron**.

Le démon **cron** exécute **uudemon.cleanu**. La commande **uudemon.cleanu** regroupe les fichiers journaux **uucico** et **uuxqt** sur le système local et les stocke dans le répertoire **/var/spool/uucp/.Old**. Simultanément, la commande supprime les anciens fichiers journaux précédemment stockés dans le répertoire **.Old**. Par défaut, la commande **uudemon.cleanu** sauvegarde les fichiers journaux datant de deux jours.

En cas d'encombrement de l'espace de stockage, réduisez la durée de conservation (nombre de jours) des fichiers journaux. Pour pister les transactions BNU sur une plus longue période, augmentez cette durée. Il est possible de changer le délai de sauvegarde par défaut des fichiers journaux : pour ce faire, modifiez la procédure shell pour la commande **uudemon.cleanu**. Ce script, stocké dans le répertoire **/usr/sbin/uucp,** peut être modifié avec des droits d'utilisateur racine.

Autres fichiers journaux BNU

BNU recueille également des informations qu'il stocke dans le répertoire **/var/spool/uucp/.Admin**. Ce répertoire contient les fichiers **errors**, **xferstats**, **Foreign** et **audit**. Consultez et supprimez régulièrement ces fichiers pour ne pas occuper inutilement de l'espace de stockage. BNU crée chaque fichier quand nécessaire.

Lorsqu'un système contacte le vôtre avec la mise au point **uucico** activée, il fait appel au démon **uucico** sur votre système avec mise au point activée. Les messages de mise au point générés par le démon sur le système local sont stockés dans le fichier **audit**. Ce fichier peut être relativement volumineux. Consultez souvent le fichier **audit** et supprimez–le.

Le fichier **errors** enregistre les erreurs détectées par le démon **uucico**. Consultez-le pour corriger les incidents relevés (droits d'accès erronés sur les fichiers de travail BNU par exemple).

Le fichier **xferstats** contient les informations d'état sur tout transfert de fichiers. Consultez-le régulièrement et supprimez-le.

Le fichier **Foreign** joue un rôle déterminant dans la sécurité du système. Chaque fois qu'un système inconnu tente de se connecter au système local, BNU appelle la procédure shell **remote.unknown**. Cette procédure shell consigne la tentative dans le fichier **Foreign**. Le fichier **Foreign** contient le nom de tous les systèmes qui ont tenté en vain de se connecter au système local. Si un système a effectué plusieurs tentatives d'accès, vous pouvez envisager d'autoriser son accès.

Fichiers journaux au niveau système utilisés par BNU

Nombre de processus BNU requièrent des droits racine et génèrent de multiples entrées dans le fichier journal **/var/spool/sulog**. De même, la planification des tâches BNU via le démon **cron** génère diverses entrées dans le fichier **/var/spool/cron/log**. Consultez et videz régulièrement ces fichiers.

Commandes de maintenance BNU

BNU regroupe diverses commandes destinées à surveiller les activités BNU et à nettoyer les fichiers et répertoires BNU.

Commandes de nettoyage

BNU propose trois commandes pour nettoyer les répertoires et supprimer les fichiers non envoyés :

uuclean	Supprime, dans les répertoires administratifs BNU, les fichiers datant de plus d'un certain nombre d'heures. Spécifiez, via la commande **uuclean** le répertoire à vider ou le type de fichier à supprimer. Vous pouvez également demander sur la commande prévienne les propriétaires des fichiers supprimés. La commande **uuclean** est l'équivalent Berkeley de la commande **uucleanup.**
uucleanup	Exécute des fonctions semblables à celles de la commande **uuclean**. Une différence : la commande **uucleanup** vérifie l'âge des fichiers en *jours* et non en heures. Utilisez la commande **uucleanup** pour avertir les utilisateurs dont les fichiers n'ont pas été transférés et sont maintenus en file d'attente. La commande **uucleanup** permet également de supprimer des fichiers relatifs à un système distant particulier.
uudemon.cleanu	Procédure shell qui émet les commandes **uulog** et **`uucleanup`** pour compresser les fichiers journaux et fichiers de travail BNU datant de plus de trois jours. La commande **uudemon.cleanu** est exécutée par le démon **cron**.

Commandes de contrôle d'état

BNU propose également des commandes pour contrôler l'état des transferts et des fichiers journaux :

uuq	Affiche les travaux actuellement en file attente BNU. Lancez la commande **uuq** pour afficher l'état d'un travail particulier ou de tous les travaux. En session racine, vous pouvez utiliser la commande **uuq** pour supprimer un travail de la file d'attente.
uustat	Remplit des fonctions similaires à la commande **`uuq`** mais présente les informations sous un format différent. Utilisez la commande **uustat** pour contrôler l'état des travaux et supprimer vos propres travaux. En session racine, vous pouvez également l'utiliser pour supprimer des travaux appartenant à d'autres utilisateurs.
uulog	Fournit un récapitulatif, par utilisateur ou par système, des requêtes **uucp** et **`uux.`** La commande **uulog** affiche le nom des fichiers. Reportez-vous à "Fichiers journaux BNU", page 8-18.
uupoll	Force une interrogation d'un système distant. Cette opération est utile lorsqu'un travail destiné à ce système est en attente et doit être transféré, alors que l'appel automatique du système n'a pas encore été programmé.
uusnap	Affiche un récapitulatif succinct de l'état de BNU. Pour chaque système distant, cette commande affiche le nombre de fichiers en attente de transfert. Elle n'indique toutefois pas la durée de l'attente. La commande **uusnap** est l'équivalent Berkeley de la commande **uustat**.

Procédures shell

BNU est livré avec deux procédures shell dédiées à la maintenance :

uudemon.cleanu	Reportez-vous à "Commandes de nettoyage", page 8-20.
uudemon.admin	Lance la commande **uustat**. La commande **uustat** fournit l'état des travaux BNU. Elle transmet le résultat sous forme de courrier à l'ID de connexion uucp. Vous pouvez modifier la procédure shell **uudemon.admin** pour réacheminer le courrier, ou utiliser un programme de messagerie pour réacheminer le courrier destiné à un ID de connexion uucp vers l'administrateur BNU.

Ces procédures shell sont stockées dans le répertoire **/usr/sbin/uucp**. Si vous souhaitez modifier les procédures, copiez-les et modifiez la copie. Lancez les procédures à partir de la ligne de commande ou programmez leur exécution par le démon **cron**.

Pour exécuter automatiquement les commandes **uudemon.cleanu** et **uudemon.admin**, supprimez les marques de commentaire (#) au début des lignes correspondantes, dans le fichier **/var/spool/cron/crontabs/uucp**.

Contrôle d'une connexion distante BNU

Prérequis

- Le programme BNU doit être installé sur votre système.
- Une liaison (par câble, modem ou TCP/IP) doit relier votre système au système distant.
- Les fichiers de configuration BNU **Systems**, **Permissions**, **Devices, Dialers** (et **Sysfiles**, le cas échéant) doivent autoriser la communication entre votre système et le système distant.

Remarque : Vous devez être utilisateur racine pour modifier les fichiers de configuration BNU.

Procédure

La commande **Uutry** aide à contrôler le processus démon **uucico** en cas d'incident de transfert de fichier signalé par les utilisateurs de votre site.

1. Lancez la commande **uustat** pour déterminer l'état de tous les travaux de transfert actuellement en file d'attente :

   ```
   uustat -q
   ```

   Le système affiche un compte rendu d'état comme suit :

   ```
   venus 3C (2) 05/09-11:02 CAN'T ACCESS DEVICE
   hera 1C 05/09-11:12 SUCCESSFUL
   merlin 2C 5/09-10:54 NO DEVICES AVAILABLE
   ```

   Ce compte rendu indique que trois fichiers de commande (**C.***) destinés au système distant `venus` sont en file d'attente depuis deux jours. Ce délai peut être dû à différentes causes. Par exemple, le système `venus` a été arrêté pour maintenance, le modem est éteint, etc.

2. Avant de poursuivre plus avant les procédures de résolution d'incident, lancez la commande **Uutry** pour vérifier que votre système local est en mesure de contacter le système `venus` :

   ```
   /usr/sbin/uucp/Uutry -r venus
   ```

   Cette commande lance le démon **uucico** avec un niveau moyen de mise au point et sans tenir compte du délai imparti par défaut pour les tentatives. La commande **Uutry** dirige le résultat de mise au point vers le fichier temporaire `/tmp/venus`.

3. Si votre système local parvient à établir la connexion avec le système `venus`, la sortie de mise au point contient de nombreuses informations. C'est la dernière ligne du script qui présente le plus d'intérêt :

   ```
   Conversation Complete: Status SUCCEEDED
   ```

   Si la connexion est établie, l'incident de transfert vers le fichier temporaire est supposé résolu. Relancez la commande **`uustat`** pour vous assurer que les fichiers stockés dans le répertoire de spoulage sont effectivement transférés vers le système distant. Sinon, exécutez les étapes décrites à la section `"Contrôle du transfert de fichier BNU", page 8-22`, pour tester le transfert entre votre système et le système distant.

4. Si le système local ne parvient pas à contacter le système distant, le résultat de mise au point généré par la commande **Uutry** fournit des informations sous la forme ci-dessous (la présentation peut varier) :

   ```
   mchFind called (venus)
   conn (venus)
   getto ret -1
   Call Failed: CAN'T ACCESS DEVICE
   exit code 101
   Conversation Complete: Status FAILED
   ```

   Vérifiez les connexions physiques entre le système local et le système distant. Vérifiez la mise sous tension de la machine distante, le câblage, l'activation adéquate des ports sur les deux systèmes et le fonctionnement du modem.

   Si les connexions physiques sont correctes et fiables, examinez les fichiers de configuration des deux systèmes :

   – Contrôlez les entrées des fichiers **Devices**, **Systems**,**Permissions** (et, le cas échéant, **Sysfiles**) dans le répertoire **/etc/uucp.**

   – Dans le cas d'une liaison par modem, vérifiez que le fichier **/etc/uucp/Dialers** (ou tout autre fichier déclaré dans **/etc/uucp/Sysfiles**) contient l'entrée adéquate. Si vous utilisez des codes d'accès directs, vérifiez-les dans le fichier **/etc/uucp/Dialcodes**.

   – Dans le cas d'une liaison TCP/IP, vérifiez que le démon **uucpd** peut être exécuté sur le système distant et que les fichiers de configuration contiennent les entrées TCP correctes.

5. Une fois les connexions physiques et les fichiers de configuration contrôlés, relancez la commande **Uutry.** Si le résultat de mise au point signale toujours l'échec de la connexion, contactez le support technique. Sauvegardez le résultat de la commande **Uutry**. Il pourra être utile pour diagnostiquer l'incident.

Contrôle du transfert de fichier BNU

Prérequis

1. Le programme BNU doit être installé et configuré sur votre système.
2. Etablissez une connexion au système distant comme indiqué à "Contrôle d'une connexion distante BNU", page 8-21.

Contrôle du transfert de fichier

Cette procédure permet de contrôler un transfert de fichier vers un système distant.
Ce contrôle est utile lorsque les transferts de fichiers vers un système distant n'aboutissent pas pour une raison inconnue. Les informations de mise au point générées par le démon **uucico** (appelé par la commande **Uutry**) peuvent servir à identifier l'incident.

Pour effectuer le contrôle, utilisez la commande **Uutry** comme suit :

1. Préparez un fichier au transfert en exécutant la commande **uucp** assortie de l'indicateur **–r** :

   ```
   uucp -r test1 venus!~/test2
   ```

   -r demande au programme BNU de placer le fichier `test1` dans la file d'attente *sans* lancer le démon **uucico**.

2. Exécutez la commande **Uutry** assortie de l'indicateur **–r** pour lancer le démon **uucico** avec la mise au point activée :

   ```
   /usr/sbin/uucp/Uutry -r venus
   ```

   Cette commande demande au démon **uucico** de contacter le système distant `venus` sans tenir compte du délai imparti par défaut pour les tentatives. Le démon contacte alors le système `venus`, établit la connexion et transfère le fichier. Dans le même temps, la commande **Uutry** génère une sortie de mise au point qui vous permettra de contrôler le processus **uucico**. Appuyez sur la combinaison de touches d'interruption pour arrêter la sortie de mise au point et revenir à l'invite de commande.

   La commande **Uutry** enregistre également la sortie de mise au point dans le fichier /**tmp**/*SystemName*. Si vous interrompez la sortie de mise au point avant l'établissement de la connexion, vous pourrez parcourir les pages du fichier de sortie pour visualiser l'aboutissement de la connexion.

Résolution des incidents BNU

Des messages d'erreur BNU peuvent être liés à une phase particulière des échanges. Utilisez le schéma de flux BNU et le descriptif des erreurs ci-après pour diagnostiquer les incidents. Certains messages ne sont pas émis par BNU mais sont néanmoins cités en cas d'utilisation d'une autre version d'UUCP.

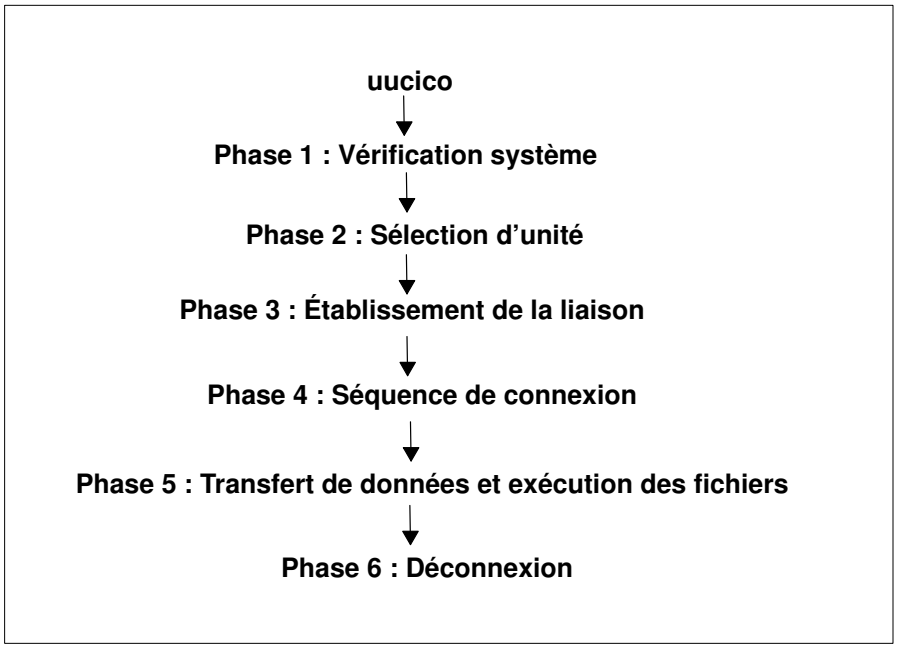


Schéma de flux BNU

Messages d'état de la phase 1

`Assert Error`	Problèmes au niveau de l'unité du système local. Recherchez les causes possibles dans le compte rendu d'erreur, à l'aide de la commande **errpt –a | pg**.
`System not in Systems`	Le nom de système distant indiqué ne figure pas dans les fichiers **Systems**. BNU s'arrête. Lancez la commande **uuname** pour vérifier ce nom.
`Wrong time to call`	Des restrictions définies sur le système **Systems** limitent les plages horaires où les appels sortants sont autorisés. BNU renouvelle la tentative jusqu'à ce que l'heure admise soit atteinte. Vérifiez le fichier **Systems**.
`Callback required`	L'utilisation du réseau est limitée pour des questions de sécurité ou d'économie. L'accès est refusé à ce moment précis.
`Cannot call No Call`	BNU a récemment tenté sans succès d'appeler le système distant. Il n'effectue pas immédiatement de nouvelle tentative. Ce message peut également être dû à un ancien fichier d'état du système qui empêche **uucico** d'effectuer une nouvelle tentative.

Messages d'état de la phase 2

`Dialer Script Failed`	Votre script du fichier **Dialers** n'a pas abouti.
`No Device Available Can't Access Device`	Le modem ou la ligne téléphonique sortante de votre système est occupé. Vérifiez l'entrée relative à l'unité dans le fichier **Systems**. Examinez les fichiers **Devices** et **Dialers** : les unités logiques doivent avoir des unités physiques associées. Le fichier /**etc/uucp/Sysfiles** peut spécifier un autre fichier **Systems**, **Devices** ou **Dialers** qui n'a pas été correctement configuré. L'unité est-elle utilisée par d'autres programmes ? Vérifiez le verrouillage des ports dans le répertoire /**etc/locks**. Si un fichier de verrouillage existe (par exemple, **LCK..TTY0**), vérifiez que le processus identifié par le numéro dans le fichier de verrouillage est toujours actif. Dans la négative, supprimez-le (par exemple, `rm /etc/locks/LCK..TTY0`). Vérifiez également les droits d'accès au port.
`Dial Failed Failed (call to system)`	Votre système est parvenu à contacter un autre système mais ce dernier ne répond pas. Il se peut également que les fichiers **Devices** comportent une anomalie. Entrez la commande `uucico –r1 –x6 –s` *`SystemName`*. Il est possible que BNU attende une chaîne qu'il ne reçoit pas. Effectuez la connexion manuellement pour déterminer ce qui doit être ajouté à l'entrée de fichiers **Systems** pour satisfaire la requête. Veillez à respecter les éventuels délais (par exemple, si la séquence d'appel d'un modem est associée à un délai). D'autres causes peuvent être à l'origine du message : port occupé, numéro composé erroné, BNU non propriétaire du port, etc.
`OK Auto Dial`	Messages d'information ne signalant aucune erreur.

Messages d'état de la phase 3

`Handshake Failed (LCK)`	L'unité est en cours d'utilisation par un autre utilisateur. Le processus n'a pas pu créer de fichier **LCK**. Parfois, les fichiers **LCK** doivent être supprimés manuellement par l'administrateur. Après un certain nombre de tentatives, faites appel à l'administrateur système. Vérifiez si un autre processus mobilise le port (par exemple, une autre instance **uucico**).
`Login Failed`	Échec d'établissement de liaison du fait d'une connexion défaillante ou d'une machine trop lente.
`Timeout`	Le système distant n'a pas répondu dans les délais impartis. Il se peut également qu'il y ait un problème avec le script chat.
`Succeeded (Call to System)`	L'appel a abouti.
`BNU (continued)`	Messages d'information ne signalant aucune erreur.

Messages d'état de la phase 4

`Startup Failed Remote reject after login`	Après connexion, **uucico** est lancé sur le système distant. Ces messages s'affichent lorsqu'un incident se produit en début de conversation entre les deux systèmes. Il se peut également que la connexion n'ait pas été établie sur le compte BNU adéquat ou que la mise en liaison initiale ("handshaking") ait échoué.
`Wrong machine name`	Vous avez mal appelé une machine ou son nom a changé.
`Bad login/machine combination`	La connexion au système distant a échoué. Plusieurs causes possibles : numéro de téléphone incorrect, nom de connexion ou mot de passe incorrect, erreur dans le script chat, etc.
`Remote has a LCK file for me`	Les deux systèmes ont tenté simultanément de s'appeler. La requête locale échoue temporairement.

`OK` `Talking`	Messages d'information ne signalant aucune erreur.
`LOGIN:` `PASSWORD:`	Si l'invite de connexion ou de mot de passe figure entièrement en lettres majuscules, le modem fonctionne en mode écho (E1 sur compatibles Hayes). Dans ce cas, le modem envoie (ou renvoie) un code RING à votre système, à la réception d'un appel entrant. La commande **getty** reçoit la chaîne et passe l'invite de connexion `login:` ou de mot de passe `password:` en lettres majuscules. Désactivez (**off**) le mode écho sur le modem (via `ATE0` pour les compatibles Hayes). **Remarque :** Après avoir effectué cette modification, vous devez utiliser `ATE1` dans le script chat de vos fichiers **Dialers**, faute de quoi vous n'obtiendrez pas la réponse `OK` de la part de votre modem. Si le port distant est configuré pour `delay` ou `getty -r` et que le script chat attend que vous appuyiez sur une touche, les ports configurés pour `delay` attendent l'entrée d'un ou plusieurs retours chariot avant de poursuivre la procédure de connexion. Insérez en début du script chat, côté système appelant, la ligne : `"" \r\d\r\d\r\d\r in:--in: ...` Cette ligne signifie : aucune touche attendue, envoyer les codes retour (return), délai (delay), retour, délai, retour, délai, retour.

Messages d'état de la phase 5

`Alarm`	**uucico** rencontre des difficultés de connexion. La connexion est défaillante ou "xon/xoff" est activé sur le modem.
`Remote access to path/file denied copy (failed)`	Messages signalant une anomalie relative aux droits d'accès. Vérifiez les droits associés aux fichiers et aux chemins.
`Bad read`	Espace insuffisant sur le système distant, probablement dans la zone de spoulage, ou lecture ou écriture sur l'unité impossible pour **uucico.**
`Conversation failed`	La détection de porteuse du modem a été perdue. Le modem a été mis hors tension, le câble est desserré ou déconnecté, le système distant est arrêté ou bloqué. Ou alors la liaison téléphonique est interrompue.
`Requested Copy (succeeded)`	Messages d'information ne signalant aucune erreur.

Messages d'état de la phase 6

`OK (Conversation Complete)`	Le système distant refuse la demande de raccrochage et inverse les rôles (il a un travail à soumettre au système local). Dès que les deux **uucico** n'ont plus de travaux à soumettre, ils raccrochent.
`Conversation succeeded`	Message d'information ne signalant aucune erreur.

Résolution des incidents de connexion BNU via le démon uucico

Prérequis

- BNU doit être installé sur votre système.
- Une liaison (par câble, modem ou TCP/IP) doit relier votre système au système distant.
- Les fichiers de configuration BNU **Systems**, **Permissions**, **Devices, Dialers** (et **Sysfiles**, le cas échéant) doivent autoriser la communication entre votre système et le système distant.

  Remarque : Vous devez être utilisateur racine pour modifier les fichiers de configuration BNU.
- Vous devez être utilisateur racine pour appeler le démon **uucico** en mode mise au point.

Procédure

1. Pour obtenir des informations de mise au point sur une connexion défaillante entre systèmes local et distant, lancez le démon **uucico** assorti de l'indicateur **–x** :

   ```
   /usr/sbin/uucp/uucico -r 1 -s venus -x 9
   ```

   `-r 1` indique le mode maître ou appelant ; `-s venus`, le nom du système distant et `-x 9`, le niveau de mise au point maximal (informations de mise au point les plus détaillées).

2. Si l'entrée expect-send du fichier Systems au format **/etc/uucp/Systems** est :

   ```
   venus Any venus 1200 - "" \n in:--in: uucp1 word:
    mirror
   ```

   Le démon **uucico** connecte le système local au système distant `venus`. La mise au point renvoie un résultat du type :

   ```
   expect: ""
   got it
   sendthem (^J^M)
   expect (in:)^
   M^Jlogin:got it
   sendthem (uucp1^M)
   expect (word:)^
   M^JPassword:got it
   sendthem (mirror^M)
   imsg >^M^J^PShere^@Login Successful: System=venus
   ```

   où :

   `expect: ""`
   : Indique que le système local n'attend pas d'informations de la part du système distant.

   `got it`
   : Accusé de réception du message.

   `sendthem (^J^M)`
   : Indique que le système local va envoyer au système distant un retour chariot et un caractère de ligne suivante.

   `expect (in:)`
   : Indique que le système local attend du système distant une invite de connexion, terminée par la chaîne `in:`.

   `^M^Jlogin:got it`
   : Confirme que le système local va recevoir l'invite de connexion distante.

`sendthem (uucp1^M)`

Indique que le système va envoyer l'ID de connexion `uucp1` au système distant.

`expect (word:)`

Indique que le système local attend du système distant une invite de connexion, terminée par le mot `word:`.

`^M^JPassword:got it`

Confirme que le système local va recevoir l'invite de connexion distante.

`sendthem (mirror^M)`

Indique que le système local va envoyer le mot de passe pour l'ID de connexion `uucp1` au système distant.

`imsg >^M^J^PShere^@Login Successful: System=venus`

Confirme la connexion du système local au système distant `venus`.

Remarques :

1. La sortie de mise au point "expect-send" générée par la commande **uucico** peut provenir d'informations issues du fichier **/etc/uucp/Dialers** ou du fichier **/etc/uucp/Systems**. Les informations de communication sur le modem sont extraites du fichier **Dialers**, et celles sur le système distant, du fichier **Systems**. (Notez que **/etc/uucp/Systems** et **/etc/uucp/Dialers** sont les fichiers de configuration par défaut de BNU. D'autres fichiers peuvent être spécifiés dans **/etc/uucp/Sysfiles** pour jouer le même rôle.)
2. Pour établir une connexion avec un système distant, vous devez connaître la séquence de connexion à ce système.

Communication avec des systèmes UNIX via la commande tip

Utilisez la commande **tip** pour contacter un système connecté et exploité sous UNIX. La commande **tip**, installée avec BNU, peut utiliser les mêmes connexions asynchrones que celles de BNU.

La commande **tip** a recours à des variables, séquences d'échappement et indicateurs. Les indicateurs peuvent être entrés à partir de la ligne de commande. Les séquences d'échappement peuvent être utilisées sur une connexion à distance pour lancer, réacheminer et arrêter des transferts de fichier et se brancher sur un sous-shell.

Variables de tip

Les variables de la commande **tip** définissent des paramètres tels que le caractère de fin de ligne, le signal d'interruption et le mode de transfert de fichier. Les variables peuvent être initialisées au moment de l'exécution via un fichier **.tiprc**. Les variables peuvent également être modifiées pendant l'exécution via le signal d'échappement **~s**. Certaines variables, tel le caractère de fin de ligne, peuvent être définies pour un système particulier, via l'entrée propre à ce système dans le fichier **remote**.

La commande **tip** lit trois fichiers (**phones**, **remote** et **.tiprc**) pour déterminer la configuration initiale de ses variables. Le fichier **.tiprc** doit toujours résider dans le répertoire personnel de l'utilisateur. Le nom et l'implantation des fichiers **remote** et **phones** peuvent varier. Pour déterminer le nom des fichiers **remote** et **phones**, vous disposez des variables d'environnement :

PHONES	Fichier téléphonique de l'utilisateur. Ce fichier peut avoir n'importe quel nom valide et doit respecter le format du fichier **/usr/lib/phones–file**. Le fichier par défaut est **etc/phones**. Le cas échéant, le fichier spécifié avec la variable **PHONES** remplace le fichier **/etc/phones**.
REMOTE	Fichier de définition du système distant de l'utilisateur. Ce fichier peut avoir n'importe quel nom valide et doit respecter le format du fichier **/usr/lib/remote–file**. Le fichier par défaut est **/etc/remote**. Le cas échéant, le fichier spécifié avec la variable **REMOTE** remplace le fichier **/etc/remote**.

Une variable d'environnement n'est applicable que définie avant le lancement de la commande **tip**. Vous pouvez également redéfinir le nom des fichiers **phones** et **remote** à l'aide de la commande **tip** et des variables **phones** et **remote** dans le fichier **.tiprc**.

Remarque : La commande **tip** ne lit que le *dernier* fichier **remote** ou **phones** spécifié. Ainsi, si vous spécifiez un fichier **remote** ou **phones** avec une variable, le nouveau fichier remplace ceux spécifiés précédemment.

La commande **tip** lit les variables dans l'ordre suivant :

1. La commande vérifie la valeur des variables d'environnement **PHONES** et **REMOTE** pour les fichiers à utiliser en tant que **phones** et **remote**.
2. La commande lit le fichier **.tiprc** et attribue ensuite une valeur aux variables. Si la variable **phones** ou **remote** est définie dans le fichier **.tiprc**, cette valeur prime sur celle de la variable d'environnement.
3. Lorsqu'une connexion à un système distant est lancée, la commande lit l'entrée du fichier **remote** pour ce système. La valeur de l'entrée du fichier **remote** prime sur celle définie dans le fichier **.tiprc**.
4. Si l'indicateur **-***débit_baud* est associé à la commande **tip**, le taux spécifié prime sur ceux définis précédemment.
5. La valeur attribuée à une variable via la séquence d'échappement **~s** prime sur toute valeur précédemment affectée à cette variable.

Remarque : Tout utilisateur de **tip** peut créer un fichier **.tiprc** et l'utiliser pour spécifier la valeur initiale de ces variables **tip**. Le fichier **.tiprc** doit être placé dans le répertoire **$HOME** de l'utilisateur.

Fichiers de configuration de tip

La commande **tip** ne permet la connexion à un système distant qu'une fois les fichiers /**etc**/**remote** et /**etc**/**phones** constitués.

/**etc**/**remote**	Définit les attributs des systèmes distants, tels que le port et le type d'unité à utiliser pour atteindre le système, de même que les signaux signifiant le début et la fin des transmissions.
/**etc**/**phones**	Répertorie les numéros d'appel pour contacter des systèmes distants via un modem.

Pour constituer l'un de ces fichiers, copiez un fichier-type, changez son nom et modifiez-le pour l'adapter à votre site. Des exemples de fichiers **remote** et **phones** sont fournis dans le module bos.net.uucp. Le fichier **remote** exemple est appelé /**usr**/**lib**/**remote–file**. Le fichier **phones** exemple est appelé /**usr**/**lib**/**phones–file**.

> **Remarque :** Vous devez être utilisateur racine pour créer des fichiers dans le répertoire /**usr**/**lib**.

Un utilisateur de **tip** peut également créer des fichiers **remote** et **phones** personnalisés. Un fichier **remote** doit respecter le format du fichier /**usr**/**lib**/**remote-file** et être spécifié avec la variable **remote** ou la variable d'environnement **REMOTE**. Un fichier **phones** doit respecter le format du fichier /**usr**/**lib**/**phones-file** et être spécifié avec la variable **phones** ou la variable d'environnement **PHONES**. Associer une de ces variables au fichier **phones** ou **remote** permet de le lire *à la place* (et non en plus) du fichier /**etc**/**phones** ou /**etc**/**remote**.

Les utilisateurs de **tip** peuvent combiner les fichiers **phones** et **remote**. Par exemple, un utilisateur peut lire le fichier **remote** par défaut, /**usr**/**lib**/**remote–file**, et utiliser un fichier **phones** personnel appelé avec la variable **phones**.

Fichiers de configuration BNU

BNU (Basic Network Utilities) utilise les fichiers de configuration suivants :

/etc/uucp	Contient tous les fichiers de configuration pour BNU.
/var/spool/uucppublic	Contient les fichiers qui ont été transférés.
/etc/uucp/Systems	Contient la liste des systèmes auxquels le programme **uucico** peut se connecter.
/etc/uucp/Devices	Définit le type, l'emplacement, la vitesse et autres paramètres de communication des unités pour plusieurs programmes d'appel de système. Seules les connexions sortantes utilisent ce fichier.
/etc/uucp/Permissions	Etablit un contrôle de sécurité, avec restrictions d'accès, pour les machines qui tentent de communiquer avec la vôtre.
/etc/uucp/Dialers	Spécifie les types de numéroteurs. Chaque numéroteur utilise un jeu de commandes spécifique pour appeler le modem. Les types de numéroteurs les plus courants sont `hayes`, `direct` et `TCP` (Transmission Control Protocol).
/etc/uucp/Dialcodes	Crée des noms normalisés pour remplacer certaines portions d'un numéro d'appel. Par exemple, si vous utilisez fréquemment le code d'une zone de San Francisco, créez l'entrée : `SF09,1415`.
/etc/uucp/Sysfiles	Permet à l'administrateur BNU de spécifier des fichiers remplaçant les fichiers de configuration BNU **/etc/uucp/Systems**, **/etc/uucp/Devices** et **/etc/uucp/Dialers.** La distinction est possible entre les fichiers destinés aux activités **uucico** et **cu** (**cu**, **ct**, **slattach**).
/usr/sbin/uucp/remote.unknown	Définit un script shell. Il est exécuté par BNU lorsqu'une machine distante non répertoriée dans la liste des machines autorisées tente de communiquer avec le système local.
/etc/uucp/Poll	Planifie l'interrogation des systèmes passants. Son format est similaire à celui du fichier **crontab**. La séquence d'appel observe le format : *nom_site*, tabulation et heures d'appel (0-23), séparés par des espaces.

Corrélation de fichiers

Fichier Systems :	`SystemName  Any  v32ibm  9600  555-1111`
Fichier Devices :	`v32ibm  tty0  -  Any  ibm  \D`
Fichier Dialers :	`ibm  =, -, #" \d ATSFI\r\c#OK#AFE1SD3L2MIC0SCI\r\c#OK...`

Exemple de configuration BNU pour connexion TCP/IP

Les fichiers suivants sont configurés pour une connexion TCP/IP (Transmission Control Protocol/Internet Protocol) entre les systèmes `zeus` et `hera`, où `zeus` est supposé être le système local et `hera` le système distant.

Entrées dans les fichiers du système local

Les fichiers contenant des entrées de connexion téléphonique sur le système local `venus` sont les suivants :

Fichier Systems

Pour que `zeus` puisse contacter `hera`, le fichier **Systems** sur `zeus` doit comporter la ligne :

```
hera Any TCP,t - - in:--in: uzeus word: birthday
```

Cette ligne indique que le système `zeus` peut appeler `hera` à tout moment via le protocole **t** pour communiquer avec le système `hera`. Le système `zeus` se connecte au système `hera` comme `uzeus` avec le mot de passe `birthday`.

Remarque : Le protocole **t** prend en charge le protocole **tcp**. Par conséquent, utilisez toujours le protocole **t** pour les communications BNU via des connexions TCP/IP. En revanche, le protocole **t** n'est pas admis avec une connexion par modem ou dont le champ *Type* est `ACU`.

BNU se fonde sur les champs *Type* et *Class* du fichier **Systems** pour déterminer l'unité adaptée à la connexion. Sur cette base, il recherche une entrée de type `TCP` dans le fichier **Devices**.

Fichier Devices

Un fichier **Devices** utilisé par **uucico** sur le système `zeus` doit comporter pour les connexions TCP/IP l'entrée :

```
TCP  -  -  -  TCP
```

Le type d'unité étant `TCP`, il n'y a pas d'entrées *Class*, *Line* ou *Line2*. De même, `TCP` est également spécifié pour *Dialer*. BNU recherche alors une entrée `TCP` pour les fichiers **Dialers**.

Fichier Dialers

Le fichier **Dialers** utilisé par **uucico** sur `zeus` doit comporter l'entrée TCP/IP :

```
TCP
```

Cette entrée indique qu'aucune configuration de numéroteur n'est requise.

Remarque : La configuration du numéroteur n'est jamais requise sur une connexion TCP/IP.

Fichier Permissions

Pour donner à `hera` accès à `zeus`, le fichier **Permissions** du système `zeus` contient l'entrée :

```
LOGNAME=uhera SENDFILES=yes REQUEST=yes \
MACHINE=zeus:hera VALIDATE=uhera /
READ=/var/spool/uucppublic:/home/hera \
WRITE=/var/spool/uucppublic:/home/hera COMMANDS=ALL
```

La combinaison des entrées LOGNAME et MACHINE fournit au système `hera` les droits d'accès au système `zeus` :

- `hera` peut demander et envoyer des fichiers quel que soit l'émetteur de l'appel.
- `hera` peut lire et écrire sur le répertoire public et le répertoire /**home**/**hera** du système `zeus`.

- `hera` peut exécuter toutes les commandes sur le système `zeus`.
- `hera` doit se connecter à `zeus` sous le nom d'utilisateur `uhera` et ne peut pas utiliser d'autre ID de connexion pour des transactions BNU.

Remarque : Les droits d'accès restent inchangés quel que soit le système émetteur de l'appel, c'est pourquoi les entrées LOGNAME et MACHINE sont combinées. Spécifiées séparément, elles se présentent comme suit :

```
LOGNAME=uhera VALIDATE=hera SENDFILES=yes REQUEST=yes \
READ=/var/spool/uucppublic:/home/hera \
WRITE=/var/spool/uucppublic:/home/hera

MACHINE=zeus:hera REQUEST=yes COMMANDS=ALL\
READ=/var/spool/uucppublic:/home/hera \
WRITE=/var/spool/uucppublic:/home/hera
```

Entrées dans les fichiers du système distant

Les fichiers contenant des entrées de connexion téléphonique sur le système distant `merlin` sont les suivants.

Fichier Systems

Pour permettre à `hera` de contacter `zeus`, un fichier **Systems** sur `hera` doit comporter l'entrée suivante :

```
zeus Any TCP,t - - ogin:--ogin: uhera ord: lightning
```

Cette ligne indique que le système `hera` peut appeler `zeus` à tout moment via le protocole **t** pour communiquer avec le système `zeus`. Le système `hera` se connecte à `zeus` sous le nom d'utilisateur `uhera` et le mot de passe `lightning`. De nouveau, BNU recherche une entrée de type `TCP` dans le fichier **Devices**.

Remarque : Le protocole **t** prend en charge le protocole **tcp**. Par conséquent, utilisez toujours le protocole **t** pour les communications BNU via des connexions TCP/IP. Le protocole **t** ne peut toutefois être utilisé si le champ *Type* a la valeur `ACU` ou que la connexion est établie via un modem.

Fichier Devices

Le fichier **Devices** utilisé par **uucico** sur `hera` doit comporter pour les connexions TCP/IP l'entrée suivante :

```
TCP  -  -  -  TCP
```

Le type d'unité étant `TCP`, il n'y a pas d'entrées *Class*, *Line* ou *Line2*. De même, `TCP` est également spécifié pour *Dialer*. BNU recherche alors une entrée `TCP` pour les fichiers **Dialers**.

Fichier Dialers

Le fichier **Dialers** utilisé par **uucico** sur le système `hera` doit comporter une entrée TCP/IP comme suit :

```
TCP
```

Cette entrée indique qu'aucune configuration de numéroteur n'est requise.

Remarque : La configuration du numéroteur n'est jamais requise sur une connexion TCP/IP.

Fichier Permissions

Pour donner à `zeus` accès à `hera`, le fichier **Permissions** du système `hera` contient l'entrée :

```
LOGNAME=uzeus SENDFILES=yes REQUEST=yes \
MACHINE=hera:zeus VALIDATE=zeus COMMANDS=rmail:who:uucp
```

La combinaison des entrées LOGNAME et MACHINE fournit au système `zeus` les droits d'accès au système `hera` :

- `zeus` peut demander et envoyer des fichiers quel que soit l'émetteur de l'appel.
- `zeus` peut lire et écrire uniquement sur le répertoire public (par défaut).
- `zeus` ne peut exécuter que les commandes **rmail**, **who** et **uucp.**
- `zeus` doit se connecter à `hera` sous le nom d'utilisateur `uzeus` et ne peut pas utiliser d'autre ID de connexion pour les transactions BNU.

Remarque : Séparément, les entrées LOGNAME et MACHINE se présentent comme suit :

```
LOGNAME=uzeus VALIDATE=zeus SENDFILES=yes REQUEST=yes
MACHINE=hera:zeus COMMANDS=rmail:who:uucp REQUEST=yes
```

Exemple de configuration BNU pour connexion téléphonique

Les fichiers exemples suivants sont configurés pour connecter les systèmes `venus` et `merlin` par le biais d'une ligne téléphonique et de modems. `venus` est supposé être le système local et `merlin` le système distant.

Sur les deux systèmes, l'unité `tty1` est raccordée à un modem Hayes à 1200 bauds. L'ID de connexion utilisé par `venus` pour se connecter à `merlin` est `uvenus` et le mot de passe associé est `mirror`. L'ID de connexion utilisé par `merlin` pour se connecter à `venus` est `umerlin` et le mot de passe associé est `oaktree`. Le numéro d'appel du modem raccordé à `venus` est `9=3251436`, celui du modem raccordé à `merlin` est `9=4458784`. Les deux machines comportent des numéros d'appel partiels dans leurs fichiers **Systems** et des codes d'accès dans leurs fichiers **Dialcodes**.

Entrées sur le système local

Les fichiers contenant des entrées de connexion téléphonique sur le système local `venus` sont les suivants.

Fichier Systems

Le fichier **Systems** sur `venus` doit comporter une entrée pour `merlin` incluant un numéro et un préfixe d'appel, comme suit :

```
merlin Any ACU 1200 local8784 "" in:--in: uvenus word: mirror
```

`venus` peut appeler `merlin` à tout moment avec une unité `ACU` à `1200` bauds, sous le nom `uvenus` et le mot de passe `mirror`. Le numéro d'appel est développé avec le code `local` dans le fichier **Dialcodes** et l'unité à utiliser est déterminée en fonction des entrées *Type* et *Class*. Sur cette base, BNU recherche une unité de type `ACU` et de classe `1200` dans les fichiers **Devices**.

Fichier Dialcodes

Le fichier **Dialcodes** sur `venus` comporte le préfixe d'appel à associer au numéro figurant dans le fichier **Systems** :

```
local 9=445
```

Ainsi, le développé du numéro d'appel pour le système `merlin` dans **Systems** est `9=4458784`.

Fichier Devices

Le fichier **Devices** côté `venus` doit comporter, pour la connexion à `merlin`, l'entrée suivante :

```
ACU tty1  -  1200  hayes \T
```

Le port à utiliser est `tty1` et la valeur associée à l'entrée *Dialer* dans le champ *Dialer-Token Pairs* est `hayes`. Pour l'entrée *Token*, `\T` indique que le numéro d'appel est développé à l'aide d'un code issu du fichier **Dialcodes**. BNU recherche le numéroteur `hayes` dans les fichiers **Dialers**.

Fichier Dialers

Un fichier **Dialers** utilisé par **uucico** sur `venus` doit comporter pour le modem `hayes` l'entrée suivante :

```
hayes =,-, "" \dAT\r\c OK \pATDT\T\r\c CONNECT
```

Remarque : La séquence expect-send est définie dans le format de fichier **Dialers.**

Fichier Permissions

Pour spécifier au système `merlin` le mode d'exécution des transactions **uucico** et **uuxqt** avec le système `venus`, le fichier **Permissions** sur `venus` doit contenir les entrées :

```
LOGNAME=umerlin REQUEST=yes SENDFILES=yes \
READ=/var/spool/uucppublic:/home/merlin \
WRITE=/var/spool/uucppublic:/home/merlin
MACHINE=venus:merlin VALIDATE=umerlin REQUEST=yes SENDFILES=yes
 \
COMMANDS=ALL \
READ=/var/spool/uucppublic:/home/merlin \
WRITE=/var/spool/uucppublic:/home/merlin
```

Le système `merlin` se connecte à `venus` sous le nom de `umerlin`, qui est un nom de connexion unique pour le système `merlin`. Il peut demander et envoyer des fichiers quel que soit l'émetteur de l'appel. Le système `merlin` peut en outre lire et écrire dans le répertoire **/var/spool/uucppublic** et dans le répertoire **/home/merlin** sur le système `venus`. Il peut lancer toutes les commandes du jeu de commandes par défaut sur le système `venus`.

Entrées sur le système distant

Les fichiers contenant des entrées de connexion téléphonique sur le système distant `merlin` sont les suivants :

Fichier Systems

Un fichier **Systems** sur `merlin` doit contenir pour `venus` une entrée incluant un numéro et un préfixe d'appel, comme suit :

```
venus Any ACU 1200 intown4362 "" in:--in: umerlin word: oaktree
```

`merlin` peut appeler `venus` à tout moment, avec une unité `ACU` à `1200` bauds, sous le nom `umerlin` avec le mot de passe `oaktree`. Le numéro d'appel est développé avec le code `local` dans le fichier **Dialcodes** et l'unité à utiliser est déterminée en fonction des entrées *Type* et *Class*. Sur cette base, BNU recherche une unité de type `ACU` et de classe `1200` dans les fichiers **Devices.**

Fichier Dialcodes

Le fichier **Dialcodes** sur `merlin` comporte le préfixe d'appel à associer au numéro figurant dans le fichier **Systems** :

```
intown 9=325
```

Ainsi, le numéro d'appel développé pour accéder au système `venus` est `9=3254362`.

Fichier Devices

Pour la connexion à venus, un fichier **Devices** côté merlin doit comporter la ligne :

```
ACU  tty1  -  1200  hayes \T
```

L'unité ACU est raccordée au port tty1 et le numéroteur est hayes. Le numéro d'appel est développé à l'aide des informations extraites du fichier **Dialcodes**. BNU recherche une entrée pour modem hayes dans les fichiers **Dialers**.

Fichiers Dialers

Un fichier **Dialers** utilisé par **uucico** sur merlin doit comporter pour son modem l'entrée :

```
hayes  =,-,  ""  \dAT\r\c OK \pATDT\T\r\c CONNECT
```

Fichier Permissions

Pour que venus puisse accéder à merlin, le fichier **Permissions** sur merlin doit comporter les entrées suivantes :

```
LOGNAME=uvenus SENDFILES=call REQUEST=no \
WRITE=/var/spool/uucppublic:/home/venus \
READ=/var/spool/uucppublic:/home/venus
MACHINE=merlin:venus VALIDATE=uvenus  \
READ=/ WRITE=/ COMMANDS=ALL REQUEST=yes \
NOREAD=/etc/uucp:/usr/etc/secure \
NOWRITE=/etc/uucp:/usr/etc/secure
```

Exemple de configuration BNU pour connexion directe

Les fichiers suivants sont configurés pour une connexion câblée entre les systèmes zeus et hera, où zeus est supposé être le système local et hera le système distant. L'unité câblée est tty5 sur zeus et tty1 côté hera. La vitesse de connexion est 1200 bps. L'ID de connexion à zeus sur hera est uzeus avec le mot de passe associé thunder. L'ID de connexion à hera sur zeus est uhera avec le mot de passe portent.

Entrées dans les fichiers du système local

Les fichiers contenant des entrées de connexion téléphonique sur le système local venus sont les suivants :

Fichier Systems

Un fichier **Systems** sur zeus doit contenir pour le système distant hera l'entrée suivante :

```
hera Any hera 1200 - "" \r\d\r\d\r in:--in: uzeus word:  thunder
```

Cette entrée indique que le système hera peut se connecter à zeus à tout moment via une connexion directe spécifiée dans le fichier **Devices**. Pour trouver cette entrée dans les fichiers **Devices**, BNU utilise le troisième et le quatrième champs de l'entrée **Systems**. BNU recherche dans les fichiers **Devices** une entrée dont le champ *Type* a la valeur hera et la classe 1200. Le système zeus se connecte au système hera sous le nom uzeus avec le mot de passe thunder.

Fichier Devices

Pour la connexion au système distant herald, le fichier **Devices** sur zeus doit comporter l'entrée :

```
hera    tty5  -  1200  direct
```

Cette entrée indique que le système zeus utilise l'unité tty5 à 1200 bps pour communiquer avec hera. Notez que *Dialer* dans les deux champs *Dialer-Token Pairs* a la valeur direct. Lors de la connexion à hera, BNU recherche une entrée direct dans le fichier **Dialers**.

Fichiers Dialers

Pour les connexions directes, un fichier **Dialers** sur `zeus` doit comporter l'entrée :

```
direct
```

Cette entrée spécifie qu'aucune mise en liaison ("handshaking") n'est requise pour la connexion directe.

Fichier Permissions

Pour spécifier au système `hera` le mode d'exécution des transactions **uucico** et **uuxqt** avec `zeus`, le fichier **Permissions** du système `zeus` doit contenir les entrées suivantes :

```
LOGNAME=uhera MACHINE=hera VALIDATE=uhera REQUEST=yes \
SENDFILES=yes MACHINE=hera READ=/ WRITE=/ COMMANDS=ALL
```

Cette entrée indique que le système `hera` se connecte sous le nom de `uhera`. L'option `VALIDATE=uhera` étant incluse, le système `hera` ne peut pas se connecter à `zeus` avec un autre ID de connexion et aucun autre système distant ne peut utiliser l'ID `uhera`. Le système `hera` peut lire et écrire sur n'importe quel répertoire du système `zeus`, et demander et envoyer des fichiers quel que soit l'émetteur de l'appel. `hera` peut également lancer toutes les commandes sur le système `zeus`.

Remarque : Les droits d'accès accordés sont les mêmes quel que soit l'émetteur de la connexion. C'est pourquoi les entrées LOGNAME et MACHINE ont été combinées. Spécifiées séparément, elles se présentent comme suit :

```
LOGNAME=uhera REQUEST=yes SENDFILES=yes READ=/ WRITE=/
MACHINE=zeus:hera VALIDATE=uhera READ=/ WRITE=/ REQUEST=yes \
COMMANDS=ALL
```

Attention : Attribuer des droits d'accès comme dans l'exemple précédent équivaut à doter tout utilisateur résidant sur le système distant d'un ID de connexion sur le système local. Ces droits d'accès souples peuvent nuire à la sécurité de votre système et il est conseillé de ne les accorder qu'aux systèmes distants sécurisés résidant sur le même site.

Entrées dans les fichiers du système distant

Les fichiers contenant des entrées de connexion téléphonique sur le système distant `merlin` sont les suivants.

Fichier Systems

Un fichier **Systems** sur le système `hera` doit contenir une entrée pour le système `zeus`:

```
zeus Any zeus 1200 - "" \r\d\r\d\r in:--in: uhera word: portent
```

Cette entrée spécifie que `hera` peut se connecter à `zeus` à tout moment, via une connexion directe spécifiée dans le(s) fichier(s) **Devices**. Pour trouver cette entrée dans les fichiers **Devices**, BNU utilise le troisième et le quatrième champs de l'entrée **Systems**. BNU recherche une entrée dans le fichier **Devices** avec pour *Type* `zeus` et *Class* `1200`. Le système `hera` se connecte à `zeus` sous le nom d'utilisateur `uhera` et le mot de passe `portent`.

Fichier Devices

Un fichier **Devices** sur le système `hera` doit comporter pour la communication avec `zeus` l'entrée suivante :

```
zeus    tty1  -  1200  direct
```

Cette entrée indique que le système `hera` utilise l'unité `tty1` à `1200` bps pour communiquer avec le système `zeus`. *Dialer* étant positionné sur `direct`, BNU recherche dans les fichiers **Dialers** une entrée `direct`.

Fichiers Dialers

Un fichier **Dialers** sur `hera` doit comporter pour les connexions directes l'entrée :

```
direct
```

Cette entrée indique qu'aucune configuration de numéroteur n'est requise sur la connexion directe.

Fichier Permissions

Le fichier **Permissions** sur `hera` doit comporter l'entrée ci-dessous pour spécifier le mode d'exécution des transactions **uucico** et **uuxqt** par `zeus` sur `hera` :

```
LOGNAME=uzeus REQUEST=yes SENDFILES=yes READ=/ WRITE=/
MACHINE=hera:zeus VALIDATE=uzeus REQUEST=yes COMMANDS=ALL READ=/\
WRITE=/
```

Ces entrées indiquent que le système `zeus` se connecte à `hera` sous le nom de `uzeus`. L'option `VALIDATE=uzeus` étant incluse, le système `zeus` ne peut pas se connecter à `hera` avec un autre ID de connexion et aucun autre système distant ne peut utiliser l'ID `uzeus`. Le système `zeus` peut lire et écrire sur n'importe quel répertoire du système `hera`, et demander et envoyer des fichiers quel que soit l'émetteur de l'appel. `zeusa` peut également lancer toutes les commandes sur le système `hera`.

Attention : Attribuer des droits d'accès comme dans l'exemple précédent équivaut à doter tout utilisateur résidant sur le système distant d'un ID de connexion sur le système local. Ces droits d'accès souples peuvent nuire à la sécurité de votre système et il est conseillé de ne les accorder qu'aux systèmes distants résidant sur le même site.

Référence des fichiers, commandes et répertoires BNU

Répertoires BNU

/etc/uucp	Contient tous les fichiers de configuration BNU (Basic Network Utilities).
/etc/locks	Contient les fichiers de verrouillage pour les unités système. Utilisé par les autres sous-systèmes en complément de BNU.
/var/spool/uucppublic	Contient les fichiers qui ont été transférés par BNU.
/var/spool/uucp	Contient les fichiers administratifs BNU.
/var/spool/uucp/.Workspace	Contient les fichiers temporaires utilisés en interne par les programmes de transport de fichier.
/var/spool/uucp/.Xqtdir	Contient les fichiers exécutables avec les listes des commandes exécutables par les systèmes distants.
/var/spool/uucp/*SystemName*	Contient les fichiers utilisés par les programmes de transport de fichier.

Fichiers BNU

/etc/uucp/Systems	Liste de systèmes auxquels **uucico** peut se connecter.
/etc/uucp/Devices	Définit les paramètres de communication de base pour les connexions sortantes.
/etc/uucp/Permissions	Définit les autorisations pour les machines distantes contactant la machine locale via BNU.
Maxuuscheds	Limite les travaux programmés simultanément.
Maxuuxqts	Limite les exécutions simultanées de commandes à distance.
/etc/uucp/Dialers	Spécifie le type du modem et du numéroteur.
/etc/uucp/Dialcodes	Contient les premiers chiffres des numéros de téléphone utilisés pour établir les connexions à distance via une ligne téléphonique.
/usr/sbin/uucp/remote.unknown	Script shell exécuté lorsqu'un ordinateur distant inconnu tente d'établir une communication.
/usr/sbin/uucp/Sysfiles	Affecte des fichiers système, unité et numéroteur, secondaires ou supplémentaires.
/etc/uucp/Poll	Détermine le moment d'appel d'un système distant.
uudemon.admin	Envoie un rapport d'état BNU à l'ID de connexion spécifié.
uudemon.cleanu	Nettoie les répertoires de spoulage BNU à des moments programmés.
uudemon.hour	Lance les appels de transport de fichier vers les systèmes distants.
uudemon.poll	Interroge les systèmes distants répertoriés dans le fichier **/etc/uucp/Poll**.

/var/spool/uucp/audit	Contient les informations d'audit relatives aux activités BNU.
/var/spool/uucp/Foreign	Contient les informations relatives aux erreurs intervenues au cours des activités BNU.
/var/spool/uucp/errors	Contient les informations relatives aux erreurs intervenues au cours des activités BNU.
/var/spool/uucp/xferstats	Contient les informations relatives aux statistiques sur les activités BNU.
/var/spool/uucp/Corrupt	Contient la copie des fichiers que le programme BNU ne peut pas traiter.
/var/spool/uucp/.Log	Contient les fichiers journaux issus des transactions BNU courantes.
/var/spool/uucp/.Old	Contient les fichiers journaux issus des anciennes transactions BNU.
/var/spool/uucp/.Status	Prend date de la dernière tentative du démon **uucico** de communiquer avec les systèmes distants.
/var/spool/uucp/*SystemName***/C.***	Ces fichiers sont les commandes autorisées lors d'une connexion avec *SystemName*.
/var/spool/uucp/*SystemName***/D.***	Ces fichiers sont des fichiers de données associés à *SystemName*.
/var/spool/uucp/*SystemName***/X.***	Fichiers exécutables sur *SystemName*.
/var/spool/uucp/*SystemName***/TM.***	Fichiers temporaires utilisés pendant la connexion à *SystemName*.

Commandes BNU

ct	Établit la connexion à un autre système via une ligne téléphonique.
cu	Établit la connexion à un autre système.
tip	Variante de **cu** qui nécessite une configuration particulière.
uucp	Copie les fichiers d'un système vers un autre système exécutant BNU ou une version d'UUCP (UNIX–to–UNIX Copy Program).
uudecode	Reconstitue un fichier binaire codé avec **uuencode**.
uuencode	Code un fichier binaire dans un format ASCII pour la transmission via BNU.
uuname	Fournit des informations sur les systèmes accessibles.
uupoll	Force un appel à un système distant.
uuq	Affiche la file d'attente des travaux BNU.
uusend	Envoie un fichier à un hôte distant exécutant BNU ou UUCP.
uusnap	Affiche un récapitulatif succinct de l'état de BNU.
uustat	Rend compte de l'état des opérations BNU.
uuto	Copie des fichiers vers un autre système exécutant BNU ou UUCP.
uux	Exécute une commande sur un système distant.
uucheck	Recherche dans le fichier **/etc/uucp/Permissions** la configuration correcte.
uuname	Affiche les noms de tous les systèmes accessibles via BNU.
uuclean	Nettoie les répertoires de spoulage BNU.

uucleanup	Nettoie les répertoires de spoulage BNU.
uukick	Contacte un système distant avec la mise au point activée.
uulog	Affiche les fichiers journaux BNU.
uutry	Contacte un système distant avec la mise au point activée. Ne tient pas compte des délais impartis pour les tentatives.
uucpadm	Administre le système BNU.
uupick	Permet de récupérer des fichiers dans le répertoire **/var/spool/uucppublic.**
uucp	ID de connexion avec droits d'accès administratifs complets sur le sous-système BNU.
Uutry	Contacte un système distant avec la mise au point activée et sauvegarde la sortie de mise au point dans un fichier.

Démons BNU

uucico	Contacte les systèmes distants et transfère les fichiers.
uucpd	Permet l'exécution de BNU sur le dessus de TCP/IP (Transmission Control Protocol/Internet Protocol).
uusched	Planifie les travaux BNU.
uuxqt	Exécute des requêtes de commande à partir de systèmes distants.

Chapitre 9. Administration du réseau

Administrer un réseau consiste à gérer globalement des réseaux systèmes, via le protocole SNMP, permettant aux hôtes d'échanger des informations de gestion. SNMP (Simple Network Management Protocol) est un protocole conçu pour les interrréseaux basés sur TCP/IP. Ce chapitre traite des points suivants :

Consultez également la section "SNMP Overview for Programmers" du manuel dans *AIX Communications Programming Concepts*.

Administration de réseau avec SNMP

L'administration de réseau SNMP repose sur le modèle client/serveur, largement exploité dans les applications basées sur TCP/IP. Chaque hôte à gérer exécute un processus appelé un *agent*. L'agent est un processus serveur qui maintient la base de données MIB (Management Information Base) pour l'hôte. Les hôtes impliqués dans les décisions d'administration du réseau peuvent exécuter un processus appelé un gestionnaire. Un *gestionnaire* est une application client qui génère les requêtes d'informations à la MIB et traite les réponses. Un gestionnaire peut en outre envoyer des requêtes aux serveurs de l'agent pour modifier les informations MIB.

Pour plus d'informations, consultez la section "Simple Network Management Protocol (SNMP)" dans *AIX Communications Programming Concepts*. Vous pouvez également consulter les RFC suivants :

RFC 1155	Structure et identification des données de gestion (SMI) pour les interréseaux TCP/IP.
RFC 1157	SNMP (Simple Network Management Protocol).
RFC 1213	Base MIB pour l'administration des interréseaux basés sur TCP/IP.
RFC 1227	Protocole SNMP (Simple Network Management Protocol), protocole SMUX (single multiplexer) et base MIB (Management Information Base).
RFC 1228	SNMP–DPI (Simple Network Management Protocol–Distributed Program Interface).
RFC 1229	Extensions à l'interface générique MIB (Management Information Base).
RFC 1231	MIB (Management Information Base) anneau à jeton IEEE 802.5.
RFC 1398	Définitions des objets gérés pour Ethernet. Par exemple, type d'interface.
RFC 1512	Base MIB de FDDI (Fiber Distributed Data Interface).

Règles d’accès de SNMP

L’agent **snmpd** utilise un schéma d’authentification simple pour connaître les stations du gestionnaire ayant accès aux variables MIB. Le schéma d’authentification suppose de spécifier les politiques d’accès SNMP. Une politique d’accès SNMP est un ensemble de relations administratives impliquant une association au sein d’une communauté SNMP, un mode d’accès et une vue MIB.

On appelle *communauté SNMP* un groupe d’hôtes doté d’un nom. Un nom de communauté est une chaîne d’octets qu’un gestionnaire SNMP doit imbriquer dans un paquet de requêtes SNMP à des fins d’authentification.

Le *mode d’accès* spécifie l’accès accordé aux hôtes de la communauté, en ce qui concerne la récupération et la modification des variables MIB à partir d’un agent SNMP spécifique. Le mode d’accès peut être : *none*, *read–only*, *read–write*, or *write–only*.

Une *vue MIB* définit une ou plusieurs sous-arborescences MIB accessibles par une communauté SNMP donnée. Il peut s’agir de toute l’arborescence MIB ou d’un sous-ensemble de cette arborescence.

Lorsque l’agent SNMP reçoit une requête, il compare le nom de la communauté à l’adresse IP de l’hôte demandeur pour savoir si ce dernier est un membre de la communauté SNMP. Si oui, il détermine ensuite si l’hôte demandeur a le droit d’accès spécifié aux variables MIB voulues, tel que défini dans la politique d’accès associée à cette communauté. Si tous les critères sont vérifiés, l’agent SNMP tente de répondre à la demande. Sinon, il génère une interruption d’échec d’authentification (*authenticationFailure*) ou envoie un message d’erreur à l’hôte demandeur.

Les politiques d’accès de SNMP pour l’agent **snmpd,** configurables par l’utilisateur, sont spécifiées dans le fichier **/etc/snmpd.conf**. Pour configurer les politiques d’accès SNMP pour l’agent **snmpd**, reportez-vous donc au fichier **/etc/snmpd.conf**.

Démon SNMP

Le démon SNMP (Simple Network Management Protocol) est un processus serveur d'arrière-plan exécutable sur n'importe quel hôte station de travail TCP/IP (Transmission Control Protocol/Internet Protocol). Ce démon, qui sert d'agent SNMP, reçoit, authentifie et traite les requêtes SNMP issues des applications du gestionnaire. Pour en savoir plus, reportez-vous aux sections "Simple Network Management Protocol," "How a Manager Functions" et "How an Agent Functions"dans *AIX Communications Programming Concepts*.

Remarque : Les termes démon SNMP, agent SNMP et agent sont synonymes.

Pour une configuration minimale, il faut que l'interface TCP/IP de boucle soit active pour le démon **snmpd**. Avant de lancer TCP/IP, entrez la commande :

```
ifconfig lo0 loopback up
```

Configuration du démon SNMP

Le démon SNMP (Simple Network Management Protocol) tente de lier les sockets à certain ports UDP (User Datagram Protocol) et TCP (Transmission Control Protocol) identifiés, qui doivent être définis dans le fichier **/etc/services**, comme suit :

```
snmp            161/udp
snmp-trap       162/udp
smux            199/tcp
```

Le service `snmp` doit être affecté du port `161`, conformément à RFC 1157. Le fichier **/etc/services** assigne les ports 161, 162 et 199 à ces services. Si le fichier **/etc/services** est mis à disposition à partir d'une autre machine, ces ports assignés doivent être rendus disponibles dans le fichier **/etc/services** servi pour que le démon SNMP puisse s'exécuter.

Le démon SNMP lit le fichier de configuration **/etc/snmpd.conf**, au lancement et à l'émission d'une commande **refresh** (si le démon **snmpd** est appelé sous le contrôle SRC) ou d'un signal **kill –1**. Ce fichier de configuration spécifie les noms de communauté et les vues et droits d'accès associés, les hôtes pour la notification d'interruption, les attributs de connexion, les paramètres spécifiques de **snmpd** et les configurations SMUX (single multiplexer) pour le démon SNMP. Pour en savoir plus, consultez le fichier **/etc/snmpd.conf**.

Fonctionnement du démon SNMP

Le démo, SNMP (Simple Network Management Protocol) traite les requêtes SNMP issues des applications du gestionnaire. Pour en savoir plus, consultez les sections ”Simple Network Management Protocol (SNMP),” ”How a Manager Functions” et ”How an Agent Functions” dans *AIX Communications Programming Concepts*.

Traitement d’un message et authentification

Toutes les requêtes, interruptions et réponses sont transmises sous la forme de messages codés en ASN.1. Un message, tel que défini par RFC 1157, a la structure suivante :

Version Communauté PDU

Version étant la version de SNMP (actuellement la version 1), *Communauté,* le nom de la communauté et *PDU*, l’unité des données de protocole contenant les données de requête, de réponse ou d’interruption SNMP. Un PDU est également codé selon les règles ASN.1.

Le démon SNMP reçoit et transmet tous les messages du protocole SNMP via UDP (User Datagram Protocol) TCP/IP (Transmission Control Protocol/Internet Protocol). Les requêtes sont acceptées sur le port identifié 161. Les interruptions sont transmises aux hôtes répertoriés dans les entrées d’interruption du fichier **/etc/snmpd.conf** qui écoutent le port identifié 162.

A réception d’une requête, l’adresse IP source et le nom de la communauté sont comparés à la liste des adresses IP, des noms de communauté, des droits et des vues, spécifiés dans le fichier **/etc/snmpd.conf**. L’agent **snmpd** lit ce fichier au lancement et à l’émission d’une commande **refresh** ou d’un signal **kill –1**. En l’absence d’entrée correspondante, la requête est ignorée. Dans le cas contraire, l’accès est accordé, en fonction des droits spécifiés pour cette association (adresse IP, communauté et nom de vue) dans le fichier **/etc/snmpd.conf**. Le message et le PDU doivent être codés conformément aux règles ASN.1.

Ce schéma d’authentification n’est pas censé garantir une sécurité totale. Si le démon SNMP n’est utilisé que pour les requêtes ”get” et ”get-next”, la sécurité n’est pas forcément très importante. En revanche, si des requêtes ”set” sont autorisées, il est possible de restreindre le privilège ”set”.

Pour en savoir plus, consultez le fichier **/etc/snmpd.conf**. Pour en savoir plus, reportez-vous à ”Management Information Base (MIB)”dans *AIX Communications Programming Concepts*.

Traitement d’une requête

Le démon SNMP peut recevoir trois types de requêtes PDU. Les types de requêtes, définies dans RFC 1157, et les PDU ont tous le format suivant :

Format de PDU de requête			
ID requête	**état-erreur**	**index-erreur**	**liaisons-variable**
GET	0	0	*VarBindList*
GET–NEXT	0	0	*VarBindList*
SET	0	0	*VarBindList*

Le champ ID-requête indique la nature de la requête ; les champs état-erreur et index-erreur sont inutilisés et doivent être définis à 0 (zéro) ; le champ liaisons-variable contient une liste de longueur variable des ID d’instance, au format numérique, dont les valeurs sont demandées. Si la valeur du champ ID requête est SET, le champ liaisons-variable est une liste de paires ID d’instance/valeur.

Pour en savoir plus, consultez la section ”Using the Management Information Base (MIB) Database”dans *AIX Communications Programming Concepts*.

Traitement d’une réponse

Les PDU de réponse ont presque le même format que les PDU de requête :

Format de PDU de réponse			
ID requête	**état-erreur**	**index-erreur**	**liaisons-variable**
GET–RESPONSE	*ErrorStatus*	*ErrorIndex*	*VarBindList*

Si la requête a abouti, la valeur des champs état-erreur et index-erreur est 0 (zéro), et le champ liaisons-variable contient la liste complète des paires ID d’instance/valeur.

Si un ID d’instance du champ liaisons-variable du PDU de requête n’a pas abouti, l’agent SNMP interrompt le traitement, entre l’index de l’ID d’instance défaillant dans le champ index-erreur, enregistre un code d’erreur dans le champ état-erreur et copie la liste de résultats partiellement complétée dans le champ liaisons-variable.

RFC 1157 définit les valeurs suivantes pour le champ état-erreur :

Valeurs du champ état-erreur		
Valeur	**Valeur**	**Explication**
noError	0	Traitement réussi (index d’erreur = 0).
tooBig	1	La taille du PDU de réponse dépasse une limite définie par l’implémentation (index d’erreur = 0).
noSuchName	2	Un ID d’instance n’existe pas dans la vue MIB appropriée pour les types de requête GET et SET ou n’a pas de successeur dans l’arborescence MIB dans la vue MIB appropriée pour les requêtes GET-NEXT (index d’erreur différent de zéro).
badValue	3	Pour les requêtes SET uniquement, une valeur spécifiée est syntaxiquement incompatible avec l’attribut de type de l’ID d’instance correspondant (index d’erreur différent de zéro).
readOnly	4	Non défini.
genErr	5	Une erreur définie par l’implémentation s’est produite (index d’erreur différent de zéro) ; par exemple, une tentative d’assignation d’une valeur dépassant les limites d’implémentation.

Traitement d’une interruption

Les PDU d’interruption sont définis par RFC 1157 de façon à avoir le format suivant :

Format de PDU d’interruption					
entreprise	**agent-adresse**	**générique-interruption**	**spécifique-interruption**	**horodate.**	**variable-liaisons**
ID Objet	*Entier*	*Entier*	*Entier*	*Tics d’horloge*	*VarBindList*

Les champs sont utilisés comme suit :

entreprise	Identificateur d'objet assigné au fournisseur implémentant l'agent. Valeur de la variable **sysObjectID**, unique pour chaque metteur en oeuvre d'un agent SNMP. La valeur assignée à cette implémentation de l'agent est **1.3.6.1.4.1.2.3.1.2.1.1.3** ou **risc6000snmpd.3**.
adresse-agent	Adresse IP de l'objet générateur de l'interruption.
interruption-générique	Entier, comme suit : 0 *coldStart* 1 *warmStart* 2 *linkDown* 3 *linkUp* 4 *authenticationFailure* 5 *egpNeighborLoss* 6 *enterpriseSpecific*
interruption-spécifique	Inutilisé, réservé à un usage ultérieur.
horodate	Temps écoulé, en centièmes de seconde, depuis la dernière réinitialisation de l'agent jusqu'à l'événement générant l'interruption.
liaisons-variable	Informations supplémentaires, fonction du type d'*interruption-générique*.

Les valeurs d'interruption générique suivantes indiquent que certains événements système ont été détectés :

coldStart	L'agent est en cours de réinitialisation. Les données de configuration et/ou la valeur des variables MIB peuvent avoir changé. Les epochs de mesure doivent être relancés.
warmStart	L'agent est en cours de réinitialisation, mais les données de configuration ou la valeur des variables MIB n'ont pas changé. Dans cette mise en oeuvre de l'agent SNMP, une interruption *warmStart* est générée à la relecture du fichier **/etc/snmpd.conf**. Les informations de configuration dans le fichier **/etc/snmpd.conf** concernent la configuration de l'agent sans effets sur les bases de données du gestionnaire SNMP. Les epochs de mesure ne doivent pas être relancés.
linkDown	L'agent a détecté qu'une interface de communication identifiée a été désactivée.
linkUp	L'agent a détecté qu'une interface de communication identifiée a été activée.
authenticationFailure	Un message reçu n'a pu être authentifié.
egpNeighborLoss	Un neighbor EGP (Exterior Gateway Protocol) est perdu. Cette valeur n'est générée que lorsque l'agent s'exécute sur un hôte exécutant le démon **gated**, avec le protocole EGP (Exterior Gateway Protocol).
enterpriseSpecific	Non implémenté, réservé à un usage ultérieur.

Les interruptions *linkDown* et *linkUp* contiennent une paire ID d'instance/valeur unique dans la liste des liaisons de variable. L'ID d'instance identifie l'**ifIndex** de la carte désactivée ou activée, et la valeur est celle de **ifIndex**. L'interruption pour *egpNeighborLoss* contient également une liaison consistant en l'ID d'instance et la valeur de *egpNeighAddr* pour le voisin perdu.

Génération d'interruptions linkUp et linkDown

Remarque : Dans les sections suivants, le terme interface s'applique à une interface TCP/IP avec unité anneau à jeton CDLI (Common Data Link Interface), Ethernet ou FFDI (Fiber Distributed Data Interface). CDLI permet à **snmpd** de contrôler les unités Ethernet, anneau à jeton et FDDI même si elles n'exécutent TCP/IP. Le démon SNMP a toujours besoin d'une boucle TCP/IP, à l'inverse des interfaces.

Les interruptions *linkUp* et *linkDown* sont générées lorsque l'agent **snmpd** détecte un changement d'état pour une interface identifiée. Si l'état actuel d'une interface connue est "down" et qu'il passe à "up", une interruption *linkUp* est générée. De même, si l'état actuel d'une interface connue est "up" et qu'il passe à "down", une interruption *linDown* est générée.

Le concept opérationnel ou non opérationnel n'existe pas pour une unité CDLI en l'absence d'interface TCP/IP. Les unités CDLI avec une couche d'interface TCP/IP attachée sont toujours considérées comme opérationnelles, à moins que l'unité ne soit supprimée du système. Les autres valeurs de la table d'interfaces dépendent également de la présence ou non d'une interface TCP/IP. Si une unité CDLI a une telle interface, toutes les statistiques de cette table se rapportent à l'interface TCP/IP, et la MIB spécifique de l'unité doit être utilisée pour retrouver des statistiques propres à l'unité. Si elle n'en a pas, les entrées de la table sont extraites de l'unité CDLI elle-même.

A toute interface identifiée par l'agent **snmpd** est associée une entrée dans la table d'interfaces **snmpd**. Lorsqu'une interface est attachée ou détachée par la commande **ifconfig**, les entrées de la table sont modifiées. Une interruption *coldStart* est générée pour indiquer le changement de configuration. L'objectif de cette interruption *coldStart*, est de prévenir l'hôte récepteur que des variables MIB fondamentales ont changé. En particulier, les epochs de mesure doivent être relancés. Même si des liaisons peuvent être activées ou désactivées, aucune interruption *linkUp* ou *linkDown* n'est générée.

Pour la configuration d'un réseau hôte, une commande **netstat –in** génère, par exemple :

```
Name    Mtu    Network       Address        Ipkts  Ierrs  Opkts   Oerrs Coll
lo0     1536   127           127.0.0.1       6228     0    6228     0    0
en0     1500   192.100.154   192.100.154.7  585287   0    666636   0    0
tr0     1500   129.35.32     129.35.42.141  3976323  0    2414030  0    0
```

Dans cet exemple, l'agent **snmpd** possède trois entrées dans sa table d'interfaces TCP/IP : une pour *lo0*, une pour *en0* et une pour *tr0*. Dans la table d'index d'interface, ifIndex.3 peut référencer lo0, ifIndex.2, *en0,* et ifIndex.2, *tr0*. L'expression "peut référencer" signifie que, étant donné que les interfaces sont dynamiques, le numéro d'entrée réel peut varier. Dans l'exemple, il existe une carte token-ring supplémentaire sur la station de travail, non identifiée par le noyau TCP/IP ; l'interface correspondante s'appelle *tr1*. La carte token-ring étant une unité CDLI, une entrée lui est associée dans la table d'interfaces, par exemple ifIndex.4. La station de travail est dotée d'une unité optique série. L'unité optique série n'est pas configurée pour TCP/IP et n'est pas une unité CDLI. Ainsi, ni TCP/IP ni **snmpd** ne reconnaissent cette unité. Son nom d'interface est so0.

Si vous émettez la commande **ifconfig tr1**, TCP/IP attache *tr1*, mais ne marque pas l'interface comme opérationnelle. L'agent **snmpd** modifie la méthode de report des statistiques de table d'interfaces au niveau de la couche TCP/IP à partir des statistiques du niveau unité CDLI. L'agent **snmpd** génère ensuite une interruption *coldStart*. Cette action n'ajoute aucune entrée, puisque celle correspondant à *tr1* existait déjà.

Si vous émettez la commande **ifconfig so0**, TCP/IP attache *so1*, mais ne marque pas l'interface comme opérationnelle. L'agent **snmpd** ajoute alors une cinquième entrée à sa table d'interfaces et définit ifIndex.5 comme référençant *so0*. L'agent SNMP génère ensuite une interruption *coldStart*. *so0* n'étant pas une unité CDLI, il n'a pas été intégré à la table d'interfaces lors de la configuration de l'unité, et doit donc l'être au moment de la configuration de la couche d'interface TCP/IP.

Les valeurs fondamentales de l'index d'interface (ifIndex) éventuellement stockées par un gestionnaire SNMP pour les quatre entrées originales ne changent pas. Mais l'interruption *coldStart* signale aux gestionnaires SNMP qu'ils doivent mettre à jour leur base MIB. Lorsqu'il rafraîchit sa base de données, un gestionnaire SNMP prend connaissance de cette nouvelle entrée dans la table d'interface de l'agent **snmpd**.

Si l'administrateur système a lancé une commande **ifconfig tr1 up**, la nouvelle interface est marquée opérationnelle et la méthode d'obtention des statistiquess est modifiée. L'agent **snmpd** envoie une interruption *coldStart* ; une interruption *linkUp* n'est pas envoyée car l'état de l'unité n'a pas changé. Une unité CDLI est toujours considérée comme opérationnelle jusqu'à ce qu'elle obtienne une interface TCP/IP.

L'interruption *coldStart* indique aux gestionnaires SNMP que, la configuration de l'agent **snmpd** ayant changé, ils doivent mettre à jour leur base MIB. Si une interruption *linkUp* suit l'interruption *coldStart*, elle n'a aucune importance pour le gestionnaire SNMP puisque les informations de sa base de données sont déjà rafraîchies.

L'administrateur système a choisi de détacher l'interface *en0* de la configuration réseau ci-dessus. Une fois détaché, l'agent **snmpd** met à jour sa méthode de collecte des statistiques pour exploiter les statistiques de l'unité CDLI (Ethernet est une unité CDLI). Il génère une interruption *coldStart* pour informer les gestionnaires SNMP de la modification des interfaces. Dans ce cas, les valeurs ifIndex fondamentales ne changent pas (seule la méthode d'obtention de statistiques change).

L'administrateur système a choisi de détacher l'interface *so0* de la configuration réseau ci-dessus. Pendant le détachment d'une interface, l'agent **snmpd** met à jour sa table d'interfaces. Dans cet exemple, tous les index restent identiques, à l'exception de la cinquième entrée qui est supprimée. Si la troisième entrée avait été retirée, les quatrième et cinquième entrées auraient été renumérotées comme troisième et quatrième entrées, respectivement. Dans les deux cas, l'agent **snmpd** génère une interruption *coldStart*.

Par conséquent, les valeurs ifIndex fondamentales éventuellement enregistrées par un gestionnaire SNMP changent. Celui-ci doit rafraîchir sa base MIB pour qu'elle reflète les changements de la table d'interfaces de l'agent **snmpd**. Dans ce cas, une interruption *linkDown* n'est pas générée. Un gestionnaire SNMP ne peut pas agir immédiatement à réception d'une interruption *linkDown* : les valeurs ifIndex de sa base ne sont plus valides.

Pour que l'agent **snmpd** soit au fait de toutes les modifications d'état, il doit contrôler régulièrement le noyau TCP/IP et la liste des unités CDLI pour connaître l'état des interfaces. La fréquence des contrôles est configurable par l'utilisateur.

Si l'agent **snmpd** a reçu une requête portant sur une variable MIB dans la table d'interfaces et qu'il détecte un changement d'état de l'interface qui requiert une interruption *coldStart*, il renvoie un message d'erreur *genErr* et génère une interruption *coldStart*.

Pour en savoir plus sur les protocoles et les adresses d'interréseau, reportez-vous à "Protocole UDP", page 3-30, "Protocole EGP", page 3-34 et "Adressage TCP/IP, page 3-56.

Support du démon SNMP pour la famille EGP de variables MIB

Si l'hôte de l'agent exécute le démon **gated** alors que le protocole EGP (Exterior Gateway Protocol) est activé, plusieurs variables MIB (Management Information Base) du groupe EGP sont acceptées par le démon **gated** et accessibles par l'agent **snmpd**.

Les variables MIB EGP suivantes ont une instance unique :

egpInMsgs	Nombre de messages EGP reçus sans erreur.
egpInErrors	Nombre de messages EGP reçus avec erreur.
egpOutMsgs	Nombre total de messages EGP transmis par le démon **gated** actif sur l'hôte de l'agent.
egpOutErrors	Nombre de messages EGP qui n'ont pas pu être envoyés au démon **gated** de l'hôte de l'agent, par suite de limitations des ressources.
egpAs	Numéro système autonome du démon **gated** de l'hôte de l'agent.

Les variables MIB EGP suivantes ont une instance pour chaque homologue ou voisin EGP acquis par le démon **gated** de l'hôte de l'agent :

egpNeighState	État de cet homologue EGP :	
	1	idle
	2	acquisition
	3	down
	4	up
	5	cease
egpNeighAddr	Adresse IP de cet homologue EGP.	
egpNeighAs	Numéro système autonome de cet homologue EGP. Zéro (0) indique que ce numéro n'est pas encore connu.	
egpInNeighMsgs	Nombre de messages EGP reçus sans erreur de cet homologue EGP.	
egpNeighInErrs	Nombre de messages EGP reçus avec erreur de cet homologue EGP.	
egpNeighOutMsgs	Nombre de messages EGP générés localement pour cet homologue EGP.	
egpNeighOutErrs	Nombre de messages EGP générés en local, non envoyés à cet homologue EGP par suite de limitations des ressources.	
egpNeighInErrMsgs	Nombre de messages d'erreur définis par EGP reçus de cet homologue EGP.	
egpNeighOutErrMsgs	Nombre de messages d'erreur définis par EGP envoyés à cet homologue EGP.	
egpNeighStateUp	Nombre de transitions de l'état EGP jusqu'à l'état UP avec cet homologue EGP.	
egpNeighStateDowns	Nombre de transitions de l'état EGP à partir de l'état UP jusqu'à n'importe quel état avec cet homologue EGP.	
egpNeighIntervalHello	Intervalle entre les retransmissions de la commande Hello d'EGP, en centièmes de seconde.	
egpNeighIntervalPoll	Intervalle entre les retransmissions de la commande d'interrogation d'EGP, en centièmes de seconde.	

egpNeighMode Mode d'interrogation de cet homologue EGP : actif (1) ou passif (2).

egpNeighEventTrigger Une variable de contrôle déclenche des événements de lancement et d'arrêt initiés par l'opérateur sur cet homologue EGP. Cette variable MIB peut alors être définie pour le lancement (1) ou l'arrêt (2).

Si le démon **gated** n'est pas actif, que le démon **gated** n'est pas configuré pour communiquer avec l'agent **snmpd** ou que le démon **gated** n'est pas configuré pour EGP, les requêtes get et set pour les valeurs de ces variables renvoient le code d'erreur *noSuchName*.

Le fichier de configuration du démon **gated**, **/etc/gated.conf**, doit contenir l'instruction :

```
snmp      yes;
```

Le démon **gated** est configuré en interne pour être un homologue du protocole SMUX (SNMP multiplexing), ou un agent mandataire (proxy) du démon **snmpd**. A son lancement, le démon **gated** enregistre l'arborescence de la variable MIB *ipRouteTable* avec l'agent **snmpd**. Si le démon **gated** est configuré pour EGP, le démon **gated** enregistre également l'arborescence de la variable MIB EGP. Une fois l'enregistrement terminé, un gestionnaire SNMP peut envoyer des requêtes à l'agent **snmpd** concernant les variables MIB *ipRouteTable* d'un EGP, prises en charge par le démon **gated** de l'hôte de cet agent. Ainsi, lorsque le démon **gated** s'exécute, toutes les informations de routage MIB sont obtenues via le démon **gated**. Dans ce cas, les requêtes set pour *ipRouteTable* ne sont pas autorisées.

La communication SMUX entre les démons **gated** et **snmpd** s'effectue via le port TCP (Transmission Control Protocol) identifié 199. Si le démon **gated** doit s'arrêter, **snmpd** désenregistre immédiatement les arborescences précédemment enregistrées par **gated**. Si **gated** démarre avant **snmpd**, **gated** contrôle régulièrement le démon **snmpd** jusqu'à établissement de l'association SMUX.

Pour configurer l'agent **snmpd** pour qu'il reconnaisse et autorise l'association SMUX avec le client du démon **gated**, il faut ajouter une entrée SMUX dans le fichier **/etc/snmpd.conf**. L'identificateur et le mot de passe de l'objet client spécifiés dans cette entrée SMUX pour le démon **gated** doivent correspondre à ceux du fichier **/etc/snmpd.peers**.

L'agent **snmpd** prend en charge les requêtes set pour les variables en lecture-écriture MIB I et MIB II suivantes :

sysContact Identification textuelle de la personne à contacter pour l'hôte de cet agent. Cette information indique le nom de la personne et le moyen de la contacter : par exemple, "Bob Smith, 555-5555, ext 5." La valeur est limitée à 256 caractères. Si, pour une requête set, cette chaîne dépasse 256 caractères, l'agent **snmpd** renvoie l'erreur *badValue*, et l'opération set n'est pas exécutée. La valeur initiale de *sysContact* est définie dans **/etc.snmp.conf**. Valeur par défaut : chaîne nulle.

Instance	Valeur	Action
0	"chaîne"	La variable MIB est définie comme "chaîne".

sysName Nom de l'hôte de cet agent. Il s'agit généralement du nom qualifié complet du domaine. La valeur est limitée à 256 caractères. Si, pour une requête set, cette chaîne dépasse 256 caractères, l'agent **snmpd** renvoie l'erreur *badValue*, et l'opération set n'est pas exécutée.

Instance	Valeur	Action
0	”chaîne”	La variable MIB est définie comme ”chaîne”.

sysLocation Chaîne textuelle indiquant l’emplacement physique de la machine sur laquelle se trouve l’agent **snmpd.** Exemple : ”Site Austin, bâtiment 802, lab 3C-23.” La valeur est limitée à 256 caractères. Si, pour une requête set, cette chaîne dépasse 256 caractères, l’agent **snmpd** renvoie l’erreur *badValue*, et l’opération set n’est pas exécutée. La valeur initiale de *sysLocation* est définie dans /**etc**/**snmp.conf**. Valeur par défaut : chaîne nulle.

Instance	Valeur	Action
0	”chaîne”	La variable MIB est définie comme ”chaîne”.

ifAdminStatus État souhaité d’une carte d’interface sur l’hôte de l’agent. Les états possibles sont actif/inactif. Un état ”test” peut également être défini, mais cette valeur est sans effet sur l’état effectif de l’interface.

Instance	Valeur	Action
f	1	La carte d’interface avec **ifIndex f** est activée.

Remarque : Il est possible que, même si l’état *ifAdminStatus* est défini comme actif ou inactif, le changement effectif d’état n’ait pas eu lieu. Dans ce cas, une requête get de *ifAdminStatus* peut indiquer un état *up* (actif), et un *ifOperStatus* un état *down* (inactif) pour cette interface. Il faut alors que l’administrateur de réseau réémette une requête set de passage de *ifAdminStatus* à l’état actif pour retenter l’opération.

atPhysAddress Partie matérielle de l’adresse d’une liaison de table d’adresses sur l’hôte de l’agent (entrée de la table ARP (Address Resolution Protocol)). Même variable MIB que *ipNetToMediaPhysAddress*.

Instance	Valeur	Action
f.1.n.n.n.n	hh:hh:hh:hh:hh:hh	Pour l’interface avec **ifIndex f,** toute liaison de table ARP existante pour l’adresse IP n.n.n.n est remplacée par la liaison (n.n.n.n, hh:hh:hh:hh:hh:hh). S’il n’y en a pas, la nouvelle liaison est ajoutée. hh:hh:hh:hh:hh:hh est une adresse matérielle hexadécimale à douze chiffres.

atNetAddress Adresse IP correspondant à l’adresse matérielle ou physique spécifiée dans *atPhysAddress*. Il s’agit de la même variable MIB que *ipNetToMediaNetAddress*.

Instance	Valeur	Action
f.1.n.n.n.n	m.m.m.m	Pour l’interface avec **ifIndex f,** une entrée de table ARP existante pour l’adresse IP n.n.n.n est remplacée par l’adresse IP m.m.m.m.

ipForwarding Indique si l'hôte de l'agent achemine les datagrammes. Reportez-vous à "Restrictions d'implémentation du démon SNMP", page 9-25.

Instance	Valeur	Action
0	1	Si l'hôte de l'agent possède plusieurs interfaces actives, le noyau TCP/IP est configuré pour l'acheminement des paquets. S'il ne possède qu'une seule interface active, la requête set échoue.
	2	Le noyau TCP/IP sur l'hôte de l'agent est configuré de sorte qu'il n'achemine pas les paquets.

ipDefaultTTL Durée de vie (TTL) par défaut, insérée dans l'en-tête IP des datagrammes générés par l'hôte de l'agent.

Instance	Valeur	Action
0	n	La valeur de durée de vie par défaut, utilisée par le support de protocole IP, est définie comme l'entier n.

ipRouteDest Adresse IP de destination d'une route dans la table des routes.

Instance	Valeur	Action
n.n.n.n	m.m.m.m	La route de destination pour la route n.n.n.n est définie à l'adresse IP m.m.m.m.

ipRouteNextHop Passerelle par laquelle une adresse IP de destination peut être atteinte par l'hôte de l'agent (entrée de la table des routes).

Instance	Valeur	Action
n.n.n.n	m.m.m.m	Une entrée de la table des routes pour atteindre le réseau n.n.n.n via la passerelle m.m.m.m est ajoutée à la table des routes. La portion hôte de l'adresse IP n.n.n.n doit être égale à 0 pour indiquer une adresse de réseau.

ipRouteType Etat d'une entrée de la table des routes sur l'hôte de l'agent (utilisé pour supprimer des entrées).

Instance	Valeur	Action
h.h.h.h	1	Toute route à destination de l'adresse IP de l'hôte h.h.h.h est supprimée.
n.n.n.n	2	Toute route à destination de l'adresse IP de l'hôte n.n.n.n est supprimée.

ipNetToMediaPhysAddress Partie matérielle de l'adresse d'une liaison de table d'adresses sur l'hôte de l'agent (entrée de la table ARP). Même variable MIB que *atPhysAddress*.

Instance	Valeur	Action
f.1.n.n.n.n	hh:hh:hh:hh:hh:hh	Pour l'interface avec **ifIndex f,** toute liaison de table ARP existante pour l'adresse IP n.n.n.n est remplacée par la liaison (n.n.n.n, hh:hh:hh:hh:hh:hh). S'il n'y en a pas, la nouvelle liaison est ajoutée. hh:hh:hh:hh:hh:hh est une adresse matérielle hexadécimale à douze chiffres.

ipNetToMediaNetAddress Adresse IP correspondant à l'adresse matérielle ou physique spécifiée dans *ipNetToMediaPhysAddress*. Même variable MIB que *atNetAddress*.

Instance	Valeur	Action
f.1.n.n.n.n	m.m.m.m	Pour l'interface avec **ifIndex f,** une entrée de table ARP existante pour l'adresse IP n.n.n.n est remplacée par l'adresse IP m.m.m.m.

ipNetToMediaType Type de mappage de l'adresse IP vers l'adresse physique.

Instance	Valeur	Action
f.1.n.n.n.n	1	Pour l'interface avec **ifIndex f,** pour une liaison ARP existante de l'adresse IP vers l'adresse physique, le type de mappage a la valeur 1, ou autre.
	2	Pour l'interface avec **ifIndex f,** pour une liaison ARP existante de l'adresse IP vers l'adresse physique, le type de mappage a la valeur 2, ou n'est pas valide. Un effet secondaire est que l'entrée correspondante de **ipNetMediaTable** est invalidée, c'est-à-dire que l'interface est dissociée de cette entrée **ipNetToMediaTable**.
	3	Pour l'interface avec **ifIndex f,** pour une liaison ARP existante de l'adresse IP vers l'adresse physique, le type de mappage a la valeur 3, ou dynamique.
	4	Pour l'interface avec **ifIndex f,** pour une liaison ARP existante de l'adresse IP vers l'adresse physique, le type de mappage a la valeur 4, ou statique.

snmpEnableAuthenTraps Indique si l'agent **snmpd** est configuré de façon à générer des interruptions *authenticationFailure*.

Instance	Valeur	Action
0	1	L'agent **snmpd** ne générera pas d'interruptions "authentication failure".
	2	L'agent **snmpd** générera des interruptions "authentication failure".

smuxPstatus Etat d'un homologue de protocole SMUX (utilisé pour supprimer des homologues SMUX).

Instance	Valeur	Action
n	1	L'agent **snmpd** ne fait rien.
	2	L'agent **snmpd** arrête de communiquer avec l'homologue SMUX n.

smuxTstatus Etat d'une arborescence SMUX (utilisé pour supprimer des montages d'arborescence MIB).

Instance	Valeur	Action
l.m.m.m._ _ _ .p	1	L'agent **snmpd** ne fait rien.
	2	Démonte le montage SMUX de l'arborescence MIB m.m.m... avec *l* comme longueur d'une instance d'arborescence MIB et *p* la valeur de smuxTpriority.

Les variables ci-après sont définissables, via le démon **snmpd,** conformément à RFC 1229. L'unité sous-jacente peut ne pas autoriser leur définition. Vérifiez ce qui est admis dans chaque cas.

ifExtnsPromiscuous Etat du mode promiscuous sur une unité. Cette opération permet d'activer ou de désactiver le mode promiscuous sur une unité donnée. L'action **snmpd** est finalisée et terminée. Lorsque **snmpd** est instruit de s'arrêter, le mode promiscuous est complètement désactivé, quelles que soient les autres applications sur la machine.

Instance	Valeur	Action
n	1	Active le mode promiscuous pour l'unité n.
	2	Désactive le mode promiscuous pour l'unité n.

ifExtnsTestType Variable d'initiation de test. Lorsqu'elle est définie, le test approprié est lancé pour cette unité. La valeur de cette variable est un identificateur d'objet. La valeur spécifique dépend du type d'unité et du test à exécuter. Actuellement, FullDiplexLoopBack est le seul test défini que **snmpd** sait exécuter.

Instance	Valeur	Action
n	oid	Lance le test spécifié par oid.

ifExtnsRcvAddrStatus Variable d'état d'adresse. Lorsqu'elle est définie, l'adresse spécifiée est créée avec un niveau de durée approprié. **snmpd** permet la définition d'une adresse temporaire uniquement, car il est incapable de définir des enregistrements ODM d'unité et qu'il n'est autorisé qu'à définir des adresses multidestinataires/multidiffusion.

Instance	Valeur	Action
n.m.m.m.m.m.m	1	Ajoute l'adresse à titre ni temporaire ni permanent.
	2	Empêche l'utilisation de l'adresse.
	3	Ajoute l'adresse à titre temporaire.
	4	Ajoute l'adresse à titre permanent.

Les variables ci-après sont définissables, via le démon **snmpd**, conformément à RFC 1231. L'unité sous-jacente peut ne pas autoriser leur définition. Vérifiez ce qui est admis dans chaque cas.

dot5Commands Commande que l'unité token-ring doit exécuter.

Instance	Valeur	Action
n	1	Ne fait rien. Renvoyé.
	2	Demande à l'unité token-ring de s'ouvrir.
	3	Demande au token-ring de se réinitialiser.
	4	Demande à l'unité token-ring de se fermer.

dot5RindSpeed Vitesse ou largeur de bande de l'anneau actuel.

Instance	Valeur	Action
n	1	Vitesse inconnue.
	2	Vitesse d'anneau de 1 mégabits.
	3	Vitesse d'anneau de 4 mégabits.
	4	Vitesse d'anneau de 16 mégabits.

dot5ActMonParticipate L'objet indique si l'unité doit participer ou non au processus de sélection active du moniteur.

Instance	Valeur	Action
n	1	Doit participer.
	2	Ne doit pas participer.

dot5Functional Masque fonctionnel permettant à l'unité token-ring de spécifier les adresses à partir desquelles elle recevra des trames.

Instance	Valeur	Action
n	m.m.m.m.m.m	Masque fonctionnel à définir.

Les variables suivantes sont définies dans la consigne RFC comme étant en lecture seule, mais nous vous conseillons de leur affecter des droits en lecture-écriture. Elles concernent des manipulations d'horloge complexes. Etudiez-les attentivement dans RFC pour bien comprendre leurs interactions. **snmpd** permet au demandeur de les définir, mais l'unité ne le pourra peut-être pas. Pour plus d'informations, consultez la documentation relative au pilote de l'unité. Les variables sont :

- dot5TimerReturnRepeat
- dot5TimerHolding
- dot5TimerQueuePDU
- dot5TimerValidTransmit
- dot5TimerNoToken
- dot5TimerActiveMon
- dot5TimerStandbyMon
- dot5TimerErrorReport
- dot5TimerBeaconTransmit
- dot5TimerBeaconReceive

Les variables ci-après sont définissables, via le démon SNMPD, conformément à RFC 1512. Celui-ci se sert de la norme de protocole FDDI Station Management (SMT) 7.2 pour obtenir des informations. Ceci est déterminé au niveau du microcode. Contrôlez le microcode dans la documentation FDDI pour vérifier que le microcode SMT 7.2 est utilisé.

fddimibSMTUserData Variable contenant 32 octets d'informations utilisateur.

Instance	Valeur	Action
n	chaîne	Stocke 32 octets d'informations utilisateur.

fddimibSMTConfigPolicy Etat des politiques de configuration, notamment l'utilisation de la politique "hold" de maintien en l'état.

Instance	Valeur	Action
n	0	Ne pas utiliser la politique "hold".
	1	Utiliser la politique "hold".

fddimibSMTConnectionPolicy Etat des politiques de connexion dans le noeud FDDI. Voir RFC 1512 pour plus d'informations sur les valeurs définissables spécifiques.

Instance	Valeur	Action
n	k	Définit les politiques de connexion.

fddimibSMTTNotify Horloge, exprimée en secondes, utilisée dans le protocole Neighbor Notification. Sa valeur est comprise entre 2 et 30 secondes (30 secondes par défaut).

Instance	Valeur	Action
n	k	Définit la valeur de l'horloge.

fddimibSMTStatRptPolicy Etat de la génération de trames de compte rendu d'état.

Instance	Valeur	Action
n	1	Le noeud génère des trames de compte rendu d'état pour les événements implémentés.
	2	Le noeud ne crée pas de trames de compte rendu d'état.

fddimibSMTTraceMaxExpiration Cette variable définit la valeur maximale d'expiration de l'horloge pour le suivi.

Instance	Valeur	Action
n	k	Définit l'expiration maximale de l'horloge (en millisecondes).

fddimibSMTStationAction Cette variable provoque l'exécution par l'entité SMT d'une action spécifique. Pour en savoir plus, voir la RFC.

Instance	Valeur	Action
n	k	Définit une action sur l'entité SMIT. Valeurs comprises entre 1 et 8.

fddimibMACRequestedPaths Définit les chemins dans lesquels le MAC (medium access control) doit être inséré.

Instance	Valeur	Action
n.n	k	Définit le chemin demandé pour le MAC.

fddimibMACFrameErrorThreshold
Seuil au-delà duquel un compte rendu d'état du MAC doit être généré. Définit le nombre d'erreurs à partir duquel générer un compte rendu.

Instance	Valeur	Action
n.n	k	Définit le nombre d'erreurs à partir duquel générer un compte rendu d'état MAC.

fddimibMACMAUnitdataEnable
Cette variable détermine la valeur de l'indicateur **MA_UNITDATA_Enable** dans RMT. La valeur initiale et par défaut de cet indicateur est "vrai" (1).

Instance	Valeur	Action
n.n	1	Marque l'indicateur MA_UNITDATA_Enable comme vrai (true).
	2	Marque l'indicateur MA_UNITDATA_Enable comme faux (false).

fddimibMACNotCopiedThreshold
Seuil déterminant à quel moment est généré un compte rendu de condition de MAC.

Instance	Valeur	Action
n.n	k	Définit le nombre d'erreurs à partir duquel générer un compte rendu de condition de MAC.

Les trois variables suivantes, interdépendantes, concernent l'horloge. Avant de les modifier, assurez-vous que vous avez bien assimilé leur fonction, telle que définie dans **RFC 1512**.

- fddimibPATHTVXLowerBound
- fddimibPATHTMaxLowerBound
- fddimibPATHMaxTReq

fddimibPORTConnectionPolicies
Spécifie les politiques de connexion pour le port spécifié.

Instance	Valeur	Action
n.n	k	Définit les politiques de connexion pour le port spécifié.

fddimibPORTRequestedPaths
Cette variable est la liste des chemins permis du port. Le premier octet correspond à "aucun", le deuxième, à "arborescence", et le troisième, à "homologue".

Instance	Valeur	Action
n.n	ccc	Définit les chemins du port.

fddimibPORTLerCutoff Estimation du taux d'erreur de liaison au-delà duquel une connexion de liaison sera rompue. La valeur est comprise entre 10**-4 et 10**-15, et est rapportée comme la valeur absolue du logarithme à base 10 (valeur par défaut : 7).

Instance	Valeur	Action
n.n	k	Définit le LerCutoff du port.

fddimibPORTLerAlarm Estimation du taux d'erreur de liaison au-delà duquel une connexion de liaison génère une alarme. La valeur est comprise entre 10**-4 et 10**-15 et est rapportée comme la valeur absolue du logarithme à base 10 de l'estimation (valeur par défaut : 8).

Instance	Valeur	Action
n.n	k	Définit le LerAlarm du port.

fddimibPORTAction Cette variable entraîne l'exécution d'une action spécifique par le PORT. Pour en savoir plus, voir la RFC.

Instance	Valeur	Action
n	k	Définit une action sur le port défini. Valeurs comprises entre 1 et 6.

Remarque : RFC 1213 décrit toutes les variables des tables *atEntry* et *ipNetToMediaEntry* comme étant en lecture-écriture. Le support de set n'est assuré que pour les variables *atEntry* aux adresses *atPhysAddress* et *atNetAddress*, et pour les variables *ipNetToMediaEntry* aux adresses *ipNetToMediaPhysAddress*, *ipNetToMediaNetAddress*, et de type *ipNetToMediaType*. Les requêtes set acceptées qui spécifient les autres attributs non acceptés dans ces deux tables sont : *atIfIndex* et *ipNetToMediaIfIndex*. Aucune réponse d'erreur n'est renvoyée à l'émetteur de la requête set, mais la requête get suivante montrera que les valeurs originales sont retenues.

RFC 1213 décrit toutes les variables de la table *ipRouteEntry* comme étant en lecture-écriture, sauf *ipRouteProto*. Comme mentionné ci-dessus, le support de set n'est assuré que pour les variables *ipRouteDest*, *ipRouteNextHop* et *ipRouteType*. Pour accepter des requêtes set pouvant spécifier plusieurs attributs de route non supportés, les requêtes set pour les autres variables de la table *ipRouteEntry* sont acceptées : *ipRouteIfIndex*, *ipRouteMetric1*, *ipRouteMetric2*, *ipRouteMetric3*, *ipRouteMetric4*, *ipRouteMetric5*, *ipRouteAge* et *ipRouteMask*. Aucune réponse d'erreur n'est renvoyée à l'émetteur de la requête set, mais la requête get suivante montrera que les valeurs originales sont retenues. Le démon **snmpd** ne coordonne pas le routage avec le démon **routed**. Si le démon **gated** s'exécute et a enregistré la variable *ipRouteTable* avec le démon **snmpd**, les requêtes set sur *ipRouteTable* ne sont pas autorisées.

RFC 1229 décrit les variables définissables ; **snmpd** permet leur définition. Pour les exceptions, reportez-vous aux entrées précédentes.

Exemples

Les exemples suivants utilisent la commande **snmpinfo**. Le nom de communauté par défaut de *snmpinfo*, public, est supposé avoir accès en lecture-écriture à la sous-arborescence MIB correspondante :

```
snmpinfo -m set sysContact.0="Primary contact: Bob Smith, office
phone: 555-5555, beeper: 9-123-4567. Secondary contact: John
Harris, phone: 555-1234."
```

Cette commande affecte à `sysContact.0` la valeur de la chaîne spécifiée. S'il existe déjà une entrée pour `sysContact.0`, elle est remplacée.

```
snmpinfo -m set sysName.0="bears.austin.ibm.com"
```

Cette commande affecte à `sysName.0` la valeur de la chaîne spécifiée. S'il existe déjà une entrée pour `sysName.0`, elle est remplacée.

```
snmpinfo -m set sysLocation.0="Austin site, building 802, lab
3C-23, southeast corner of the room."
```

Cette commande affecte à `sysLocation.0` la valeur de la chaîne spécifiée. S'il existe déjà une entrée pour `sysLocation.0`, elle est remplacée.

```
snmpinfo -m set ifAdminStatus.2=2
```

Désactive la carte d'interface réseau dont l'ifIndex a la valeur 2. Si la valeur affectée est égale à 1, la carte d'interface est activée.

```
snmpinfo -m set atPhysAddress.2.1.192.100.154.2=02:60:8c:2e:c2:00
snmpinfo -m set
ipNetToMediaPhysAddress.2.1.192.100.154.2=02:60:8c:2e:c2:00
```

Changent l'adresse matérielle dans l'entrée de la table ARP de `192.100.154.2` en `02:60:8c:2e:c2:00`. Elles affectent la même entrée de table ARP. La variable MIB *atPhysAddress* est une variable dépréciée, remplacée par la variable MIB *ipNetToMediaPhysAddress*. Donc, *atPhysAddress* et *ipNetToMediaPhysAddress* ont accès à la même structure dans la table ARP du noyau TCP/IP.

```
snmpinfo -m set atNetAddress.2.1.192.100.154.2=192.100.154.3
snmpinfo -m set
ipNetToMediaNetAddress.2.1.192.100.154.2=192.100.154.3
```

Changent l'adresse IP dans l'entrée de la table ARP de `192.100.154.2` en `192.100.154.3`. Elles affectent la même entrée de table ARP. La variable MIB *atNetAddress* est une variable dépréciée, remplacée par la variable MIB *ipNetToMediaNetAddress*. Ainsi, *atNetAddress* et *ipNetToMediaNetAddress* ont accès à la même structure dans la table ARP du noyau TCP/IP.

```
snmpinfo -m set ipForwarding.0=1
```

Définit le noyau TCP/IP de sorte qu'il puisse acheminer les paquets si l'hôte de l'agent a plusieurs interfaces actives. S'il n'en a qu'une, la requête set échoue et l'agent **snmpd** renvoie l'erreur *badValue*.

```
snmpinfo -m set ipDefaultTTL=50
```

Permet à un datagramme IP utilisant la durée de vie (TTL) par défaut de passer par des passerelles (50 maximum) avant d'être rejeté. A chaque traitement du datagramme par une passerelle, cette dernière décrémente de 1 le champ de durée de vie. En outre, chaque passerelle décrémente ce champ du nombre de secondes qu'a attendu le datagramme pour être traité avant d'être transmis à la destination suivante.

```
snmpinfo -m set ipRouteDest.192.100.154.0=192.100.154.5
```

Définit l'adresse IP de destination de la route associée à `192.100.154.0` comme étant `192.100.154.5` (en supposant que la route `192.100.154` existait déjà).

```
snmpinfo -m set ipRouteNextHop.192.100.154.1=129.35.38.47
```

Définit une route vers l'hôte `192.100.154.1` via la passerelle hôte `129.35.38.47` (en supposant que la route `192.100.154.1` existait déjà).

```
snmpinfo -m set ipRouteNextHop.192.100.154.0=192.100.154.7
```

Définit une route vers le serveur de classe C `192.100.154` via la passerelle hôte `192.100.154.7` (en supposant que la route `192.100.154.0` existait déjà). Remarquez que la partie hôte de l'adresse doit être 0 pour indiquer une adresse de réseau.

```
snmpinfo -m set ipRouteType.192.100.154.5=2
```

Supprime toute route pour l'hôte `192.100.154.5`.

```
snmpinfo -m set ipRouteDest.129.35.128.1=129.35.128.1
                ipRouteType.129.35.128.1=3
            ipRouteNextHop.129.35.128.1=129.35.128.90
```

Crée une nouvelle route depuis l'hôte `129.35.128.90` jusqu'à `129.35.128.1` comme passerelle.

```
snmpinfo -m set ipNetToMediaType.2.1.192.100.154.11=4
```

Définit l'entrée de la table ARP en `192.100.154.11` comme statique.

```
snmpinfo -m set snmpEnableAuthenTraps=2
```

Indique à l'agent **snmpd** sur l'hôte spécifié de ne pas générer d'interruptions de type *authenticationFailure*.

```
snmpinfo -m set smuxPstatus.1=2
```

Annule la validité de l'homologue SMUX 1. L'effet secondaire est que la connexion entre l'agent **snmpd** et cet homologue SMUX prend fin.

```
snmpinfo -m set smuxTstatus.8.1.3.6.1.2.1.4.21.0=2
```

Annule la validité ou supprime le montage de l'arborescence SMUX `1.3.6.1.2.1.4.21`, la table *ipRoute*Table. Le premier nombre de l'instance indique le nombre de niveaux dans l'identificateur d'arborescence SMUX. Le dernier nombre indique la priorité smuxTpriority. Dans cet exemple, il y a huit niveaux dans l'identificateur de l'arborescence SMUX : `1.3.6.1.2.1.4.21`. La priorité 0 est la plus élevée.

```
snmpinfo -m set ifExtnsPromiscuous.1=1 ifExtnsPromiscuous.2=2
```

Active le mode "promiscuous" pour la première unité de la table d'interfaces et le désactive pour la deuxième unité.

```
snmpinfo -m set ifExtnsTestType.1=testFullDuplexLoopBack
```

Lance le test testFullDuplexLoopBack sur l'interface 1.

```
snmpinfo -m set ifExtnsRcvAddrStatus.1.129.35.128.1.3.2=2
```

Indique à l'interface 1 de supprimer l'adresse physique `129.35.128.1.3.2` de la liste des adresses acceptables.

```
snmpinfo -m set dot5Commands.1=2
```

Demande à la première interface d'exécuter une ouverture.

```
snmpinfo -m set dot5RingSpeed.1=2
```

Indique à la première interface de définir sa vitesse d'anneau à 1 mégabit.

```
snmpinfo -m set dot5ActMonParticipate.1=1
```

Indique à la première interface de participer au processus de sélection du moniteur actif.

```
snmpinfo -m set dot5Functional.1=255.255.255.255.255.255
```

Définit le masque d'adresse fonctionnel de sorte que tout soit autorisé.

```
snmpinfo -m set fddimibSMTUserData.1="Greg's Data"
```

Définit les données utilisateur sur la première entité SMT comme "Greg's Data".

```
snmpinfo -m set fddimibMACFrameErrorThreshold.1.1=345
```

Définit le seuil des erreurs de trame à 345 sur le premier MAC de la première entité SMT.

Remarque : Toutes les variables décrites sont définissables par l'une ou l'autre des méthodes indiquées précédemment.

Pour en savoir plus sur les protocoles et les adresses Internet, reportez-vous à *Protocole ARP*, page 3-24 et à *Adresses Internet*, page 3-56.

Conformité RFC du démon SNMP

RFC 1157 exige que chaque affectation de variable d'une requête set "soit effectuée comme si elle était définie simultanément conformément à toutes les autres assignations spécifiées dans le même message" (pages 25 et 26 de la RFC). Autrement dit, une requête set avec plusieurs paires ID d'instance/valeur doit être traitée globalement ou pas du tout (*all–or–none*) : soit toutes les nouvelles valeurs sont affectées sans erreur, soit aucune des variables de la requête n'est modifiée. On parle également de "atomic commit with rollback" (validation atomique avec annulation).

Remarque : RFC 1157 ne considère pas les questions de cohérence ou de dépendance en fonction d'un ordre. Des dépendances par ordre peuvent exister, du type :

```
snmpinfo -m set -h host1
ipNetToMediaPhysAddress.f.1.n.n.n=hh:hh:hh:hh:hh:hh\
ifAdminStatus.f=1

snmpinfo -m set -h host1 iproutenexthop.n.n.n.n=m.m.m.m
ifAdminStatus.f=1
```

La carte avec **ifIndex f** doit être activée avant qu'une entrée de table d'adresses puisse lui être associée ou qu'une route puisse être établie, qui atteigne une passerelle via cette carte. Dans ce cas, l'ordre des variables est important et doit être inversé par rapport à celui présenté ci-dessus. Si la politique "atomic commit" de RFC 1157 est suivie à la lettre, les requêtes set ordonnées décrites ci-dessus ont des conséquences imprévisibles.

Pour les variables MIB acceptées, l'agent **snmpd** effectue un précontrôle des valeurs spécifiées pour les variables MIB dans la requête set. Dès qu'une valeur ne répond pas aux critères du précontrôle, la requête set est rejetée. La véritable mise en oeuvre de la requête set est, techniquement parlant, un pis-aller, et non un réel "atomic commit and rollback".

Au cours du processus "set", lorsque l'agent **snmpd** modifie la valeur des variables MIB, si une panne se produit, les valeurs d'origine des variables MIB déjà définies ne sont pas restaurées.

RFC 1213 décrit toutes les variables de la table ipRouteEntry comme étant en lecture-écriture. Comme décrit auparavant, le support de "set" n'est assuré que pour **ipRouteDest**, **ipRouteType** et **ipRouteNextHop** (voir remarque). Pour accepter des requêtes set pouvant spécifier plusieurs attributs de route non pris en charge (comme **ipRouteMetric1** ou **ipRouteProto**), les requêtes set pour ces variables non prises en charge sont acceptées. Aucune réponse d'erreur n'est renvoyée au demandeur, mais une requête get suivante montrera que les valeurs d'origine ont été conservées.

Restrictions d'implémentation du démon SNMP

L'implémentation actuelle de l'agent SNMP (Simple Network Management Protocol) *n'est pas* dotée :

- d'interface utilisateur pour un support d'agent mandataire (proxy),
- d'un support d'authentification non trivial.

Toutes les valeurs définies dans RFC 1213 ne sont pas prises en charge, comme indiqué dans la remarque suivante :

> **Remarque :** Une requête set pour **ipRouteType 2** (non valide) entraîne la suppression d'une route. Une requête get ne renverra jamais cette valeur pour une route existante.

Veillez à respecter les restrictions d'implémentation suivantes :

- Pour pouvoir être activée/désactivée via la variable **ifAdminStatus,** une interface doit au préalable être activée par une commande **ifconfig** locale. Le seul moyen d'associer une adresse IP (Internet Protocol) à une interface est de lancer une commande **ifconfig** locale.
- L'agent **snmpd** ne permet pas de modifier l'adresse IP d'une carte d'interface. Seule une commande **ifconfig** locale peut le faire.
- La taille des messages envoyés ne doit pas dépasser 9 ko (9216 octets). La taille des messages reçus ne doit pas dépasser 40 ko (40960 octets).

Si vous affectez à la variable MIB **ipForwarding** la valeur 1, indiquant que le noyau TCP/IP doit acheminer les paquets, l'agent **snmpd** effectue quelques contrôles d'interface avant d'autoriser l'opération "set". S'il existe plusieurs interfaces actives, la variable MIB **ipForwarding** est définie à 1, de même que l'option configurable du noyau TCP/IP **ipforwarding.** Sinon, l'agent **snmpd** n'effectue pas l'opération "set" et une erreur *badValue* est renvoyée.

Fonction de journalisation du démon SNMP

Les activités de journalisation pour le démon **snmpd** peuvent être lancées :

- à partir de la ligne de commande de **snmpd,**
- à partir du fichier de configuration de **snmpd**,
- par le démon **syslogd**.

Le niveau de mise au point des messages de journalisation **snmpd** est configurable par l'utilisateur. Le niveau de mise au point peut être :

0	Tous les messages de type NOTICES, EXCEPTIONS et FATAL
1	Messages de niveau 0 et messages de type DEBUG
2	Messages de niveau 1 plus un vidage hexadécimal des paquets de requête et de réponse
3	Messages de niveau 2 plus une version anglaise des paquets de requête et de réponse.

Par défaut, le niveau de mise au point est 0. Les messages de niveau 3 ne sont pas écrits par le démon **syslogd**.

Si le démon **snmpd** est configuré pour la journalisation, vous pouvez l'activer ou la désactiver en émettant un signal **SIGUSR1** ou **kill –30** en direction du démon **snmpd**. Si le démon **snmpd** est appelé sous le contrôle SRC, vous pouvez également utiliser les commandes **traceson** et **tracesoff** de SRC pour lancer ou arrêter la journalisation. Si la journalisation est activatée, la commande **tracesoff** l'arrête. De même, si la journalisation est temporairement désactivée,la commande **traceson** la réactive. Si le démon **snmpd** n'est pas configuré pour la journalisation, ces commandes n'ont aucun effet.
Ces commandes n'ont aucun effet sur la journalisation effectuée par le démon **syslogd**.

Si le fichier journal atteint sa taillelimite, le démon **snmpd** le permute. Le démon **snmpd** maintient jusqu'à quatre niveaus de fichiers journaux permutés. Par exemple, si vous appelez le fichier journal FichJourn, la rotation s'effectue comme suit :

- FichJourn.3 est supprimé.
- FichJourn.2 est renommé FichJourn.3.
- FichJourn.1 est renommé FichJourn.2.
- FichJourn.0 est renommé FichJourn.1.
- FichJourn est renommé FichJourn.0.
- La journalisation continue dans FichJourn.

Si vous effectuez simultanément une journalisation avec **syslogd**, un message est enregistré par le démon **syslogd**, indiquant que les fichiers journaux sont en cours de rotation. Le fichier journal de **syslogd** n'est pas permuté par le démon **snmpd**.

Si le démon **snmpd** est appelé sous contrôle de SRC, la commande **lssrc** assortie de l'option état détaillé affiche la liste des paramètres de journalisation **snmpd**. La commande **lssrc** n'affiche pas d'informations sur les activités de journalisation **syslogd**.

Journalisation à partir de la ligne de commande snmpd

Pour lancer la journalisation à partir de la ligne de commande **snmpd**, il faut spécifier l'indicateur **–f** à l'appel de **snmpd**. Si l'indicateur **–f** n'est pas spécifié, vosu ne pourrez pas lancer la journalisation à partir de la ligne de commande. En revanche, si *-f* est spécifié, le chemin d'accès complet et le nom du fichier de journalisation doivent être indiqués dans la mesure où le démon **snmpd** "bifurque", passant au répertoire racine lors du lancement. Si le démon **snmpd** ne peut ouvrir le fichier, le démon **snmpd** lance la journalisation à partir du fichier de configuration. Si **syslogd** traite également les messages de journalisation **snmpd**, un message de type EXCEPTIONS est enregistré dans le journal **syslogd**, expliquant la raison de l'échec de l'ouverture du fichier journal **snmpd**. Si le fichier spécifié avec **-f** est ouvert correctement, il ne peut être modifié pendant l'exécution du démon **snmpd**.

Le niveau de débogage est spécifié sur la ligne de commande **snmpd** via l'indicateur **–d**. Si l'indicateur **–d** n'est pas spécifié, le niveau de débogage prend par défaut la valeur 0. Ce niveau ne peut être modifié pendant l'exécution du démon **snmpd**.

La taille du fichier journal est **unlimited** (illimitée), c'est-à-dire la taille maximale acceptée par le système.

Si la journalisation est lancée depuis la ligne de commande, les entrées de journalisation dans le fichier de configuration sont ignorées au lancement et pendant le rafraîchissement du démon **snmpd**.

Reportez-vous à la commande **snmpd** dans le manuel dans *AIX Commands Reference*.

Journalisation à partir du fichier de configuration

Dans ce cas, l'indicateur **–f** ne doit pas être spécifié sur la ligne de commande **snmpd**. Si l'indicateur **–d** est spécifié sur la ligne de commande**snmpd**, le niveau de débogage défini par l'indicateur **–d** devient le niveau de débogage par défaut. Si l'indicateur **–d** n'est pas spécifié sur la ligne de commande **snmpd**, le niveau de débogage par défaut est 0.

Les paramètres de journalisation sont spécifiés dans les entrées "journalisation" du fichier de configuration **snmpd**. Parmi ceux qui sont configurables : nom du fichier journal, taille maximale du fichier journal, niveau de débogage et activation. Si le nom du fichier journal n'est pas précisé, la journalisation n'est pas activée. Comme le démon **snmpd** "bifurque", passant au répertoire racine lors du lancement, il faut spécifier le chemin d'accès complet au fichier journal. L'activation (définie par défaut) est désactivée. Ainsi, si le paramètre d'activation n'est pas spécifié comme *enabled* (activé), la journalisation dans le fichier journal n'a pas lieu.

Par défaut, la taille du fichier journal est **unlimited** (illimitée), c'est-à-dire la taille maximale acceptée par le système.

Le fichier de configuration de **snmpd** est lu au lancement, et en cas de rafraîchissement de **snmpd**. Il est de ce fait inutile de spécifier les paramètres de journalisation avant l'appel du démon **snmpd**. Comme le fichier est relu au rafraîchissement de **snmpd** (si **snmpd** est lancé sous le contrôle SRC) ou après un signal SIGHUP (**kill –1**), il est possible de spécifier à tout moment ces paramètres de journalisation. En outre, ils peuvent être modifiés à tout moment pendant l'exécution du démon **snmpd**.

Pour en savoir plus sur la configuration du démon **snmpd** pour une journalisation à partir du fichier de configuration, reportez-vous au fichier **snmpd.conf**.

Journalisation par le démon syslogd

La journalisation lancée par le démon **syslogd** peut être indépendante ou combinée à une journalisation lancée depuis la ligne de commande **snmpd** ou le fichier de configuration.

Pour configurer le démon **syslogd** à enregistrer des messages pour le démon **snmpd**, vous devez être utilisateur racine. Editez le fichier **/etc/syslog.conf** et ajoutez-y une entrée du type :

```
daemon.debug      /var/tmp/snmpd.syslog
```

Pour que le démon **syslogd** y enregistre les messages de journalisation du démon **snmpd**, le fichier **/var/tmp/snmpd.syslog** doit exister avant que le démon **syslogd** ne relise le fichier de configuration **/etc/syslog.conf.** Pour créer ce fichier, entrez :

```
touch /var/tmp/snmpd.syslog
```

Pour forcer le démon **syslogd** à relire son fichier de configuration, entrez ensuite :

```
refresh –s syslogd
```

Le démon **syslogd** enregistre *tous* les messages du démon dans ce fichier journal, et pas uniquement les messages de journalisation **snmpd**.

Si le démon **syslogd** est configuré pour enregistrer des messages à partir de la fonction de démon au niveau de gravité LOG_DEBUG (ou supérieur) de **syslogd**, tous les messages au niveau 2 (ou inférieur) de débogage de **snmpd**, issus du démon **snmpd**, peuvent être enregistrés dans un fichier configuré de **syslogd**. Si le niveau 3 est spécifié comme niveau de débogage de **snmpd**, le démon **syslogd** n'enregistrera que des messages de niveau 2 de **snmpd**.

Si la journalisation ne doit être traitée que par le démon **syslogd**, il faut d'abord configurer le démon **syslogd** en vue de la journalisation, comme décrit ci-dessus. Le niveau de débogage du démon **snmpd** doit être spécifié sur la ligne de commande avec l'option **-d** ou dans le fichier de configuration, dans le champ *level=Valeur* d'une entrée de journalisation. Le niveau de débogage par défaut est 0. Si la journalisation est lancée à partir du fichier de configuration **snmpd**, le niveau de débogage peut changer pendant l'exécution du démon **snmpd**.

Le signal **SIGUSR1** signal (**kill –30**) et les commandes SRC **traceson** et **tracesoff** sont sans effet sur la journalisation par le démon **syslogd**.

Aucune journalisation n'a lieu si les démons **snmpd** et **syslogd** ne sont pas configurés pour enregistrer des messages, via la ligne de commande ou le fichier de configuration **snmpd**.

Incidents liés au démon SNMP

Si l'agent **snmpd** ne se comporte pas comme il le devrait, voici quelques indices pour vous aider à diagnostiquer et corriger le problème. En cas d'incident, il est fortement recommandé de démarrer l'agent **snmpd** en spécifiant une journalisation. En cas d'incident à l'appel du démon **snmpd**, il est conseillé de configurer le démon **syslogd** pour la journalisation au niveau de la fonction de démon et au niveau de gravité DEBUG. Pour plus d'informations sur la journalisation de **snmpd**, reportez-vous à "Fonction de journalisation du démon de SNMP", page 9-26, à la commande **snmpd** et au fichier **snmpd.conf**.

Interruption prématurée

Si le démon **snmpd** s'arrête dès son appel :

- La cause de l'arrêt de **snmpd** est consignée dans le fichier journal **snmpd** ou **syslogd** configuré. Consultez ce fichier pour prendre connaissance du message d'erreur **FATAL**.

  Solution : Corrigez le problème et relancez le démon **snmpd**.

- La syntaxe de la ligne de commande **snmpd** est incorrecte. Si vous avez appelé la commande **snmpd** sans SRC (System Resource Controller), la syntaxe requise s'affiche à l'écran. Si vous avez appelé le démon **snmpd** sous SRC (System Resource Controller), la syntaxe requise ne s'affiche pas à l'écran. Consultez le fichier journal pour connaître la syntaxe appropriée.

  Solution : Corrigez la syntaxe de la commande **snmpd.**

- Seul l'utilisateur racine doit appeler le démon **snmpd**. L'agent **snmpd** n'est pas exécuté s'il n'est pas appelé par l'utilisateur racine.

  Solution : Ouvrez une session utilisateur racine et relancez le démon **snmpd**.

- Le fichier **snmpd.conf** doit appartenir à l'utilisateur racine. L'agent **snmpd** vérifie la propriété du fichier de configuration. Si le fichier n'appartient pas à l'utilisateur racine, l'agent **snmpd** s'arrête, ceci étant considéré comme une erreur fatale.

  Solution : Vérifiez que vous êtes connecté en tant qu'utilisateur racine, changez le propriétaire du fichier de configuration et relancez le démon **snmpd**.

- Le fichier **snmpd.conf** doit exister. Si vous n'avez pas spécifié le fichier de journalisation sur la ligne de commande **snmpd** via l'indicateur **–c**, c'est le fichier **/etc/snmpd.conf** qui doit exister. Si vous avez accidentellement supprimé le fichier **/etc/snmpd.conf**, réinstallez l'image **bos.net.tcp.client** ou reconstituez le fichier avec les entrées de configuration adéquates, telles que définies dans la page man du fichier **snmpd.conf**. Si vous aviez vraiment spécifié le fichier de configuration sur la ligne de commande **snmpd** via l'indicateur **–c**, vérifiez que ce fichier existe et qu'il appartient à l'utilisateur racine. Vous devez spécifier le chemin d'accès complet et le nom du fichier de configuration si vous ne voulez pas utiliser le fichier **/etc/snmpd.conf** par défaut.

  Solution : Assurez-vous de l'existence du fichier de configuration spécifié et de son appartenance à l'utilisateur racine. Relancez le démon **snmpd**.

- Il y a déjà une liaison avec le **port udp 161**. Vérifiez que le démon **snmpd** n'est pas déjà en cours d'exécution. Lancez la commande **ps –eaf | grep snmpd** pour déterminer si un processus du démon **snmpd** est déjà en cours. Un seul agent **snmpd** peut effectuer la liaison au **port udp 161**.

  Solution : Tuez l'agent **snmpd** existant ou n'essayez pas de démarrer un autre processus du démon **snmpd**.

Défaillance du démon

Si le démon **snmpd** échoue lorsque vous émettez un signal **refresh** ou **kill -1** :

- La cause de l'arrêt est enregistrée dans le fichier journal **snmpd** ou **syslogd** configuré. Recherchez dans l'un ou l'autre le message d'erreur FATAL.

  Solution : Corrigez le problème et relancez le démon **snmpd**.

- Vérifiez que vous avez spécifié le chemin d'accès complet et le nom du fichier de configuration à l'appel du démon **snmpd**. Le démon **snmpd** "bifurque", passant au répertoire racine lorsqu'il est appelé. Si vous n'avez pas spécifié le nom complet du fichier, l'agent **snmpd** ne peut pas le trouver lors d'un rafraîchissement. Il s'agit d'une erreur fatale qui entraîne l'arrêt prématuré de l'agent **snmpd**.

  Solution : Spécifiez le chemin d'accès ccomplet et le nom du fichier de configuration **snmpd**. Vérifiez qu'il appartient à l'utilisateur racine. Relancez le démon **snmpd**.

- Vérifiez que le fichier de configuration du **snmpd** existe encore. Il peut avoir été malencontreusement supprimé après l'appel de l'agent **snmpd**. Si l'agent **snmpd** ne peut pas l'ouvrir, l'agent **snmpd** s'arrête prématurément.

  Solution : Recréez le fichier de configuration **snmpd**, assurez-vous qu'il appartient à l'utilisateur racine et relancez le démon **snmpd**.

Accès impossible aux variables MIB

Si l'agent **snmpd** ne peut accéder aux variables MIB, ou s'il s'exécute mais que l'application du gestionnaire SNMP (Simple Network Management Protocol) dépasse le délai d'attente d'une réponse de l' agent **snmpd** :

- Vérifiez la configuration réseau de l'hôte sur lequel s'exécute l'agent **snmpd** à l'aide de la commande **netstat –in**. Vérifiez que l'unité lo0, en boucle, est active. Si l'unité n'est pas active, un * (astérisque) est affiché en regard de lo0. Pour que l'agent **snmpd** serve les requêtes, lo0 doit être active.

  Solution : Emettez la commande suivante pour démarrer l'interface de boucle :

  ```
  ifconfig lo0 inet up
  ```

- Vérifiez que le démon **snmpd** a une route conduisant à l'hôte sur lequel vous avez émis les requêtes.

  Solution : Sur l'hôte sur lequel s'exécute le démon **snmpd**, ajoutez une route conduisant à l'hôte sur lequel la requête SNMP a émis la commande **route add**. Reportez-vous à la commande **route**.

- Vérifiez que le nom de l'hôte et son adresse IP sont les mêmes.

  Solution : Redéfinissez le nom de l'hôte pour le faire correspondre à son adresse IP.

- Vérifiez si *localhost* (hôte local) est défini comme adresse IP de lo0.

  Solution : Définissez que *localhost* est à la même adresse que celle utilisée par l'adresse IP de lo0 (généralement `127.0.0.1`).

Accès impossible aux variables MIB dans une entrée de communauté

Si une entrée de communauté est spécifiée dans le fichier de configuration avec un nom de vue MIB, mais qu'il est impossible d'accéder aux variables MIB :

- Vérifiez l'entrée de communauté. Si vous y avez indiqué un nom de vue, tous les champs de cette entrée sont obligatoires.

  Solution : Spécifiez tous les champs de l'entrée de la communauté dans le fichier de configuration. Rafraîchissez l'agent **snmpd** et relancez la requête.

- Assurez-vous que le mode d'accès défini dans l'entrée de la communauté correspond à votre type de requête. Si vous émettez une requête **get** ou **get–next**, vérifiez que la communauté est dotée de droits en lecture seule ou en lecture-écriture. Si vous émettez une requête **set**, vérifiez qu'elle est dotée de droits en lecture-écriture.

  Solution : Corrigez le mode d'accès dans l'entrée de la communauté. Rafraîchissez l'agent **snmpd** et relancez la requête.

- Assurez-vous que vous avez spécifié une entrée de vue correspondant au nom de vue indiqué dans l'entrée de communauté. Faute de quoi, l'agent **snmpd** interdit l'accès à cette communauté. Il est impératif de spécifier une entrée de vue pour une entrée de communautée dans le fichier de configuration.

  Solution : Spécifiez une entrée de vue correspondant au nom de vue indiqué dans l'entrée de la communauté. Rafraîchissez l'agent **snmpd** et relancez la requête.

- Si vous avez spécifié `iso` comme sous-arborescence MIB pour votre entrée de vue, assurez-vous d'avoir indiqué `iso.3`. L'instance de `3` est requise pour que l'agent **snmpd** ait accès à la portion `org` de l'arborescence `iso`.

  Solution : Spécifiez `iso.3` comme sous-arborescence MIB dans l'entrée de vue. Rafraîchissez l'agent **snmpd** et relancez la requête.

- Vérifiez l'*adresse IP* et le *masque de réseau* dans l'entrée de la communauté. Vérifiez que l'hôte à partir duquel vous émettez la requête SNMP est inclus dans la communauté spécifiée.

  Solution : Modifiez les champs *IP address* (adresse IP) et *network mask* (masque de réseau) dans l'entrée de communauté du fichier de configuration pour y inclure l'hôte à partir duquel vous émettez la requête SNMP.

Absence de réponse de l'agent

Si l'*adresse IP* de la communauté est 0.0.0.0, mais que l'agent **snmpd** ne répond pas :

- Vérifiez le champ *network mask* (masque de réseau) dans l'entrée de la communauté. Pour donner un accès général à ce nom de communauté, le champ *network mask* doit avoir la valeur **0.0.0.0**. Si vous avez affecté au champ *network mask* la valeur **255.255.255.255**, vous avez configuré l'agent **snmpd** de façon à interdire toute requête avec le nom de communauté spécifié.

  Solution : Donnez la valeur 0.0.0.0 au champ *network mask* (masque de réseau) de l'entrée de la communauté. Rafraîchissez l'agent **snmpd** et relancez la requête.

- Assurez-vous que le mode d'accès défini dans l'entrée de la communauté correspond à votre type de requête. Si vous émettez une requête **get** ou **get–next**, vérifiez que la communauté est dotée de droits en lecture seule ou en lecture-écriture. Si vous émettez une requête **set**, vérifiez qu'elle est dotée de droits en lecture-écriture.

  Solution : Corrigez le mode d'accès dans l'entrée de la communauté. Rafraîchissez l'agent **snmpd** et relancez la requête.

Message noSuchName

Si, lors d'une tentative de définition d'une variable MIB que l'agent **snmpd** est censé prendre en charge, le message d'erreur **noSuchName** est renvoyé :

La requête set émise n'incluait peut-être pas de nom de communauté correspondant à une communauté autorisée avec un accès en écriture. Le protocole SNMP spécifie qu'une requête set mentionnant une communauté avec des droits d'accès inadéquats doit recevoir en réponse le message d'erreur **noSuchName**.

Solution : Emettez la requête **set** avec le nom d'une communauté dotée de droits d'accès en écriture et comprenant l'hôte à partir duquel est émise la requête **set**.

Chapitre 10. Système de fichiers NFS

Ce chapitre fournit des informations sur NFS (Network File System), mécanisme de stockage des fichiers sur le réseau. Les sujets suivants sont traités :

Système de fichiers NFS : généralités

Le système NFS (Network File System) est un système de fichiers distribués, donnant aux utilisateurs accès aux fichiers et répertoires sur des ordinateurs distants - ils ont ainsi la possibilité de les traiter comme s'il s'agissait de fichiers et répertoires locaux. L'utilisateur dispose des commandes du système d'exploitation pour créer, supprimer, lire, écrire ou définir les attributs de ces répertoires et de ces fichiers.

Le module NFS contient les commandes et démons de NFS, NIS (Network Information Service) et autres services. Mais, bien qu'ils soient installés simultanément, NFS et NIS constituent deux modules distincts, configurés et administrés indépendamment. Reportez–vous au *AIX 4.3 NIS/NIS+ Guide* pour plus de détails sur NIS et NIS+.

AIX prend en charge la dernière mise à jour du protocole NFS, NFS version 3. AIX fournit également une version 2 de NFS client et serveur, et garantit de la compatibilité ascendante avec les bases d'installation clients et serveurs NFS existantes.

Cette section traite des points suivants :

Services NFS

Les services NFS sont fournis via une relation client-serveur. Les ordinateurs qui rendent leurs *systèmes de fichiers*, leurs *répertoires* et d'autres ressources accessibles à distance sont appelés des *serveurs.* Le fait de rendre ces ressources disponibles est appelé *exportation*. Les ordinateurs, ou les processus qu'ils exécutent, qui utilisent les ressources d'un serveur sont dits *clients*. Lorsqu'un client *monte* un système de fichiers exporté par un serveur, il a accès aux fichiers du serveur (l'accès aux répertoires peut être limité à certains clients).

Les principaux services NFS sont les suivants :

Service Mount	Via le démon **/usr/sbin/rpc.mountd** sur le serveur et la commande **/usr/sbin/mount** sur le client.
Remote File access	Via le démon **/usr/sbin/nfsd** sur le serveur et la commande **/usr/sbin/biod** sur le client.
Service Remote execution	Via le démon **/usr/sbin/rpc.rexd** sur le serveur et la commande **/usr/sbin/on** sur le client.
Service Remote System Statistics	A partir du démon **/usr/sbin/rpc.rstatd** sur le serveur et la commande **/usr/bin/rup** sur le client.
Service Remote User Listing	A partir du démon **/usr/lib/netsvc/rusers/rpc.rusersd** sur le serveur et la commande **/usr/bin/rusers** sur le client.

Service Boot Parameters	Fournit des paramètres d'amorçage aux clients sans disque SunOS via le démon **/usr/sbin/rpc.bootparamd** sur le serveur.
Service Remote Wall	À partir du démon **/usr/lib/netsvc/rwall/rpc.rwalld** sur le serveur et de la commande **/usr/sbin/rwall** sur le client.
Service Spray	Envoie un flot unilatéral de paquets RPC via le démon **/usr/lib/netsvc/spray/rpc.sprayd** sur le serveur et la commande **/usr/sbin/spray** sur le client.
Service PC authentication	Fournit un service d'authentification utilisateur pour PCNFS via le démon **/usr/sbin/rpc.pcnfsd** sur le serveur.

Remarque : Un ordinateur peut être simultanément serveur NFS et client NFS.

Un serveur NFS est *sans état*. C'est-à-dire qu'il n'a à mémoriser aucune information concernant les transactions de ses clients. En d'autres termes, les transactions NFS sont atomiques : une transaction correspond à une et une seule opération complète sur un fichier. C'est le client qui doit mémoriser les informations requises pour les usages ultérieurs de NFS.

Listes de contrôle d'accès (ACL) sous NFS

NFS prend en charge les listes de contrôle d'accès (ACL), mais ceci n'est plus défini par défaut. Pour utiliser les listes de contrôle d'accès avec NFS, spécifiez l'option **acl** avec l'indicateur NFS **–o**, comme illustré dans l'exemple suivant :

```
mount –o acl
```

La prise en charge des ACL est gérée par un programme RPC qui assure l'échange des informations sur ces listes entre clients et serveurs. Le support ACL n'a pas d'incidence sur les spécifications du protocole NFS : il s'agit d'une fonction distincte.

Le système d'exploitation ajoute les ACL au système de fichiers standard. Le protocole NFS standard ne les prenant pas en charge, les ACL ne sont pas visibles des clients NFS standard. Des surprises sont ainsi possibles. Un utilisateur d'un client NFS peut, par exemple, présumer qu'il a accès à un fichier, au vu des bits d'octroi de droits, et se retrouver interdit d'accès car les ACL associées au fichier ont modifié les droits. Les droits sur un serveur étant octroyés selon l'ACL associée au serveur, un utilisateur sur une machine cliente peut donc se voir notifier une erreur relative aux droits d'accès.

Lorsqu'un client tente un premier accès à un système de fichiers monté distant, il commence par essayer de contacter le programme RPC ACL sur le serveur.

S'il s'agit d'un serveur Version 3.2, le client consulte l'ACL associée au fichier avant d'accorder le droit d'accès au programme sur le client. Le client réagit alors comme il se doit lorsque la demande est envoyée vers le serveur. En outre, les commandes **aclget**, **aclput** et **aledit** sont disponibles sur le client pour manipuler les ACL.

Remarque : NFS n'utilise plus par défaut les listes de contrôle d'accès.

Système de fichiers cache (CacheFS)

Le système de fichiers cache (CacheFS) est un mécanisme de cache qui améliore les performances et l'évolutivité du serveur NFS en réduisant la charge du réseau et du serveur. Conçu comme un système de fichiers en couches, CacheFS permet de cacher un système sur un autre. Dans un environnement NFS, CacheFS augmente le taux client-par-serveur, réduit la charge du serveur et du réseau et améliore les performances des liaisons client lentes, telles que le protocole PPP (Point-to-Point Protocol).

Vous créez un cache sur le client de sorte que l'accès aux systèmes de fichiers définis pour être montés dans le cache s'effectue localement et non par le réseau. Lorsqu'un utilisateur demande pour la première fois accès à ces fichiers, ils sont placés dans le cache. Le cache reste vide tant qu'un utilisateur ne demande pas l'accès à un (ou plusieurs) fichier(s).

Les premières requêtes d'accès peuvent sembler lentes, mais les accès suivants au(x) même(s) fichier(s) sont plus rapides.

Remarques :

1. Vous ne pouvez pas cacher les systèmes de fichier / (racine) et /**usr**.
2. Vous ne pouvez monter que des systèmes de fichiers partagés. (Reportez-vous à la commande **exportfs**.)
3. Cacher un système de fichiers disque JFS local (Journaled File System) n'apporte aucun gain de performances.
4. Les tâches du tableau suivant sont réservées aux utilisateurs détenant les droits racine ou système.

Tâches CacheFS		
Raccourci Web-based System Manager, (application wsm network) OU	**wsm network**	
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Définir un cache	**cachefs_admin_create**	**cfsadmin –c** *MountDirectoryName*[1]
Spécification des fichiers à monter	**cachefs_mount**	**mount –F cachefs –o backfstype=***FileSysType***,cachedir=***CacheDirectory*[,*options*] *BackFileSystem MountDirectoryName*[2] ou edit /**etc**/**filesystems**
Modification du cache	**cachefs_admin_change**	supprime le cache, puis le recrée avec les options adéquates de la commande **mount**
Affichage des informations du cache	**cachefs_admin_change**	**cfsadmin –l** *MountDirectoryName*
Suppression d'un cache	**cachefs_admin_remove**	1. Démontage du système de fichiers **umount** *MountDirectoryName* 2. Détermination de l'ID du cache : **cfsadmin –l** *MountDirectoryName* 3. Suppression du système de fichiers **cfsadmin –d** *CacheID CacheDirectory*
Vérification de l'intégrité du système de fichiers	**cachefs_admin_check**	**fsck_cachefs***CacheDirectory*[3]

Remarques :

1. Une fois le cache créé, n'exécutez aucune opération à l'intérieur du répertoire cache lui-même (**cachedir**). Vous provoqueriez un conflit à l'intérieur du logiciel CacheFS.

2. Si vous utilisez la commande **mount** pour spécifier les fichiers à monter, vous devez relancer la commande chaque fois que le système est réamorcé.
3. Associez l'option **–m** ou **–o** à la commande **fsck_cachefs** pour vérifier les systèmes de fichiers sans effectuer aucune réparation.

Mappage de fichiers sous NFS

Le mappage de fichiers NFS donne aux programmes d'un client accès à un fichier comme s'il se trouvait en mémoire. Via la sous-routine **shmat**, les utilisateurs peuvent mapper des zones d'un fichier dans leur espace d'adressage : lorsqu'un programme lit ou écrit dans cet espace mémoire, le fichier est copié en mémoire à partir du serveur ou mis à jour sur le serveur.

Le mappage de fichiers sous NFS est limité :

- Le partage des informations entre clients est mal assuré.
- Les modifications apportées à un fichier sur un client via un fichier mappé ne sont pas visibles sur un autre client.
- Verrouiller et déverrouiller des régions d'un fichier est inefficace quant à la coordination des données entre clients.

Si un fichier NFS doit servir au partage de programmes de différents clients, il convient de verrouiller les enregistrements et d'exécuter les sous-routines standard **read** et **write.**

Plusieurs programmes sur un client peuvent partager des données via un fichier mappé. Un verrouillage astucieux d'enregistrement peut coordonner les mises à jour sur le fichier sur le client, sous réserve que l'intégralité du fichier soit verrouillé. Plusieurs clients ne peuvent partager des données via des fichiers mappés que s'il s'agit de données immuables (base de données statique, par exemple).

Types de montage

Il existe trois types de montage NFS : prédéfini, explicite et automatique.

Les montages *prédéfinis* sont spécifiés dans le fichier /**etc**/**filesystems**. Chaque strophe de ce fichier définit les caractéristiques d'un montage : elle comprend des données telles que le nom de l'hôte, le chemin d'accès à distance, le chemin d'accès local, etc. Adoptez des montages prédéfinis si l'exploitation d'un client requiert toujours le même type de montage.

Les montages *explicites* sont l'apanage de l'utilisateur racine. Généralement limités à de courtes périodes, ils permettent de répondre à un besoin occasionnel, non planifié. Ils permettent également d'effectuer un montage pour une tâche spéciale, lequel est généralement inaccessible au client NFS. Ces montages sont généralement entièrement qualifiés sur la ligne de commande via l'instruction **mount** assortie de toutes les informations requises. Les montages explicites ne requièrent pas la mise à jour du fichier /**etc**/**filesystems**. Les systèmes de fichiers explicitement montés le restent tant qu'ils ne sont pas explicitement démontés via la commande **umount** ou que le système n'est pas réinitialisé.

Les montages *automatiques* sont contrôlés par le démon **automount** ; l'extension de noyau **AutoFS** surveille alors l'activité des répertoires spécifiés. Si un programme ou un utilisateur tente d'accéder à un répertoire non monté, le démon **AutoFS** intercepte la demande, monte le système de fichiers, puis répond à la demande.

Processus de montage NFS

Pour accéder aux fichiers du serveur, les clients commencent par monter les répertoires exportés du serveur, sans effectuer une copie de ces répertoires. Le processus de montage utilise en revanche une série d'appels de procédure à distance pour donner à un client accès aux répertoires du serveur de façon transparente. Le processus de montage est le suivant :

1. Lorsque le serveur démarre, le script /**etc**/**rc.nfs** exécute la commande **exportfs,** laquelle lit le fichier /**etc**/**exports** du serveur et informe le noyau des répertoires à exporter et des restrictions d'accès qu'ils requièrent.
2. Le démon **rpc.mountd** et plusieurs démons **nfsd** (8, par défaut) sont ensuite lancés par le script /**etc**/**rc.nfs.**
3. Lorsque le client démarre, le script /**etc**/**rc.nfs** lance plusieurs démons **biod** (8, par défaut), qui acheminent les demandes de montage client vers le serveur concerné.
4. Le script /**etc**/**rc.nfs** exécute ensuite la commande **mount**, qui lit les systèmes de fichiers répertoriés dans le fichier /**etc**/**filesystems.**
5. **mount** repère le(s) serveur(s) exportant les informations demandées par le client et établit la communication avec ce(s) serveur(s). Ce processus est appelé *liaison.*
6. La commande **mount** demande ensuite qu'un ou plusieurs serveurs autorisent le client à accéder aux répertoires inscrits dans le fichier /**etc**/**filesystems.**
7. Le démon **rpc.mountd** du serveur reçoit les demandes de montage client, et les accorde ou les refuse. Si le répertoire demandé est accessible, **rpc.mountd** envoie au noyau du client un identificateur appelé *descripteur de fichier.*
8. Le noyau client attache ce descripteur au point de montage (répertoire) en enregistrant des informations dans un *enregistrement de montage.*

Une fois le système de fichiers monté, le client peut travailler sur les fichiers. Lorsque le client exécute une opération sur un fichier, le démon **biod** envoie le descripteur du fichier au serveur, où le fichier est lu par l'un des démons **nfsd** pour traiter la demande. Si le client est autorisé à exécuter l'opération demandée, le démon **nfsd** renvoie ensuite les informations requises au démon **biod** du client.

Fichier /etc/exports

Le fichier /**etc**/**exports** recense tous les répertoires exportés par un serveur à ses clients. Chaque ligne spécifie un seul répertoire. Le serveur exporte automatiquement les répertoires de la liste à chaque lancement du serveur NFS. Ces répertoires exportés peuvent ensuite être montés par les clients. La syntaxe d'une ligne du fichier /**etc**/**exports** est la suivante :

```
directory     -options[,option]
```

`directory` est le chemin d'accès complet au répertoire. Options désigne soit un indicateur simple, tel que `ro`, soit une liste de noms hôte. Reportez-vous à la documentation du fichier /**etc**/**exports** et de la commande **exportfs** pour la liste complète des options et leur description. Le script /**etc**/**rc.nfs** ne lance pas les démons **nfsd** ou le démon **rpc.mountd** si le fichier /**etc**/**exports** n'existe pas.

Exemple d'entrées d'un fichier /**etc**/**exports** :

```
/usr/games    -ro,access=ballet:jazz:tap

/home         -root=ballet,access=ballet

/var/tmp

/usr/lib      -access=clients
```

La première entrée indique que le répertoire `/usr/games` peut être monté par les systèmes `ballet`, `jazz` et `tap`. Ces systèmes sont habilités à lire des données et à exécuter des programmes du répertoire, mais ne peuvent y écrire.

La deuxième entrée spécifie que le répertoire `/home` directory peut être monté par le système `ballet` et que l'accès racine y est autorisé.

La troisième entrée spécifie que n'importe quel client peut monter le répertoire `/var/tmp`. (Notez l'absence de liste d'accès.)

La quatrième entrée spécifie une liste d'accès désignée par le groupe réseau `clients` : En d'autres termes, ces machines désignées comme appartenant au groupe réseau `clients` peuvent monter le répertoire `/usr/lib` à partir de ce serveur. (Un *groupe réseau* est groupe à l'échelle du réseau, ayant accès à certains ressources du réseau à des fins de sécurité ou d'organisation. Les Netgroups sont contrôlés à l'aide du NIS ou du NIS+. Pour plus d'informations, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

Fichier /etc/xtab

Le format du fichier **/etc/xtab** est identique à celui du fichier **/etc/exports.** Ce fichier donne la liste des répertoires exportés. A chaque exécution de la commande **exportfs,** le fichier **/etc/xtab** est modifié : vous pouvez ainsi exporter temporairement un répertoire sans avoir à modifier le fichier **/etc/exports**. Si vous annulez l'exportation du répertoire, il est retiré du fichier **/etc/xtab.**

Remarque : Le fichier **/etc/xtab,** dont la mise à jour est automatique, ne doit pas être édité.

Implémentation de NFS

NFS peut être implémenté sur nombre de types de machines, de systèmes d'exploitation et d'architectures réseau. Cette autonomie lui est conférée par le protocole RPC (*Remote Procedure Call*).

Protocole RPC (Remote Procedure Call)

RPC est une bibliothèque de procédures. Ces procédures permettent à un processus (client) de commander à un autre (processus serveur) l'exécution d'appels de procédures, comme s'il les exécutait dans son propre espace d'adressage. Les processus client et serveur étant distincts, ils n'ont pas besoin de résider sur le même système (bien qu'ils le puissent).

NFS est implémenté comme un ensemble d'appels RPC, le serveur prenant en charge certains types d'appels client. Le client lance ces appels sur la base des opérations sur systèmes de fichiers effectuées par le processus client. En ce sens, NFS est une application RPC.

Les processus serveur et client pouvant résider sur des systèmes d'architectures complètement différentes, RPC doit prendre en compte le fait que les données ne sont peut-être pas représentées de la même manière des deux côtés. D'où son adoption du protocole de représentation XDR (eXternal Data Representation).

Protocole XDR (eXternal Data Representation)

XDR est une spécification assurant une représentation standard de différents types de données. Un programme utilisant cette norme ne risque pas de mal interpréter des données, même provenant d'un système doté d'une architecture totalement différente.

Dans la pratique, la plupart des programmes n'utilisent pas XDR en interne : ils adoptent plutôt la représentation propre à l'architecture du système concerné. Lorsque le programme doit communiquer avec un autre, il convertit ses données au format XDR avant de les envoyer. De même, lorsqu'il reçoit des données, il les convertit du format XDR dans sa propre représentation de données.

Démon portmap

Chaque application RPC est associée avec un numéro de programme et un numéro de version. Ces numéros servent à communiquer avec une application serveur sur un système. Le client, effectuant une demande à partir d'un serveur, doit connaître le numéro du port sur lequel le serveur reçoit les demandes. Ce numéro de port est associé au protocole UDP (User Datagram Protocol) ou TCP (Transmission Control Protocol) utilisé par le service. Le client connaît le numéro du programme, le numéro de version et le nom du système (ou celui de l'hôte sur lequel réside le service). Le client doit pouvoir faire correspondre la paire numéro de programme/numéro de version au numéro de port de l'application serveur. Cette opération est effectuée à l'aide du démon **portmap**.

Le démon **portmap** est exécuté sur le même système que l'application NFS. Lorsque le serveur la lance, il l'enregistre avec **portmap.** Par le biais de cet enregistrement, il fournit son numéro de programme, son numéro de version et son numéro de port UDP ou TCP. Le démon **portmap** maintient une table des applications serveur. Lorsque le client émet une demande vis-à-vis du serveur, il contacte d'abord le démon **portmap** (sur un port identifié) pour connaître le port utilisé par le serveur. Le démon **portmap** répond au client en lui indiquant le port en question. Le client est alors à même d'émettre ses demandes directement à l'application serveur.

Contrôle de NFS

Les démons NFS, NIS et NIS+ sont surveillés par le contrôleur SRC (System Resource Controller). Cela signifie que vous devez utiliser les commandes telles que **startsrc**, **stopsrc** et **lssrc** pour lancer, arrêter et vérifier l'état des démons NFS, NIS et NIS+.

Certains démons NFS ne sont pas contrôlés par SRC, à savoir : **rpc.rexd**, **rpc.rusersd**, **rpc.rwalld** et **rpc.rsprayd**. Ils sont lancés et arrêtés par le démon **inetd**.

Le tableau suivant répertorie les démons et sous-systèmes contrôlés par SRC.

Démons et sous-systèmes associés		
Chemin d'accès au fichier	*Sous-système*	*Groupe*
/usr/sbin/nfsd	**nfsd**	nfs
/usr/sbin/biod	**biod**	nfs
/usr/sbin/rpc.lockd	**rpc.lockd**	nfs
/usr/sbin/rpc.statd	**rpc.statd**	nfs
/usr/sbin/rpc.mountd	**rpc.mountd**	nfs
/usr/lib/netsvc/yp/ypserv	**ypserv**	yp
/usr/lib/netsvc/yp/ypbind	**ypbind**	yp
/usr/lib/netsvc/rpc.yppasswdd	**yppasswdd**	yp
/usr/lib/netsvc/rpc.ypupdated	**ypupdated**	yp
/usr/sbin/keyserv	**keyserv**	keyserv
/usr/sbin/portmap	**portmap**	portmap

Les démons NIS+ sont traités dans le *AIX 4.3 NIS/NIS+ Guide*. Chacun de ces démons peut être défini dans les commandes SRC à l'aide de leur nom de sous–système ou de leur nom de groupe approprié.

Pour en savoir plus, reportez-vous à "Contrôleur SRC" dans *AIX 4.3 System Management Guide: Operating System and Devices*.

Modification du nombre de démons biod et nfsd

Pour modifier le nombre de démons **biod** ou **nfsd** actifs, lancez la commande **chnfs**. Ainsi, pour limiter à 10 le nombre de démons **nfsd,** et à 4 le nombre de démons **biod,** entrez :

```
chnfs -n 10 -b 4
```

Cette commande arrête temporairement les démons actifs, modifie le code de la base de données SRC et relance les démons.

Remarque : Dans l'implémentation NFS AIX, le nombre de démons **biod** n'est contrôlable que par point de montage via l'option **biod –o**. La spécification qui utilise **chnfs** n'est maintenue que pour des raisons de compatibilité et n'a pas d'effet sur le nombre réel de routine exécutant les E/S.

Modification des arguments des démons contrôlés par SRC

Nombre de démons NFS, NIS et NIS+ peuvent être assortis d'arguments, sur la ligne de commande, spécifiés une fois le démon activé. Ces démons n'étant pas eux-mêmes activés directement via la ligne de commande, vous devez mettre à jour la base de données SRC pour que les démons puissent être correctement activés. Pour ce faire, lancez la commande **chssys**. La commande **chssys** a le format :

```
chssys -s Daemon -a 'NewParameter'
```

Par exemple :

```
chssys -s nfsd -a '10'
```

modifie le sous-système **nfsd** de sorte que, à l'activation du démon, la ligne de commande soit semblable à `nfsd 10`. La modification induite par la commande **chssys** ne prend effet qu'une fois le sous-système arrêté puis relancé.

Lancement des démons NFS au démarrage du système

Par défaut, les démons NFS ne sont pas activés au cours de l'installation. Celle-ci achevée, tous les fichiers sont placés sur le système, mais les étapes d'activation de NFS ne sont pas effectuées. Vous pouvez lancer les démons NFS au démarrage du système via :

- Le raccourci Web-based System Manager, **wsm network**
- Le raccourci SMIT, **smit mknfs**
- La commande **mknfs**.

Quelle que soit la méthode choisie, une entrée est intégrée au fichier **inittab** de façon que le script **/etc/rc.nfs** soit exécuté à chaque redémarrage du système. A son tour, ce script lance tous les démons requis par un système donné.

Lancement des démons NFS

La taille maximale des fichiers situés sur un serveur NFS est définie par l'environnement du processus au démarrage de **nfsd.** Pour modifier cette valeur, éditez le fichier /**etc**/**rc.nfs** et insérez-y une commande **ulimit,** indiquant la nouvelle limite, avant la commande **startsrc** relative à **nfsd**.

Les démons NFS peuvent être lancés individuellement ou tous à la fois. Pour les lancer individuellement :

```
startsrc -s Daemon
```

Daemon étant l'un des démons contrôlés par SRC. Ainsi, pour lancer les démons **nfsd** :

```
startsrc -s nfsd
```

Pour les lancer tous simultanément :

```
startsrc -g nfs
```

Remarque : Si le fichier /**etc**/**exports** n'existe pas, les démons **nfsd** et **rpc.mountd** ne sont pas lancés. Vous pouvez créer un fichier /**etc**/**exports** vide via la commande **touch** /**etc**/**exports** : les démons **nfsd** et **rpc.mountd** seront lancés, mais aucun système de fichiers ne sera exporté.

Arrêt des démons NFS

Les démons NFS peuvent être arrêtés individuellement ou tous à la fois. Pour les arrêter individuellement :

```
stopsrc -s Daemon
```

Daemon étant l'un des démons contrôlés par SRC. Ainsi, pour arrêter **rpc.lockd** :

```
stopsrc -s rpc.lockd
```

Pour les arrêter tous simultanément :

```
stopsrc -g nfs
```

Etat des démons NFS

Vous pouvez afficher l'état de démons NFS spécifiques ou de tous les démons à la fois. Pour afficher l'état d'un démon, entrez :

```
lssrc -s Daemon
```

Daemon étant l'un des démons contrôlés par SRC. Ainsi, pour obtenir l'état de **rpc.lockd** :

```
lssrc -s rpc.lockd
```

Pour afficher simultanément l'état des tous les démons :

```
lssrc -a
```

Installation et configuration de NFS

Pour en savoir plus sur l'installation de NFS (Network File System), reportez-vous à *AIX Installation Guide*.

Etapes de configuration de NFS

Une fois le logiciel NFS installé sur vos systèmes, il faut le configurer.

1. Déterminez les systèmes du réseau qui seront serveurs, et ceux qui seront clients (un système peut être à la fois serveur et client).
2. Pour chaque système, suivez les instructions indiquées à "Lancement des démons NFS au démarrage du système", page 10-9.
3. Pour chaque serveur NFS, suivez les instructions indiquées à "Configuration d'un serveur NFS", page 10-11.
4. Pour chaque client NFS, suivez les instructions indiquées à "Configuration d'un client NFS", page 10-11.
5. Si vous souhaitez donner aux PC du réseau accès aux serveurs NFS (outre leur capacité à monter des systèmes de fichiers), configurez PC-NFS comme indiqué à "PC-NFS", page 10-20.

Configuration d'un serveur NFS

Procédez comme suit :

1. Lancez NFS comme indiqué à "Lancement des démons NFS", page 10-10.
2. Créez le fichier **/etc/exports.**

Configuration d'un client NFS

1. Vérifiez que NFS est le système de fichiers distant par défaut. (Sinon, il vous faudra assortir la commande **mount** de l'indicateur **–v nfs**.) A l'aide d'un éditeur de votre choix, ouvrez le fichier **/etc/vfs** et recherchez les entrées suivantes :

   ```
   #%defaultvfs jfs nfs
   #nfs 2 /sbin/helpers/nfsmnthelp none remote
   ```

   Si des signes dièse (#) apparaissent en tête de ligne, effacez-les.
2. Lancez NFS comme indiqué à "Lancement des démons NFS", page 10-10.
3. Définissez le point de montage local via la commande **mkdir**. La réussite d'un montage NFS suppose la présence d'un répertoire servant de point de montage. Ce répertoire doit être vide. La création de ce point de montage ne diffère en rien de celle de n'importe quel répertoire, et aucun attribut particulier ne doit être spécifié.

Remarque : Les points de montage doivent exister préalablement à tout montage, à une exception près : si vous utilisez le démon **automount,** il n'est parfois pas nécessaire de créer de points de montage. Reportez-vous à la documentation **automount**.

4. Etablissez les montages prédéfinis comme indiqué à "Etablissement de montages NFS prédéfinis", page 10-16.

Exportation d'un système de fichiers NFS

Vous pouvez exporter un système de fichiers NFS via l'application Web-based System Manager wsm network, ou utiliser l'une des procédures suivantes.

- Via SMIT :
  a. Vérifiez que NFS est actif en lançant la commande `lssrc -g nfs` **..** La sortie doit indiquer que les démons **nfsd** et **rpc.mountd** sont actifs. Dans la négative, lancez NFS comme indiqué à "Lancement des démons NFS", page 10-10.
  b. Utilisez

  ```
  smit mknfsexp
  ```

  c. Renseignez les zones Chemin d'accès du répertoire à exporter, Mode d'accès au répertoire exporté et Export répert maintenant, init-syst. ou les deux.
  d. Modifiez les autres caractéristiques ou acceptez les valeurs par défaut.
  e. Vos changements terminés, SMIT met à jour le fichier /**etc**/**exports**. Si le fichier /**etc**/**exports** n'existe pas, il est créé.
  f. Répétez les étapes 3 à 5 pour chaque répertoire à exporter.
- Pour exporter un système de fichiers NFS via un éditeur :
  a. Ouvrez le fichier /**etc**/**exports** sous votre éditeur favori.
  b. Créez une entrée pour chaque répertoire à exporter, en indiquant le chemin d'accès complet du répertoire. Répertoriez tous les répertoires à exporter en commençant à la marge gauche. Ne spécifiez pas de répertoire qui en contient un autre déjà exporté. Pour en savoir plus sur la syntaxe des entrées dans le fichier /**etc**/**exports**, reportez-vous à la documentation du fichier /**etc**/**exports**.
  c. Sauvegardez et fermez le fichier /**etc**/**exports**.
  d. Si NFS est actif, entrez :

  ```
  /usr/sbin/exportfs -a
  ```

  L'indicateur **–a** indique à la commande **exportfs** d'envoyer au noyau toutes les informations du fichier /**etc**/**exports.** Si NFS n'est pas actif, lancez-le comme indiqué à "Lancement des démons NFS", page 10-10.
- Pour exporter temporairement un système de fichiers NFS (c'est-à-dire sans modifier le fichier /**etc**/**exports**), entrez :

  ```
  exportfs -i /dirname
  ```

  dirname étant le nom du système de fichiers à exporter. La commande **exportfs –i** spécifie de ne pas rechercher le répertoire dans le fichier /**etc**/**exports**, et que toutes les options sont directement issues de la ligne de commande.

Annulation de l'exportation d'un système de fichiers NFS

Vous pouvez annuler l'exportation d'un système de fichiers NFS via l'application Web-based System Manager wsm network, ou utiliser l'une des procédures suivantes.

- Via SMIT :
  a. Entrez :

  ```
  smit rmnfsexp
  ```

  b. Entrez le chemin d'accès dans la zone *Chemin d'accès* répert exporté devant être retiré.

  Le répertoire est supprimé du fichier /**etc**/**exports** et son exportation, annulée.
- Pour annuler l'exportation d'un fichier via un éditeur :
  a. Ouvrez le fichier /**etc**/**exports** sous votre éditeur favori.

b. Repérez l'entrée correspondant au répertoire concerné et effacez la ligne.

c. Sauvegardez et fermez le fichier /**etc**/**exports**.

d. Si NFS est actif, entrez :

```
exportfs -u dirname
```

dirname étant le chemin d'accès complet au répertoire que vous venez de supprimer du fichier /**etc**/**exports.**

Modification d'un système de fichiers exporté

Vous pouvez modifier un système de fichiers NFS via l'application wsm network Web-based System Manager, ou utiliser l'une des procédures suivantes.

- Via SMIT :

  a. Annulez l'exportation du système de fichiers :

  ```
  exportfs -u /dirname
  ```

  dirname étant le nom du système de fichiers à modifier.

  b. Entrez :

  ```
  smit chnfsexp
  ```

  c. Entrez le chemin d'accès approprié dans la zone Chemin d'accès répert exporté.

  d. Effectuez les modifications souhaitées.

  e. Quittez SMIT.

  f. Réexportez le système de fichiers :

  ```
  exportfs /dirname
  ```

  dirname étant le nom du système de fichiers que vous venez de modifier.

- Pour modifier un système de fichiers via un éditeur :

  a. Annulez l'exportation du système de fichiers :

  ```
  exportfs -u /dirname
  ```

  dirname étant le nom du système de fichiers à modifier.

  b. Ouvrez le fichier /**etc**/**exports** sous votre éditeur favori.

  c. Effectuez les modifications souhaitées.

  d. Sauvegardez et fermez le fichier /**etc**/**exports**.

  e. Réexportez le système de fichiers :

  ```
  exportfs /dirname
  ```

  dirname étant le nom du système de fichiers que vous venez de modifier.

Activation de l'accès racine à un système de fichiers exporté

Lorsque vous exportez un système de fichiers, vous pouvez accorder à l'utilisateur racine les droits d'accès racine à ce système, sur une machine donnée. Par défaut, ces droits ne sont pas accordés. Lorsqu'une personne, connectée en tant qu'utilisateur racine sur un hôte, demande l'accès à un fichier NFS, son ID utilisateur est comparé (par NFS) à l'ID de l'utilisateur `nobody` (`nobody` étant l'un des noms d'utilisateur inscrits dans le fichier /**etc**/**password**). Les droits de l'utilisateur `nobody` sont les mêmes que les droits publics (*autres*) affectés à un fichier donné. Par exemple, si *autres* n'a que le droit d'exécution sur un fichier, `nobody` ne peut qu'exécuter ce fichier.

Pour activer les droits racine sur un système de fichiers exporté, suivez les instructions indiquées à "Modification d'un système de fichiers exporté", page 10-13. Si vous passez par SMIT ou par Web-based System Manager, indiquez dans la zone Hôtes ayant un accès root

le nom de l'*hôte* sur lequel vous souhaitez accorder les droits racine. Si vous faites appel à un éditeur, ajoutez le qualificateur `-root=hostname` à l'entrée correspondant au système de fichiers. Par exemple :

```
/usr/tps -root=hermes
```

spécifie que l'utilisateur racine sur l'hôte `hermes` détient des droits d'accès racine au répertoire `/usr/tps`.

Montage explicite d'un système de fichiers NFS

Pour monter explicitement un répertoire NFS, utilisez le raccourci Web-based System Manager **wsm network** ou la procédure suivante.

1. Vérifiez que le serveur NFS a exporté le répertoire :

   ```
   showmount -e ServerName
   ```

   `ServerName` étant le nom du serveur NFS. Cette commande affiche le nom des répertoires exportés du serveur NFS. Si le répertoire à monter ne s'y trouve pas, exportez-le.

2. Définissez le point de montage local via la commande **mkdir**. La réussite d'un montage NFS suppose la présence d'un répertoire servant de point de montage. Ce répertoire doit être vide. La création de ce point de montage ne diffère en rien de celle de n'importe quel répertoire, et aucun attribut particulier ne doit être spécifié.

3. Entrez :

   ```
   mount ServerName:/remote/directory /local/directory
   ```

   `ServerName` étant le nom du serveur NFS, `/remote/directory`, le répertoire du serveur NFS que vous souhaitez monter et `/local/directory` le point de montage sur le client NFS.

4. Sur la machine cliente, entrez :

   ```
   smit mknfsmnt
   ```

5. Modifiez les champs suivants en fonction de la configuration de votre réseau. Vous n'aurez peut-être pas à renseigner tous les champs de cet écran.

   Remarque : Si vous utilisez l'interface ASCII de SMIT, appuyez sur la touche de tabulation pour modifier la valeur d'un champ, mais *n'appuyez pas* sur Entrée avant l'étape 7.

   - Chemin d'accès point de montage.
   - Chemin d'accès répertoire éloigné.
   - Hôte sur lequel réside le répertoire éloigné.
   - MONTAGE immédiat, ajout /etc/filesystems ou les 2 ?
   - L'entrée /etc/filesystems entraîne le montage du répertoire lors de l'init-système.
   - Mode d'accès à ce système de fichiers NFS.

6. Conservez les valeurs par défaut ou modifiez-les en fonction de votre configuration NFS.

7. Une fois modifiés les champs requis, SMIT monte le système de fichiers NFS.

8. Lorsque le champ `Commande :` affiche OK, quittez SMIT.

Le système de fichiers NFS est prêt.

Montage automatique d'un système de fichiers à l'aide de AutoFS

AutoFS fait appel à la commande **automount** pour communiquer les informations de configuration pour le montage automatique à l'extension de noyau AutoFS et lance le démon **automountd**. L'extension est alors en mesure de monter automatiquement et de manière transparente le système de fichiers dès qu'un fichier ou un répertoire de ce système de fichiers est ouvert. L'extension informe le démon **autmountd** des requêtes de montage et de démontage, et c'est le **autmountd** qui exécute véritablement le service demandé.

La liaison nom-emplacement étant dynamique dans le démon **automount**, les mises à jour d'une mappe NIS utilisée par le démon **automount** sont transparentes pour l'utilisateur. De ce fait, il est inutile de prémonter les systèmes de fichiers partagés pour les applications dotées de références aux fichiers et aux répertoires codées matériellement. Il est également inutile de maintenir des enregistrements indiquant quels hôtes doivent être montés pour quelles applications.

AutoFS permet de monter les systèmes de fichiers à la demande. Ainsi, ceux montés avec NFS n'ont pas besoin de l'être en permanence.

Pour monter automatiquement un répertoire NFS :

1. Vérifiez que le serveur NFS a exporté le répertoire :

   `showmount –e` *`ServerName`*

   `ServerName` étant le nom du serveur NFS. Cette commande affiche le nom des répertoires exportés du serveur NFS.

2. Création d'un fichier de mappe **AutoFS**. **AutoFS** monte et démonte les répertoires indiqués dans ce fichier de mappe. Supposons, par exemple, que vous souhaitiez utiliser **AutoFS** pour monter les répertoires `/usr/local/dir1` et `/usr/local/dir2`, comme demandé par le serveur `serve1`, sur les répertoires `/usr/remote/dir1` et `/usr/remote/dir2` respectivement. Le nom du fichier mappe est ici `/tmp/mount.map`.

   ```
   dir1            –rw             serve1:/usr/local/dir1
   dir2            –rw             serve1:/usr/local/dir2
   ```

3. Vérifiez que l'extension de noyau **AutoFS** est chargée et que le démon **automountd** est en cours d'exécution. Vous disposez pour ce faire de deux méthodes :

   a. Utiliser **SRC**: Lancez **lssrc –s automountd**. Si le sous–système **automountd** ne fonctionne pas, lancez **startsrc –s automountd**.

   b. Utiliser al commande **automount** : Lancez /**usr**/**bin**/**automount –v**.

   Définissez le fichier de mappe à l'aide de l'interface de ligne de commande, en tapant :

   ```
   /usr/sbin.automount  /usr/remote  /tmp/mount.map
   ```

   `/usr/remote` étant le point de montage **AutoFS** sur le client. Dès lors, si un utilisateur exécute la commande **cd** /**usr**/**remote**/**dir1**, l'extension de noyau **AutoFS** va intercepter l'accès à ce répertoire et lancer un appel de procédure distante vers le démon **automountd**, qui montera le répertoire`/usr/remote/dir1` et permettra l'exécution de la commande **cd**.

   ```
   /usr/sbin/automount /usr/remote /tmp/mount.map
   ```

   `/usr/remote` étant le point de montage sur le client NFS. Si un utilisateur lance alors la commande **cd /usr/remote/dir1,** le démon monte le répertoire `/usr/remote/dir1`, permettant l'aboutissement de la commande **cd**.

4. Pour arrêter le démon **automount**, exécutez la commande **stopsrc -s automountd**.

   Si, pour une raison quelconque, le démon **automountd** a été lancé sans passer par **SRC** :

   kill *automountd_PID*

   automountd_PID étant l'ID de processus du démon **automountd**. (Entrez **ps –e** pour afficher l'ID de processus du démon **automountd**.) La commande **kill** envoie un signal SIGTERM au démon **automountd**.

Etablissement de montages NFS prédéfinis

Vous pouvez définir des montages NFS prédéfinis via l'application Web-based System Manager wsm network, ou utiliser l'une des procédures suivantes.

Attention : Spécifiez les options **bg** (background) et **intr** (interruptible) dans le fichier **/etc/filesystems** lorsque vous établissez un montage prédéfini à effectuer lors du démarrage du système. Les montages non interruptibles exécutés à l'avant-plan peuvent déconnecter le client pour peu que le réseau ou le serveur soit hors fonction au démarrage du système client. Si un client ne peut accéder au réseau ou à un serveur, l'utilisateur doit relancer la machine en mode maintenance et modifier en conséquence les demandes de montage.

- Pour établir des montages NFS prédéfinis via SMIT :

  a. Entrez :

  ```
  smit mknfsmnt
  ```

  b. Renseignez les champs de cet écran pour chaque montage que vous souhaitez prédéfinir. Vous devez renseigner les champs obligatoires (signalés par un astérisque (*) dans la marge gauche). Pour les autres champs, spécifiez des valeurs ou conservez les valeurs par défaut. Une entrée correspondante est créée dans le fichier **/etc/filesystems**, puis le montage est tenté.

- Pour établir des montages NFS prédéfinis en éditant le fichier **/etc/filesystems** :

  a. Ouvrez le fichier **/etc/filesystems** sous votre éditeur favori.

  b. Insérez-y une entrée pour chaque système de fichiers distant que vous souhaitez monter au démarrage du système. Par exemple :

  ```
  /home/jdoe:
  dev = /home/jdoe
  mount = false
  vfs = nfs
  nodename = mach2
  options = ro,soft
  type = nfs_mount
  ```

  Cette strophe commande au système de monter le répertoire distant `/home/jdoe` sur le point de montage local de même nom. Le système de fichiers est monté en mode lecture seule (`ro`). Etant également monté comme `soft`, une erreur est émise si le serveur ne répond pas. Si vous spécifiez `nfs_mount` pour le paramètre `type`, le système tente de monter le fichier `/home/jdoe` (avec les autres systèmes de fichiers spécifiés dans le groupe `type = nfs_mount`) au moment de l'émission de la commande **mount -t nfs_mount**.

  L'exemple ci-après commande au système de monter `/usr/games` au démarrage. Si le montage échoue, le système tente l'opération en arrière-plan.

```
/usr/games:
dev = /usr/games
mount = true
vfs = nfs
nodename = gameserver
options = ro,soft,bg
type = nfs_mount
```

Voici les paramètres requis dans les strophes relatives aux montages NFS :

`dev=`*`filesystem_name`*	Chemin d'accès au système de fichiers distant à monter.
`mount=[`*`true`*`|`*`false`*`]`	Si *`true`*, spécifie que le système de fichiers NFS sera monté à l'amorçage du système. Si *`false`*, spécifie que le système de fichiers NFS ne sera pas monté à l'amorçage du système.
`nodename=`*`hostname`*	Hôte sur lequel réside le système de fichiers distant.
`vfs=nfs`	Le système de fichiers virtuel en cours de montage est de type NFS.

Voici les paramètres facultatifs dans les strophes relatives aux montages NFS :

`type=`*`type_name`*	Le système de fichiers en cours de montage appartient au groupe *`type_name`* mount. Ce paramètre est associé à la commande **mount –t**, qui monte simultanément des groupes de systèmes de fichiers.
`options=`*`options`*	Une ou plusieurs des *`options`* suivantes :
`biods=`*`N`*	Nombre de démons **biod** à démarrer. La valeur par défaut est 6. *`N`* est un entier.
`bg`	Indique de relancer le montage en arrière-plan si la première tentative échoue.
`fg`	Indique de relancer le montage à l'avant-plan si la première tentative échoue.
`noacl`	Désactive, pour le seul montage en cours, la prise en charge des listes ACL, assurée par le système de fichiers journalisé de NFS.

Utilisé entre deux systèmes, NFS prend en charge les listes de contrôle des accès (ACL). Si l'option `noacl` est spécifiée au montage d'un système de fichiers, NFS ne se sert pas des ACL. Spécifier `noacl` a le même effet que lorsqu'un client NFS d'un système tente un montage à partir d'un serveur NFS qui ne prend pas les ACL en charge.

Pour en savoir plus, reportez-vous à "Listes de contrôle d'accès (ACL) sous NFS", page 10-3.

`retry=`*`n`*	Nombre de tentatives de montage.
`rsize=`*`n`*	Définit à *`n`* octets la taille du tampon de lecture.
`wsize=`*`n`*	Définit à *`n`* octets la taille du tampon d'écriture.
`timeo=`*`n`*	Délai (*`n`* dixièmes de seconde) au bout duquel NFS abandonne. Cette variable permet d'éviter les situations où la charge du serveur affecte considérablement les temps de réponse.
`retrans=`*`n`*	Définit à *`n`* le nombre de retransmissions NFS.
`port=`*`n`*	Définit à *`n`* le numéro du port serveur.
`soft`	Renvoie une erreur si le serveur ne répond pas.
`hard`	Relance la requête jusqu'à ce que le serveur réponde.

Si vous spécifiez un montage `hard`, il se peut que le processus se bloque pendant l'attente d'une réponse. Pour pouvoir interrompre le processus et le terminer à partir du clavier, spécifiez `intr` dans les paramètres de montage.

`intr`	Permet les interruptions à partir du clavier.
`ro`	Définit la variable lecture seule.
`rw`	Définit la variable lecture/écriture. Associée à la variable `hard`, elle évite des erreurs de conflit avec des applications si un montage `soft` est tenté en lecture/écriture. Pour en savoir plus, reportez-vous à "Identification des incidents NFS", page 10-36.
`secure`	Indique d'utiliser un protocole plus sûr pour les transactions NFS.
`actimeo=`*`n`*	Augmente de *`n`* secondes le délai avant nettoyage du cache, pour les fichiers et les répertoires standard.

Remarque : Le cache "attribut" maintient les attributs de fichier sur le client. Ces attributs sont dotés d'un délai, au bout duquel ils sont effacés. Si un fichier est modifié avant expiration, le délai est augmenté du temps écoulé depuis la dernière modification (les fichiers récemment modifiés sont supposés pouvoir l'être à nouveau rapidement). Un minimum et un maximum sont définis pour l'extension de ce délai (pour les fichiers et les répertoires standard).

`acregmin=`*`n`*	Maintient les attributs en mémoire cache au moins *`n`* secondes après la modification du fichier.
`acregmax=`*`n`*	Maintient les attributs en mémoire cache au plus *`n`* secondes après la modification du fichier.
`acdirmin=`*`n`*	Maintient les attributs en mémoire cache au moins *`n`* secondes après la mise à jour du répertoire.
`acdirmax=`*`n`*	Maintient les attributs en mémoire cache au plus *`n`* secondes après la mise à jour du répertoire.

Remarque : Si vous ne spécifiez pas les options suivantes, le noyau leur affecte une valeur par défaut :

```
biods=6
fg
retry=10000
rsize=8192
wsize=8192
timeo=7
retrans=3
port=NFS_PORT
hard
secure=off
acregmin=3
acregmax=60
acdirmin=30
acdirmax=60
```

c. Supprimez les entrées correspondant aux répertoires que vous ne souhaitez pas monter au démarrage du système.

d. Sauvegardez et fermez le fichier.

e. Lancez la commande **mount –a** pour monter tous les répertoires du fichier **/etc/filesystems.**

Démontage d’un système de fichiers monté explicitement ou automatiquement

Entrez :

```
umount /directory/to/unmount
```

Suppression de montages NFS prédéfinis

Vous pouvez supprimer un montage NFS prédéfini via l’application Web-based System Manager wsm network, ou utiliser l’une des procédures suivantes.

- Via SMIT :
  a. Entrez :

  ```
  smit rmnfsmnt
  ```

- Pour supprimer un montage NFS prédéfini en éditant le fichier /**etc/filesystems** :
  a. Entrez la commande : `umount /directory/to/unmount`.
  b. Ouvrez le fichier /**etc/filesystems** sous votre éditeur favori.
  c. Repérez l’entrée correspond au répertoire démonté et effacez-la.
  d. Sauvegardez et fermez le fichier.

PC–NFS

PC–NFS est un programme destiné aux ordinateurs personnels, qui leur permet de monter des systèmes de fichiers exportés par un serveur NFS (Network File System). L'ordinateur personnel a également la possibilité de demander à ce serveur NFS des adresses réseau et des noms d'hôte. Par ailleurs, si le serveur NFS exécute le démon **rpc.pcnfsd**, l'ordinateur personnel peut bénéficier des services d'authentification et d'impression différée.

Vous pouvez configurer le démon **rpc.pcnfsd** sur les matériels suivants :

- systèmes exécutant des services d'authentification d'utilisateur ;
- systèmes offrant des fonctions d'impression en différé ;
- tous les serveurs NIS maître et esclaves.

Remarque : Comme la configuration des réseaux NIS prévoit généralement que PC–NFS puisse sélectionner n'importe quel serveur NIS comme serveur par défaut, il est important que tous les serveurs soient dotés du programme **rpc.pcnfsd**. Si l'exécution de ce programme sur tous les serveurs NIS n'est pas envisageable, ou si vous souhaitez confiner les requêtes vers un serveur spécifique, ajoutez une commande **net pcnfsd** dans le fichier **autoexec.bat** de chaque ordinateur personnel, afin de l'obliger à faire appel à un serveur NIS spécifique. Pour plus d'informations, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

Service d'authentification PC–NFS

Par défaut, PC–NFS se présente aux serveurs NFS comme étant l'utilisateur `nobody`. Avec les privilèges `nobody`, tous les fichiers des utilisateurs de l'ordinateur personnel sont détenus par `nobody`, et il est impossible de faire la distinction entre les différents utilisateurs. Les fonctions d'authentification du démon **rpc.pcnfsd** permettent de surveiller les ressources système et la sécurité, en autorisant la reconnaissance des différents utilisateurs et l'affectation de différents privilèges.

Lorsque le démon **rpc.pcnfsd** est en cours d'exécution, un utilisateur PC–NFS peut lancer la commande **net name** à partir d'un ordinateur personnel pour ouvrir une session PC–NFS de la même manière qu'un utilisateur se connecte sur AIX. Le nom de l'utilisateur et le mot de passe sont vérifiés par le démon **rpc.pcnfsd**. Cette procédure d'authentification ne rend pas le serveur plus sûr mais elle autorise un meilleur contrôle des accès aux fichiers disponibles via NFS.

Service d'impression en différé PC–NFS

Le service d'impression en différé du démon **rpc.pcnfsd** permet aux ordinateurs personnels exécutant PC–NFS d'imprimer sur des imprimantes qui ne leur sont pas directement raccordées. Plus précisément, PC–NFS redirige les fichiers destinés aux imprimantes de l'ordinateur personnel vers un fichier placé sur un serveur NFS. Ces fichier est placa dans un répertoire de spoulage sur le serveur NFS. Le démon **rpc.pcnfsd** appelle alors la fonction d'impression du serveur. (Le répertoire de spoulage doit se trouver dans un système de fichiers exporté afin que les clients PC–NFS puissent le monter.) Lorsque PC–NFS demande au démon **rpc.pcnfsd** d'imprimer le fichier, il fournit les informations suivantes :

- Nom du fichier à imprimer
- ID d'ouverture de session de l'utilisateur sur le client
- Nom de l'imprimante à utiliser

Configuration du démon rpc.pcnfsd

Pour configurer le démon **rpc.pcnfsd** :

1. Installez le programme PC–NFS sur votre ordinateur personnel.
2. Sélectionnez un emplacement pour le répertoire de spoulage sur le serveur NFS. Le répertoire de spoulage par défaut est **/var/tmp**. Ce répertoire doit disposer d'au moins 100 Ko de mémoire disponible.
3. Exportez le répertoire de spoulage. Ne définissez pas de restrictions d'accès sur le répertoire exporté afin de ne pas engendrer de problèmes d'accès à partir du réseau. Pour plus d'informations sur la procédure, reportez–vous à "Exportation d'un système de fichiers NFS", page 10-12.
4. Lancez le démon **rpc.pcnfsd** en suivant les instructions de "Lancement du démon rpc.pcnfsd", page 10-21.
5. Vérifiez que le démon **rpc.pcnfsd** est accessible en suivant les instructions de "Vérification de la disponibilité du démon rpc.pcnfsd", page 10-22.

Remarque : Les demandes de redirection d'impression laissent parfois dans les répertoires de spoulage PC–NFS des listings de fichiers de longueur nulle ; éliminez donc régulièrement ces entrées du répertoire de spoulage.

Lancement du démon rpc.pcnfsd

Pour lancer le démon **rpc.pcnfsd** à partir du répertoire de spoulage par défaut :

1. A l'aide de votre éditeur de texte favori, annulez la mise en commentaire de l'entrée suivante dans le fichier **/etc/inetd.conf** :

   ```
   pcnfsd sunrpc_udp udp wait root /usr/sbin/rpc.pcnfsd pcnfsd 150001 1
   ```

2. Sauvegardez le fichier et quittez l'éditeur de texte.

Pour lancer le démon **rpc.pcnfsd** à partir d'un répertoire autre que le répertoire par défaut :

1. A l'aide de votre éditeur de texte favori, ajoutez l'entrée suivante dans le fichier **/etc/rc.nfs** :

   ```
   if [ –f /usr/sbin/rpc.pcnfsd ] ; puis
   /usr/sbin/rpc.pcnfsd –s spooldir ; echo ' rpc.pcnfsd\c'
   fi
   spooldir correspond au chemin d'accès complet du répertoire de
   spoulage.
   ```

2. Sauvegardez le fichier et quittez l'éditeur de texte.
3. A l'aide de votre éditeur de texte favori, mettez en commentaire l'entrée suivante dans le fichier **/etc/inetd.conf** :

   ```
   pcnfsd sunrpc_udp udp wait root /usr/sbin/rpc.pcnfsd pcnfsd 150001 1
   ```

   en insérant un signe dièse (#) au début de la ligne. Ceci évite que le démon **inetd** ne démarre le démon **rpc.pcnfsd** à partir du répertoire de spoulage par défaut.
4. Lancez le programme d'impression en différé du démon **rpc.pcnfsd** en entrant la commande suivante sur la ligne de commande :

   ```
   /usr/sbin/rpc.pcnfsd –s spooldir
   ```

   spooldir correspond au chemin d'accès complet du répertoire de spoulage.

Pour plus d'informations sur la mise à jour de la base de données de configuration **inetd**, reportez–vous à "Configuration du démon inetd", page 3-101.

Remarque : le répertoire par défaut utilisé par le démon **rpc.pcnfsd** ne peut être modifié à partir du fichier **inetd.conf**.

Vérification de la disponibilité du démon rpc.pcnfsd

Pour vérifier que le démon **rpc.pcnfsd** est accessible, entrez :

```
rpcinfo –u host 150001
```

host correspond au nom de l'hôte du système sur lequel vous configurez **rpc.pcnfsd**, et 15001 est le numéro de programme RPC du démon **rpc.pcnfsd**. Après avoir entré la commande, vous devez recevoir un message signalant que le programme est prêt et en attente.

WebNFS

AIX fournit des fonctions de serveur NFS pour WebNFS. Défini par Sun Microsystems, WebNFS est un simple prolongement du protocole NFS permettant de faciliter l'accès aux serveurs et clients par l'intermédiaire de pare–feu Internet.

Un navigateur Web WebNFS peut utiliser les adresses URL universelles NFS pour accéder directement aux données à partir du serveur. Voici un exemple d'URL NFS :

```
nfs://www.VotreSociété.com/
```

WebNFS fonctionne en conjonction avec les protocoles Web existants afin de mettre les données à la disposition des clients.

WebNFS bénéficie également de l'évolutivité des serveurs NFS.

Gestionnaire NLM (Network Lock Manager)

Le gestionnaire NLM (network lock manager) est un utilitaire qui, associé à NFS, fournit un fichier de consultation et un verrouillage des enregistrements sur le réseau à la manière de System V. Les démons du gestionnaire NLM (**rpc.lockd**) et du contrôleur d'état du réseau (**rpc.statd**) sont des démons de service réseau. Le démon **rpc.statd** est un processus de niveau utilisateur alors que le démon **rpc.lockd** est implémenté comme un ensemble de routines de noyau (semblable au serveur NFS). Les deux démons sont indispensables pour assurer la capacité du noyau à fournir les services réseau fondamentaux.

Remarque : Les verrous obligatoires ou forcés ne sont pas admis sur NFS.

Architecture du gestionnaire NLM

Le gestionnaire NLM comporte des fonctions serveur et des fonctions client. Les fonctions client traitent les demandes émises par les applications et envoient les demandes au gestionnaire NLM sur le serveur. Les fonctions serveur sont chargées d'accepter les requêtes de verrouillage émises par les clients et de générer les appels de verrouillage correspondants sur le serveur. Le serveur répond ensuite à la requête de verrouillage du client.

Contrairement à NFS, qui est "sans état", le gestionnaire NLM est doté d'un état implicite. Autrement dit, il doit mémoriser certaines informations sur le client, à savoir si le client est actuellement verrouillé. Le contrôleur d'état du réseau, **rpc.statd**, implémente un protocole simple qui permet au gestionnaire de verrous de contrôler l'état des autres machines du réseau. Grâce à la précision des informations d'état, le gestionnaire NLM parvient à maintenir un état cohérent dans l'environnement "sans état" de NFS.

Verrouillage des fichiers du réseau

Lorsqu'une application souhaite obtenir un verrou sur un fichier local, elle en adresse la demande au noyau via la sous-routine **lockf**, **fcntl** ou **flock**. Le noyau traite alors la demande. Toutefois, si une application sur un client NFS demande un verrou sur un fichier distant, Le client NFS génère un RPC (Remote Procedure Call) à destination du serveur pour qu'il prenne la requête en charge.

Lorsque le client reçoit la requête de verrou distant pour la première fois, il l'enregistre dans le serveur via le démon **rpc.statd** du client. Il est de même pour le contrôleur de verrouillage du réseau sur le serveur. Il enregistre la première requête d'un client sur le client avec le contrôleur d'état du réseau.

Processus de reprise

Chaque démon **rpc.statd** d'une machine notifie de ses activités les démons **rpc.statd** des autres machines. Lorsque le démon **rpc.statd** d'une machine apprend qu'une machine est en panne ou qu'elle a repris ses activités, il en avertit son démon **rpc.lockd.**

Si un serveur tombe en panne, les clients avec des fichiers verrouillés doivent pouvoir recouvrer leurs verrous. Si un client tombe en panne, son serveur doit conserver ses verrous jusqu'à reprise du client. En outre, pour préserver la transparence globale de NFS, le recouvrement doit s'effectuer sans intervention des applications elles-mêmes.

La procédure de reprise est simple. Si une anomalie est relevée sur un client, le serveur libère les verrous du client en question, en présumant que l'application client les redemandera au besoin. Si une anomalie est relevée sur un serveur, le gestionnaire des verrous client retransmet toutes les demandes de verrous précédemment accordées par le serveur. Ces informations retransmises sont exploitées par le serveur pour reconstituer son état de verrouillage pendant une période dite de grâce. (La période de grâce, de 45 secondes par défaut, est le délai pendant lequel un serveur autorise les clients à réclamer leurs verrous.)

Le démon **rpc.statd** se sert des noms hôte conservés dans /**etc**/**sm** et dans /**etc**/**sm.bak** pour garder trace des hôtes à informer lorsque la machine doit recouvrer ses opérations.

Lancement du gestionnaire NLM

Par défaut, le script /**etc**/**rc.nfs** lance les démons **rpc.lockd** et **rpc.statd** avec les autres démons NFS. Si NFS est déjà actif, vérifiez si **rpc.lockd** et **rpc.statd** sont actifs, comme indiqué à ”État des démons NFS”, page 10-10. Ces deux démons doivent être à l'état *actif*. Si les démons **rpc.lockd** et **rpc.statd** ne sont pas actifs, procédez comme suit :

1. A l'aide de votre éditeur favori, ouvrez le fichier /**etc**/**rc.nfs.**
2. Repérez les lignes suivantes :

```
if [ -x /usr/sbin/rpc.statd ]; then
       startsrc -s rpc.statd
fi
if [ -x /usr/sbin/rpc.lockd ]; then
       startsrc -s rpc.lockd
fi
```

3. Si certaines lignes commencent par le signe dièse (#), effacez-le, puis sauvegardez le fichier et quittez l'éditeur. Lancez ensuite successivement les démons **rpc.statd** et **rpc.lockd**, comme indiqué à ”Lancement des démons NFS”, page 10-10.

   Remarque : L'ordre de lancement est important : commencez toujours par **statd.**

4. Si NFS est actif et que les entrées du fichier /**etc**/**rc.nfs** sont correctes, arrêtez puis relancez **rpc.statd** et **rpc.lockd**, comme indiqué à ”Arrêt des démons NFS”, page 10-10 et à ”Lancement des démons NFS”, page 10-10.

   Remarque : L'ordre de lancement est important : commencez toujours par **statd.**

Si les démons **rpc.statd** et **rpc.lockd** ne sont toujours pas actifs, reportez-vous à ”Dépannage du gestionnaire NLM”.

Dépannage du gestionnaire NLM

Si vous recevez sur un client un message du style :

```
clnttcp_create: RPC: Remote System error - Connection refused
rpc.statd:cannot talk to statd at {server}
```

c'est que la machine suppose qu'il y a une autre machine qui doit être informée qu'elle doit prendre des mesures de recouvrement. Lorsqu'une machine est réamorcée, ou que **rpc.lockd** et **rpc.statd** sont arrêtés puis relancés, les noms de machine sont déplacés de /**etc**/**sm** vers /**etc**/**sm.bak** et **rpc.statd** tente d'informer chaque machine correspondant à chaque entrée de /**etc**/**sm.bak** que des procédures de reprise s'imposent.

Si **rpc.statd** parvient à atteindre la machine, son entrée dans /**etc**/**sm.bak** est supprimée. Si **rpc.statd** ne parvient pas à atteindre la machine, il poursuit sa tentative à intervalles réguliers. Chaque fois que la machine échoue à répondre, le message ci-dessus est généré à l'issue du délai de dépassement. Dans l'intérêt de l'intégrité du verrouillage, le démon poursuit ses tentatives, mais ceci peut avoir l'effet inverse sur les performances du verrouillage. La gestion est différente, selon que la machine cible ne répond simplement pas ou se trouve de façon semi-permanente hors état productif. Pour éliminer le message :

1. Vérifiez que les démons **statd** et **lockd** sur le serveur sont lancés, comme indiqué à ”État des démons NFS”, page 10-10. (Ces deux démons doivent être à l'état *actif*.)
2. Dans la négative, lancez **rpc.statd** et **rpc.lockd** sur le serveur, comme indiqué à ”Lancement des démons NFS”, page 10-10.

   Remarque : L'ordre de lancement est important : commencez toujours par **statd.**

   Une fois tous les démons relancés, n'oubliez pas le délai de grâce : pendant ce délai, les démons **lockd** autorisent les autres clients à réclamer les verrous conservés

précédemment par le serveur. L'obtention d'un nouveau verrou n'est donc pas instantanée.

Pour éliminer le message, vous pouvez également procéder comme suit :

1. Arrêtez **rpc.statd** et **rpc.lockd** sur le client, comme indiqué à "Arrêt des démons NFS", page 10-10.
2. Sur le client, supprimez l'entrée de la machine cible de **/etc/sm.bak**. Entrez :

   ```
   rm /etc/sm.bak/TargetMachineName
   ```

   Ceci action empêche la machine cible d'être informée qu'elle doit peut-être participer au recouvrement du verrouillage : ne l'effectuez que si vous êtes sûr que les applications actives sur cette machine ne participent pas au verrouillage réseau avec la machine affectée.
3. Lancez **rpc.statd** et **rpc.lockd** sur le client, comme indiqué à "Lancement des démons NFS", page 10-10.

Si vous ne parvenez pas à obtenir un verrou d'un client :

1. Lancez la commande **ping** pour vérifier si client et serveur peuvent s'atteindre et se reconnaître. Si les deux machines fonctionnent et que le réseau est intact, vérifiez, dans le fichier **/etc/hosts**, le nom d'hôte de chaque machine. Pour que les machines puissent se reconnaître, ces noms doivent être exactement les mêmes pour le serveur et pour le client. Si un serveur de noms est utilisé pour la conversion des noms d'hôte, vérifiez que les informations hôte sont identiques à celles du fichier **/etc/hosts.**
2. Vérifiez que les démons **rpc.lockd** et **rpc.statd** sur le serveur sont lancés, comme indiqué à "État des démons NFS", page 10-10. Ces deux démons doivent être à l'état *actif*.
3. Dans la négative, lancez les démons **rpc.statd** et **rpc.lockd**, comme indiqué à "Lancement des démons NFS", page 10-10.
4. S'ils sont actifs, vous devrez peut-être les réinitialiser sur les clients et les serveurs. Pour ce faire, arrêtez les applications qui demandent un verrou.
5. Ensuite, arrêtez **rpc.statd** et **rpc.lockd** sur le client et sur le serveur, comme indiqué à "Arrêt des démons NFS", page 10-10.
6. Relancez ensuite **rpc.statd** et **rpc.lockd**, d'abord sur le serveur, puis sur le client, comme indiqué à "Lancement des démons NFS", page 10-10.

   Remarque : L'ordre de lancement est important : commencez toujours par **statd.**

Si le problème de verrou persiste, exécutez le démon **lockd** en mode débogage :

1. Arrêtez **rpc.statd** et **rpc.lockd** sur le client et sur le serveur, comme indiqué à "Arrêt des démons NFS", page 10-10.
2. Lancez le démon **rpc.statd** sur le client et sur le serveur, comme indiqué à "Lancement des démons NFS", page 10-10.
3. Lancez **rpc.lockd** sur le client et sur le serveur :

   ```
   /usr/sbin/rpc.lockd -d1
   ```

   Appelé avec l'indicateur **–d1**, le démon **lockd** génère des messages de diagnostic vers la sortie standard. Les premiers messages concernent le délai de grâce : attendez qu'ils s'effacent. Exécutez ensuite l'application problématique et vérifiez qu'une demande de verrou est bien transmise du client au serveur et du serveur au client.

NFS sécurisé

Outre le système d'authentification standard d'UNIX, le service NIS (Network Information Service), NIS+ et NFS (Network File System) offrent un moyen d'authentifier utilisateurs et machines d'un réseau sur une base message par message. Ce système d'authentification complémentaire utilise le chiffrement DES (Data Encryption Standard) et le chiffrement par clé publique.

Cette section traite des points suivants :

Confidentialité

Tout au long de l'histoire, des hommes ont cherché le moyen de communiquer des messages dont le contenu ne soit intelligible que par l'expéditeur et le destinataire : c'est ainsi que le *chiffrement* a fait son apparition. Il s'agit de convertir un texte *en clair* en un texte *chiffré* et réciproquement. *Le chiffrement* est le processus de conversion d'un texte en clair en texte chiffré, et le *déchiffrement*, le processus inverse.

Un des premiers codes de chiffrement, le *code César*, est attribué à Jules César. Dans ce code, une lettre est substituée à une autre. Ainsi, 'A' devient 'C', 'B' devient 'D', ..., 'Y' devient 'A' et 'Z' devient 'B'. Par exemple, la phrase **ATTACK AT DAWN** devient **CVVCEM CV FCYP**.

Si les Carthaginois avaient réussi à *décrypter* le code, les *cryptographes* romains auraient dû en inventer un autre. Cette recherche étant coûteuse, les Romains ont imaginé de définir une *clé,* permettant d'exploiter un peu plus efficacement le chiffrement. Par exemple, au lieu d'une substitution lettre par lettre, ils ont spécifié une clé, *K*, K indiquant le nombre de positions de décalage d'une lettre. Ainsi, si K = 2, 'A' devient 'C'. Si K = 4, 'A' devient 'E', etc. Avec ce schéma, si les Carthaginois décryptent le code, il suffit aux Romains de changer de clé - en sachant, bien entendu, que les Carthaginois risquent de découvrir l'algorithme et qu'il leur suffira alors de tester le déchiffrement avec toutes les valeurs de K (1 à 26). Si les Carthaginois avaient disposé d'un ordinateur, cette tâche aurait été réduite à un petit exercice de programmation.

Chiffrement DES (Data Encryption Standard)

Les algorithmes de chiffrement modernes sont conçus en sachant que les ordinateurs sont de puissants outils, offrant à un intrus d'importants moyens de décodage. En 1977, le gouvernement américain a adopté un standard de chiffrement, le chiffrement DES (Data Encryption Standard). Ce chiffrement est largement utilisé dans l'industrie. Il s'agit d'un algorithme fort complexe, qui convertit des blocs de 64 bits de texte en clair en blocs de 64 bits de texte codé par le biais d'une clé de 56 bits. Compte tenu de la complexité de l'algorithme et de la taille de la clé, cet algorithme est pratiquement inviolable : en supposant qu'un intrus dispose d'un ordinateur capable d'analyser l'algorithme à la vitesse d'une clé par microseconde, il lui faudra deux mille ans pour tester toutes les clés.

Chiffrement par clé publique

Le point faible de tout algorithme de chiffrement est sa clé. Si l'expéditeur et le destinataire doivent communiquer en sécurité via un code de chiffrement, l'un comme l'autre doivent connaître la clé. Ils doivent se mettre d'accord sur la clé via une liaison distincte, sécurisée elle aussi bien entendu, ou directement (en personne).

Pour résoudre ce problème, deux chercheurs (Diffie et Hellman) ont développé une technique grâce à laquelle émetteur et destinataire peuvent se communiquer leur clé, sans compromettre la sécurité de leurs échanges. Cette technique suppose trois règles :

- Déchiffrement (Chiffrement (texte en clair, E), D) = texte en clair

  E étant la clé de chiffrement (publique) et D, la clé de déchiffrement (connue du seul destinataire).

  Cette règle signifie que les fonctions de chiffrement/déchiffrement sont inverses l'une de l'autre : si vous appliquez au texte codé généré par Chiffrement (texte en clair, E) la fonction Déchiffrement avec la clé D, vous obtenez le texte en clair d'origine.

- Un intrus ne peut déduire Déchiffrement() de Chiffrement().
- Chiffrement() est inviolable.

Voici la procédure d'envoi d'un message secret.

1. L'expéditeur demande la clé de chiffrement publique.
2. Il convertit son texte en appliquant la formule :

   ```
   texte_codé = Chiffrement( texte_clair, E )
   ```

3. Il envoie le texte codé au destinataire.
4. Le destinataire reçoit le texte et le convertit selon la formule :

   ```
   texte_clair = Déchiffrement( texte_codé, D )
   ```

Même s'il intercepte le message, un intrus ne peut le décoder puisqu'il ne possède pas la clé de déchiffrement. (L'expéditeur lui-même ne la connaît pas.)

Authentification

Une des principales applications de la confidentialité est l'*authentification*. Le plus souvent l'authentification fait appel aux mots de passe (l'authentification standard UNIX, notamment) : un utilisateur souhaitant se connecter doit fournir un mot de passe, connu uniquement du système et de l'utilisateur. Si le mot de passe est correct, le système suppose que l'utilisateur est bien celui qu'il déclare être. Cette méthode requiert de stocker les mots de passe dans un fichier système, ce qui, même si ce fichier est codé, présente quelques risques. Elle suppose aussi que deux entités ait connaissance du mot de passe.

Le chiffrement par clé publique offre une alternative à l'authentification par mot de passe. Soit un expéditeur souhaitant envoyant un message, et un destinataire, qui a besoin d'être sûr de l'identité de l'expéditeur. Le processus est le suivant :

1. L'expéditeur chiffre un message de "demande pour émettre" (RTS), par la clé de chiffrement publique et envoie la demande.
2. Le destinataire reçoit le message de "demande pour émettre" et le déchiffre à l'aide de sa clé privée.
3. Le destinataire chiffre un message "jeton" à l'aide de la clé publique de l'expéditeur et envoie le jeton.
4. L'expéditeur reçoit le jeton, et le déchiffre à l'aide de sa clé privée. Il commencera ensuite tous les messages qu'il envoie par ce jeton, certifiant ainsi son identité. Un intrus qui tenterait d'envoyer des messages au nom de l'expéditeur les verrait rejetés par le destinataire, qui constaterait l'absence de jeton.

Notez que, contrairement à l'authentification par mot de passe, le destinataire peut authentifier l'expéditeur sans connaître sa clé privée. Pour en savoir plus sur les systèmes d'authentification, reportez-vous à "Understanding RPC Authentication" dans le manuel *AIX Communications Programming Concepts*.

Confidentialité dans NFS

NFS, NIS et NIS+ font usage de l'algorithme DES à deux fins. NIS l'utilise pour chiffrer les zones privées des mappes NIS (mappe **publickey**, par exemple). NFS l'utilise pour chiffrer l'horodate dans les messages RPC transitant entre les clients et les serveurs NFS. Cette horodate chiffrée authentifie les machines, comme le "jeton" authentifie l'expéditeur, comme indiqué à "Authentification", page 10-28.

NFS pouvant authentifier n'importe quel message RPC échangé entre clients et serveurs NFS, un niveau de sécurité supplémentaire (optionnel) peut être associé à chaque système de fichiers. Par défaut, les systèmes de fichiers sont exportés avec l'authentification UNIX standard. Pour bénéficier de l'option de sécurité renforcée, spécifiez **secure** lorsque vous exportez un système de fichiers.

Chiffrement par clé publique pour NFS sécurisé

Les clés publique et privée sont toutes deux stockées et indexées par leur nom réseau dans la mappe NIS **publickey.byname.** La clé privée est chiffrée via DES avec le mot de passe de connexion de l'utilisateur. La commande **keylogin** utilise la clé privée chiffrée, la déchiffre avec le mot de passe de connexion et la transmet à un serveur sécurisé de clés locales, pour un usage ultérieur dans les transactions RPC. Les utilisateurs ne connaissent ni leur clé publique, ni leur clé privée, car la commande **yppasswd**, outre le fait de modifier le mot de passe de connexion, génère les clés (publique et privée) automatiquement.

Le démon **keyserv** est un service RPC, actif sur chaque machine NIS et NIS+. Pour plus d'informations sur l'utilisation de NIS+ utilisez **keyserv**, reportez–vous au *AIX 4.3 NIS/NIS+ Guide* **keyserv** qui exécute les trois sous-routines publiques suivantes :

- **key_setsecret**
- **key_encryptsession**
- **key_decryptsession**

La sous-routine **key_setsecret** indique au serveur de clés de stocker la clé privée de l'utilisateur (SK_A) pour un usage ultérieur. Elle est normalement appelée par la commande **keylogin**. Le programme client appelle la sous-routine **key_encryptsession** pour générer la clé de conversation chiffrée, qui est passée à la première transaction RPC vers un serveur. Le serveur de clés recherche la clé publique du serveur et la combine à la clé privée du client (définie par une sous-routine **key_setsecret** précédente) pour générer la clé commune. Le serveur demande au serveur de clés de déchiffrer la clé de conversation en appelant la sous-routine **key_decryptsession.**

Ces appels de sous-routine supposent un appelant, qui doit lui aussi être authentifié. Pour ce faire, le serveur de clés ne peut pas utiliser l'authentification DES, qui provoquerait un blocage total. Il résout le problème en stockant les clés privées par leur ID utilisateur (UID) et en ne répondant qu'aux demandes des processus racine locaux. Le processus client exécute ensuite une sous-routine **setuid**, appartenant à l'utilisateur racine, qui effectue la demande "de la part" du client, indiquant au serveur de clés l'UID réel du client.

Règles d'authentification

L'authentification sur NFS sécurisé est basée sur la capacité d'un expéditeur à chiffrer l'heure courante, que le destinataire peut déchiffrer et comparer avec sa propre horloge. Ce processus suppose que les deux protagonistes :

- soient d'accord sur l'heure,
- utilisent la même clé de chiffrement DES.

Accord sur l'heure

Si le réseau est synchronisé, le démon **timed** assure la synchronisation des horloges client et serveur. Sinon, le client détermine l'heure sur la base de l'horloge du serveur : il détermine l'heure serveur avant d'ouvrir la session RPC, calcule le décalage entre son horloge et celle du serveur, et règle son horloge en conséquence. Si, au cours d'une session RPC, les horloges viennent à être désynchronisées au point que le serveur commence à rejeter les demandes client, il appartient au client de réitérer le réglage.

Accord sur la clé DES

Client et serveur déterminent la clé de chiffrement DES à l'aide du chiffrement par clé publique. Pour tout couple client A et serveur B, il existe un clé que seuls A et B peuvent déduire. Cette clé est appelée *clé commune*. Le client déduit la clé commune à l'aide de la formule :

$$K_{AB} = PK_B^{SK_A}$$

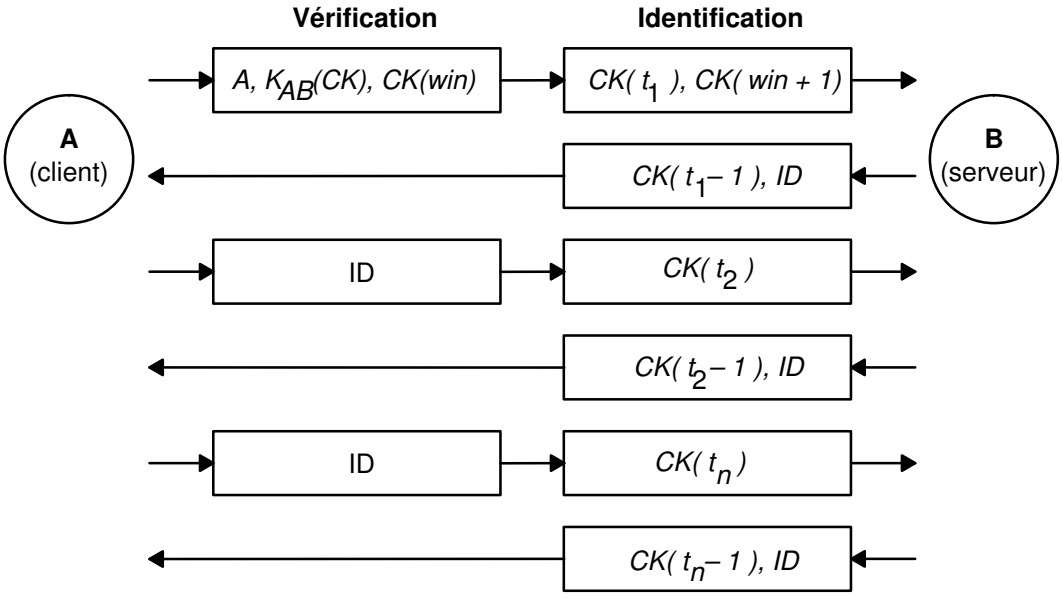
K étant la *clé commune*, *PK* la *clé publique* et *SK* la *clé privée*, chaque clé correspondant à un nombre sur 128 bits. Le serveur déduit la clé commune à l'aide de la formule :

$$K_{AB} = PK_A^{SK_B}$$

Le calcul de cette clé commune, dans lequel intervient la clé privée de chacun, ne peut être effectué que par le client et le serveur concernés. Cette clé ayant 128 bits et DES utilisant une clé de 56 bits, le client et le serveur extraient 56 bits de la clé commune pour constituer la clé DES.

La figure illustre la connexion entre le client A et le serveur B.

Lorsqu'un client souhaite "parler " à un serveur, il génère de façon aléatoire une clé, utilisée pour chiffrer les horodates. Cette clé est appelée *clé de conversation* (*CK*). Le client chiffre cette clé via la clé commune DES (voir "Authentication Requirements", page 10-29) et l'envoie au serveur dans la première transaction RPC. Le schéma Processus d'authentification illustre ce processus.



Processus d'authentification

La figure illustre la connexion entre le client A et le serveur B. Le terme *K*(*CK*) signifie que *CK* est chiffrée par la clé DES commune *K*. Dans la première demande, l'identification RPC du client contient son nom (*A*), la clé de conversation (*CK*) et la variable *win* (window) chiffrée via *CK* (dont la valeur par défaut est de 30 minutes). Le vérificateur client dans la première demande contient l'horodate chiffrée et un vérificateur chiffré de la fenêtre

spécifiée, *win* + 1. Grâce à ce vérificateur, il est encore plus difficile de deviner la bonne identification - la sécurité en est accrue d'autant.

Après authentification du client, le serveur enregistre dans une table les éléments suivants :

- le nom du client, *A*
- le clé de conversation, *CK*
- la fenêtre (window),
- l'horodate.

Le serveur n'accepte que les horodates postérieures à la dernière reçue, aussi les transactions répétées sont-elles rejetées. Le serveur renvoie au client dans le vérificateur un ID index dans la table d'authentification, ainsi que l'horodate du client moins un, chiffrée via *CK*. Le client sait alors que seul le serveur peut avoir envoyé ce vérificateur, car il est le seul à connaître l'horodate envoyée par le client. Soustraire un de l'horodate garantit que l'horodate n'est plus valide et ne peut plus être réutilisée comme vérificateur de client. Après la première transaction RPC, le client envoie juste son ID et une horodate chiffrée au serveur, lequel lui renvoie l'horodate diminuée de 1, chiffrée via *CK*.

Nom des entités réseau pour l'authentification DES

L'authentification DES se base sur les noms "net". Les paragraphes suivants traitent du mode de traitement de l'authentification DES par le NIS. Pour plus d'informations sur le mode d'authentification DES par le NIS+, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

Un *net name* est une chaîne de caractères imprimables destinés à l'identification. Les clés secrètes et publiques sont stockées sur la base d'un "per–net–name" plutôt que d'un "per–user–name". La mappe **netid.byname** NIS place le nom "net" au sein d'un UID local et d'une liste d'accès de groupe.

Les noms d'utilisateur sont uniques dans un domaine. Les noms réseau sont formés par concaténation des ID système et utilisateur avec les noms de domaine NIS et Internet. Pour nommer les domaines, optez pour la convention qui consiste à ajouter le nom Internet du domaine (com, edu, gov, mil) à son nom local.

Les noms réseau sont attribués aux machines et aux utilisateurs. Les noms de machine sont formés à peu près comme ceux des utilisateurs. Par exemple, un machine nommée `hal` dans le domaine `eng.ibm.com` possède le nom réseau `unix.hal@eng.ibm.com` . Une authentification correcte des machines est essentielle, surtout lorsqu'il s'agit de machines sans disque qui nécessitent un accès total à leur répertoire personnel dans le réseau.

Pour authentifier les utilisateurs d'un domaine distant, vous devez insérer les entrées correspondantes dans deux bases de données NIS : une entrée pour leurs clés publiques et privées, l'autre pour le mappage UID local et liste d'accès groupe. Les utilisateurs du domaine distant peuvent alors accéder à tous les services du réseau local (NFS, connexion à distance, etc.).

Fichier /etc/publickey

Le fichier **/etc/publickey** contient les noms et les clés publiques, utilisées par NIS et NIS+ pour créer la mappe **publickey**. La mappe **publickey** assure la sécurité du réseau. Chaque entrée du fichier est constituée du nom d'un utilisateur du réseau (référençant un utilisateur ou un hôte), suivi de la clé publique de l'utilisateur (en hexadécimal), d'un deux-points et de la clé privée chiffrée de l'utilisateur (également en hexadécimal). Par défaut, l'unique utilisateur inscrit dans le fichier **/etc/publickey** est `nobody`.

Ne faites pas appel à un éditeur de texte pour modifier le fichier **/etc/publickey,** car il contient des clés de chiffrement. Si vous devez modifier le fichier **/etc/publickey**, passez plutôt par la commande **chkey** ou **newkey**.

Remarques sur l’amorçage des systèmes à clé publique

Lorsque vous réamorcez une machine après une coupure de courant, toutes les clés privées stockées sont perdues et aucun processus ne peut accéder aux services sécurisés du réseau (tel le montage d’un NFS). Les processus racine peuvent se poursuivre, sous réserve que quelqu’un puisse indiquer le mot de passe qui déchiffre la clé privée de l’utilisateur racine. La solution est de stocker la clé privée de l’utilisateur racine déchiffrée dans un fichier accessible par le serveur de clés.

Tous les appels de sous-routine **setuid** n’aboutissent pas comme prévu. Par exemple, si une sous-routine **setuid** est appelée par l’utilisateur `dave`, qui ne s’est pas reconnecté depuis le réamorçage de la machine, la sous-routine ne peut accéder aux services réseau sécurisés en tant que `dave`. Toutefois, la plupart des appels de sous-routine **setuid** sont propriété de l’utilisateur racine - dont la clé privée est toujours enregistrée au moment de l’amorçage.

Remarques sur les performances

Travailler sous NFS sécurisé n’est pas sans incidence sur les performances du système. Pour commencer, le client et le serveur doivent tous deux calculer la clé commune. Ce calcul demande environ 1 seconde. Autrement dit, il faut environ 2 secondes pour établir la connexion RPC initiale, le client et le serveur ayant tous deux à effectuer cette opération. Une fois cette connexion établie, le serveur conserve le résultat de l’opération en mémoire cache, ce qui évite de recalculer la clé à chaque fois.

D’autre part, chaque transaction RPC requiert 4 opérations de chiffrement DES :

1. Le client chiffre l’horodate de la demande.
2. Le serveur la déchiffre.
3. Le serveur chiffre l’horodate de la réponse.
4. Enfin, le client la déchiffre.

Pesez donc bien le pour (sécurité accrue) et le contre (performances moindres) avant de passer sous NFS sécurisé.

Administration de NFS sécurisé

Voici quelques règles qui vous aideront à vérifier que NFS sécurisé opère correctement :

- Lorsque vous montez un système de fichiers sur un client, en spécifiant l’option **–secure**, le nom du serveur doit correspondre au nom d’hôte du serveur tel qu’il apparaît dans le fichier **/etc/hosts.** Si un serveur de noms sert à la résolution des noms d’hôte, vérifiez que les informations hôte renvoyées par ce serveur correspondent à l’entrée du fichier **/etc/hosts.** Faute de quoi, des erreurs d’authentification risquent de se produire, car les noms réseau des machines sont basés sur les entrées principales du fichier **/etc/hosts,** et que c’est le nom réseau qui sert à l’accès aux clés de la mappe **publickey.**
- Ne panachez pas montages et exportations sécurisés et non sécurisés : l’accès aux fichiers risque d’être mal déterminé. Ainsi, si une machine client monte un système de fichiers sécurisé sans option **secure** ou un système non sécurisé avec option **secure,** les utilisateurs y accéderont en tant que `nobody`, et non en tant qu’eux-mêmes. Cette situation se produit également si un utilisateur inconnu de NIS ou NIS+ tente de créer ou de modifier des fichiers d’un système sécurisé.
- NIS diffusant une nouvelle mappe à chaque émission des commandes **chkey** et **newkey**, ne les lancez que lorsque le réseau est peu chargé.
- Ne supprimez ni le fichier **/etc/keystore** ni le fichier **/etc/.rootkey**. Si vous réinstallez, déplacez ou mettez à jour une machine, sauvegardez les fichiers **/etc/keystore** et **/etc/.rootkey**.

- Dites aux utilisateurs d'employer la commande **yppasswd** de préférence à la commande **passwd** pour changer de mot de passe : mots de passe et clés privées resteront synchronisés.
- La commande **login** ne recherchant pas de clés dans la mappe **publickey** pour le démon **keyserv**, l'utilisateur doit exécuter la commande **keylogin.** Vous pouvez placer la commande **keylogin** dans le fichier **profile** de chaque utilisateur pour qu'elle soit exécutée automatiquement. Notez que la commande **keylogin** demande à l'utilisateur de donner son mot de passe une deuxième fois.
- Lorsque vous générez les clés de l'utilisateur racine au niveau de chaque hôte, via la commande **newkey -h** ou **chkey**, vous devez exécuter la commande **keylogin** pour transmettre les nouvelles clés au démon **keyserv.** Les clés sont stockées dans le fichier **/etc/.rootkey**, lu par le démon **keyserv** chaque fois que celui-ci est lancé.
- Vérifiez régulièrement que les démons **yppasswdd** et **ypupdated** sont actifs sur le serveur NIS maître : ces démons sont requis pour maintenir la mappe **publickey.**
- Vérifiez régulièrement que le démon **keyserv** est actif sur toutes machines sous NFS sécurisé.

Configuration de NFS sécurisé

Pour configurer NFS sécurisé sur les serveurs NIS maître et esclaves, passez par l'application Web-based System Manager wsm network ou procédez comme suit. Pour plus d'informations sur l'utilisation de NFS avec NIS+, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

1. Sur le serveur NIS maître, créez une entrée pour chaque utilisateur dans le fichier NIS **/etc/publickey** via la commande **newkey**. Cette commande propose deux options. Pour un utilisateur standard, entrez :

   ```
   smit newkey
   ```

   OU

   ```
   newkey –u username
   ```

   Pour un utilisateur racine sur une machine hôte, entrez :

   ```
   newkey –h hostname
   ```

   Les utilisateurs peuvent également définir leurs propres clés publiques via la commande **chkey** ou **newkey**.

2. Créez la mappe NIS **publickey,** comme indiqué à *AIX 4.3 NIS/NIS+ Guide* La mappe NIS correspondante **publickey.byname** ne doit résider que sur les serveurs NIS.

3. Annulez la mise en commentaire des strophes suivantes dans le fichier **/etc/rc.nfs** :

   ```
   #if [ –x /usr/sbin/keyserv ]; then
   #  startsrc –s keyserv
   #fi
   #if [ –x /usr/lib/netsvc/yp/rpc.ypupdated –a –d
   /etc/yp/‘domainname‘ ]; then
   #  startsrc –s ypupdated
   #fi
   #DIR=/etc/passwd
   #if [ –x /usr/lib/netsvc/yp/rpc.yppasswdd –a –f $DIR/passwd ];
   then
   #  startsrc –s yppasswdd
   #fi
   ```

4. Lancez les démons **keyserv**, **ypupdated** et **yppasswdd** à l'aide de la commande startsrc.

Pour configurer NFS sécurisé sur des clients NIS, lancez le démon **keyserv** à l'aide de la commande startsrc.

Exportation d'un système de fichiers via NFS sécurisé

Vous pouvez exporter un NFS sécurisé via l'application Web-based System Manager wsm network, ou utiliser l'une des procédures suivantes.

- Via SMIT :
  a. Vérifiez que NFS est actif en lançant la commande **lssrc –g nfs**. La sortie doit indiquer que les démons **nfsd** et **rpc.mountd** sont actifs. Dans la négative, lancez NFS comme indiqué à "Lancement des démons NFS", page 10-10.
  b. Vérifiez que la mappe **publickey** existe et que le démon **keyserv** est actif. Pour en savoir plus, reportez–vous à "Configuration de NFS sécurisé", page 10-33.
  c. Lancez le raccourci **smit mknfsexp.**
  d. Renseignez les zones Chemin d'accès du répertoire à exporter, Mode d'accès au répertoire exporté et Export répertoire maintenant, init-syst. ou les deux. Spécifiez **oui** à la rubrique Utilisation de l'option de montage SECURE.
  e. Modifiez les autres caractéristiques ou acceptez les valeurs par défaut.
  f. Quittez SMIT. Si le fichier /**etc**/**exports** n'existe pas, il est créé.
  g. Répétez les étapes 3 à 6 pour chaque répertoire à exporter.
- Pour exporter un système de fichiers NFS sécurisé via un éditeur :
  a. Ouvrez le fichier /**etc**/**exports** sous votre éditeur favori.
  b. Créez une entrée pour chaque répertoire à exporter, en indiquant le chemin d'accès complet du répertoire. Répertoriez tous les répertoires à exporter en commençant à la marge gauche. Ne spécifiez pas de répertoire qui en contient un autre déjà exporté. Pour en savoir plus sur la syntaxe des entrées dans le fichier /**etc**/**exports**, reportez-vous à la documentation du fichier /**etc**/**exports**.
  c. Sauvegardez et fermez le fichier /**etc**/**exports**.
  d. Si NFS est actif, entrez :

  ```
  /usr/sbin/exportfs –a
  ```

  L'indicateur **–a** indique à la commande **exportfs** d'envoyer au noyau toutes les informations du fichier /**etc**/**exports.** Si NFS n'est pas actif, lancez-le comme indiqué à "Lancement des démons NFS", page 10-10.
- Pour exporter temporairement un système de fichiers NFS (c'est-à-dire sans modifier le fichier /**etc**/**exports**),

  Entrez :

  ```
  exportfs –i –o secure /dirname
  ```

  dirname étant le nom du système de fichiers à exporter. La commande **exportfs –i** spécifie de ne pas rechercher le répertoire dans le fichier /**etc**/**exports**, et que toutes les options sont directement issues de la ligne de commande.

Montage d’un système de fichiers NFS sécurisé

Procédez comme suit :

1. Vérifiez que le serveur NFS a exporté le répertoire. Pour ce faire, lancez la commande :

   `showmount –e` *`ServerName`*

   `ServerName` étant le nom du serveur NFS. Cette commande affiche le nom des répertoires exportés du serveur NFS. Si le répertoire à monter ne s’y trouve pas, exportez-le.

2. Définissez le point de montage local via la commande **mkdir**. La réussite d’un montage NFS suppose la présence d’un répertoire servant de point de montage. Ce répertoire doit être vide. La création de ce point de montage ne diffère en rien de celle de n’importe quel répertoire, et aucun attribut particulier ne doit être spécifié.

3. Vérifiez que la mappe **publickey** existe et que le démon **keyserv** est actif. Pour en savoir plus, reportez–vous à ”Configuration de NFS sécurisé”, page 10-33.

4. Entrez :

   `mount –o secure` *`ServerName`*`:`*`/remote/directory /local/directory`*

   `ServerName` étant le nom du serveur NFS, *`/remote/directory,`* le répertoire du serveur NFS que vous souhaitez monter et *`/local/directory`* le point de montage sur le client NFS.

Remarque : Seul un utilisateur racine peut monter un système de fichiers NFS sécurisé.

Pour en savoir plus, reportez-vous à ”Etablissement de montages NFS prédéfinis”, page 10-16.

Identification des incidents NFS

Les machines utilisant NFS, comme tout service de réseau, ne sont pas à l'abri d'incidents. Pour résoudre ces défaillances, il faut être en mesure de les identifier, d'interpréter les messages d'erreur et de déterminer la méthode de résolution appropriée. Il s'agit dans un premier temps de localiser le dysfonctionnement sur l'un des trois principaux éléments : serveur, client ou réseau.

Remarque : Reportez-vous à "Dépannage du gestionnaire NLM", page 10-25.

Inaccessibilité des fichiers en montage fixe ou logiciel

En cas de défaillance du réseau ou serveur, les programmes ne parviennent plus à accéder aux fichiers distants, mais ce mécanisme diffère selon que le fichier fait l'objet d'un montage fixe ou logiciel.

Dans le cas d'un montage fixe, NFS signale l'échec du serveur par le message :

```
NFS server hostname not responding, still trying
```

Les systèmes de fichiers distants en montage fixe mettent les programmes en attente jusqu'à la réponse du serveur de sorte que le client peut relancer la demande de montage jusqu'à obtenir satisfaction. Pour un montage fixe, associez l'indicateur **–bg** à la commande **mount** pour que le client puisse tenter le montage en arrière-plan si le serveur ne répond pas.

Dans le cas d'un montage logiciel, NFS signale l'échec du serveur par le message :

```
Connection timed out
```

Passé un certain délai, en cas de tentatives infructueuses, les systèmes de fichiers distants en montage logiciel renvoient un message d'erreur. Mais un grand nombre de programmes ne vérifient pas le résultat des opérations sur systèmes de fichiers. Ce message d'erreur ne vous est alors pas communiqué au moment d'accéder aux fichiers en montage logiciel. Il est toutefois affiché à la console.

Liste de contrôle pour l'identification des incidents NFS

En cas d'incident sur un client NFS :

1. Vérifiez les connexions au réseau.
2. Vérifiez que les démons **inetd**, **portmap** et **biod** sont exécutés sur le client comme indiqué à "État des démons NFS", page 10-10.
3. Vérifiez qu'un point de montage valide est disponible pour le système de fichiers en cours de montage. Pour plus d'informations, reportez-vous à "Configuration d'un client NFS", page 10-11.
4. Vérifiez que le serveur fonctionne en exécutant, à partir de l'invite du shell, côté client, la commande suivante :

   ```
   /usr/bin/rpcinfo -p server_name
   ```

   Si le serveur fonctionne, la liste des programmes, versions, protocoles et ports s'affiche comme suit :

```
program    vers  proto      port
100000        2      tcp        111    portmapper
100000        2      udp        111    portmapper
100005        1      udp       1025    mountd
100001        1      udp       1030    rstatd
100001        2      udp       1030    rstatd
100001        3      udp       1030    rstatd
100002        1      udp       1036    rusersd
100002        2      udp       1036    rusersd
100008        1      udp       1040    walld
100012        1      udp       1043    sprayd
100005        1      udp       694    mountd
100003        2      udp       2049    nfs
100024        1      udp         713    status
100024        1      tcp         715    status
100021        1      tcp         716    nlockmgr
100021        1      udp         718    nlockmgr
100021        3      tcp         721    nlockmgr
100021        3      udp         723    nlockmgr
100020        1      udp         726    llockmgr
100020        1      tcp         728    llockmgr
100021        2      tcp         731    nlockmgr
```

Sinon, connectez-vous au serveur à partir de la console du serveur et vérifiez l'état du démon **inetd** comme indiqué à "État des démons NFS", page 10-10.

5. Vérifiez que les démons **mountd**, **portmap** et **nfsd** sont actifs sur le serveur NFS en spécifiant à partir de l'invite du shell les commandes :

   ```
   /usr/bin/rpcinfo  -u  server_name  mount
   /usr/bin/rpcinfo  -u  server_name  portmap
   /usr/bin/rpcinfo  -u  server_name  nfs
   ```

   Si le démon est exécuté au niveau du serveur, les réponses renvoyées sont les suivantes :

   ```
   program  100005  version  1  ready  and  waiting
   program  100000  version  2  ready  and  waiting
   program  100003  version  2  ready  and  waiting
   ```

   Les numéros de programme correspondent aux commandes, comme indiqué dans l'exemple ci-dessus. Sinon, connectez-vous au serveur à partir de la console du serveur et vérifiez l'état des démons comme indiqué à "État des démons NFS", page 10-10.

6. Vérifiez que le fichier **/etc/exports** sur le serveur comporte le nom du système de fichiers que le client souhaite monter et que ce système de fichiers est exporté. Pour ce faire, entrez :

   ```
   showmount -e server_name
   ```

   Cette commande affiche la liste de tous les systèmes de fichiers exportés par *server_name*.

Erreurs d'écriture asynchrone

Lorsqu'un programme d'application inscrit des données dans un fichier appartenant à un système de fichiers monté NFS, l'écriture est planifiée pour être traitée en mode asynchrone par le démon **biod**. Si une erreur se produit au niveau du serveur NFS pendant l'écriture sur le disque, elle est signalée au client NFS et le démon **biod** la sauvegarde en interne dans les structures de données NFS. L'erreur enregistrée est ensuite renvoyée au programme d'application dès qu'il fait appel aux fonctions **fsync** ou **close**. Autrement dit, l'application n'est avertie de l'erreur que lorsque le programme ferme le fichier.
Cet événement survient généralement lors de la saturation d'un système de fichiers sur le serveur, toute tentative d'écriture entreprise par le client sur ce système étant vouée à l'échec.

Messages d'erreur NFS

Voici les messages d'erreur qui peuvent être générés lors de l'utilisation de NFS.

Message d'erreur nfs_server

Un nombre insuffisant de tampons de transmission peut entraîner le message d'erreur :

```
nfs_server:  bad  sendreply
```

Pour augmenter le nombre de tampons, vous disposez du raccourci Web-based System Manager **wsm network** ou du raccourci SMIT **smit hostent**. Sélectionnez ensuite votre type de carte et augmentez le nombre de tampons de transmission.

Messages d'erreur mount

Plusieurs cause peuvent provoquer l'échec d'un montage à distance. Les messages d'erreur associés aux échecs de montage sont les suivants :

`mount: ... already mounted`
: Le système de fichiers que vous tentez de monter l'est déjà.

`mount: ... not found in /etc/filesystems`
: Le système de fichiers ou le répertoire spécifié est introuvable.

Si vous exécutez la commande **mount** en spécifiant soit un répertoire soit un système de fichiers, et non les deux, la commande recherche dans le fichier **/etc/filesystems** l'entrée qui comporte le système de fichiers ou le répertoire correspondant. Si la commande **mount** trouve une entrée de la forme :

```
/dancer.src:
          dev=/usr/src
          nodename  =  d61server
          type  =  nfs
          mount  =  false
```

elle exécute le montage comme si vous aviez spécifié sur la ligne de commande :

```
/usr/sbin/mount -n dancer -o rw,hard /usr/src /dancer.src
```

`... not in hosts database`
: Emis sur un réseau sans NIS, ce message indique que l'hôte spécifié à la commande **mount** ne figure pas dans le fichier **/etc/hosts**. En revanche, sur un réseau exécutant NIS, ce message indique que NIS n'a pas pu trouver le nom d'hôte dans la base de données **/etc/hosts** ou que le démon NIS **ypbind** de votre machine n'est plus actif. Si le fichier **/etc/resolv.conf** existe, la résolution des noms d'hôte se fait via le serveur de noms. Le problème peut alors provenir de la base de données **named**.
Reportez-vous à "Résolution de noms sur un serveur NFS", page 10-42.

Vérifiez le libellé et la syntaxe de la commande **mount**. Si la commande est correctement spécifiée, vous pouvez en déduire que votre réseau n'exécute pas NIS et que ce message ne concerne que ce nom d'hôte. Vérifiez l'entrée correspondante dans le fichier **/etc/hosts.**

Si votre réseau exécute NIS, assurez-vous que le démon **ypbind** s'exécute en spécifiant à partir de la ligne de commande :

```
ps  -ef
```

Le démon **ypbind** doit apparaître dans la liste. Lancez la commande **rlogin** pour tenter de vous connecter à une autre machine distante ou la commande **rcp** pour effectuer une copie à distance sur une autre machine. Si ces opérations échouent, il est probable que votre démon **ypbind** est arrêté ou bloqué.

Si le message ne concerne que ce nom d'hôte, vérifiez l'entrée /**etc**/**hosts** sur le serveur NIS.

`mount:...server not responding: port mapper failure - RPC timed out`
: Soit le serveur à partir duquel le montage est effectué est hors service, soit le programme de mappage de ports est arrêté ou bloqué. Tentez de réamorcer le serveur pour relancer les démons **inetd**, **portmap** et **ypbind.**

Si la connexion au serveur à distance avec **rlogin** échoue, mais que le serveur fonctionne, testez la connexion réseau en vous connectant à une autre machine distante. Vérifiez également la connexion réseau du serveur.

`mount: ... server not responding: program not registered`
: La commande **mount** a contacté le programme de mappage de port, mais le démon de montage NFS **rpc.mountd** NFS n'était pas répertorié.

`mount: access denied ...`
: Le nom de votre machine ne figure pas dans la liste d'exportation du système de fichiers que vous tentez de monter à partir du serveur.

Pour obtenir la liste des systèmes de fichiers exportés du serveur, exécutez à partir de la ligne de commande :

```
showmount -e hostname
```

Si le système de fichiers recherché n'est pas répertorié ou que le nom de votre machine ou groupe de réseau ne figure pas dans la liste des utilisateurs du système de fichiers, connectez-vous au serveur et recherchez dans le fichier /**etc**/**exports** l'entrée correcte pour le système de fichiers. Un nom de système de fichiers apparaissant dans /**etc**/**exports** mais absent de la sortie de la commande **showmount** révèle une défaillance du démon **mountd** : soit le démon n'a pas pu analyser cette ligne dans le fichier, soit il n'a pas trouvé le répertoire, soit le répertoire spécifié n'a pas été monté localement. Si le fichier /**etc**/**exports** semble correct et que le réseau exécute NIS, vérifiez le démon **ypbind** sur le serveur : il est peut-être arrêté ou bloqué. Pour plus d'informations, reportez–vous au *AIX 4.3 NIS/NIS+ Guide*.

`mount: ...: Permission denied`
: Ce message signale tout échec d'authentification sur le serveur. Il peut s'afficher, dans l'exemple précédent, si vous ne figurez pas dans la liste d'exportation, si le serveur n'a pas reconnu le démon **ypbind** sur votre machine ou si le serveur refuse l'identité que vous lui avez soumise.

Vérifiez le fichier /**etc**/**exports** du serveur et, le cas échéant, le démon **ypbind.** Dans ce cas, changez simplement votre nom d'hôte à l'aide de la commande **hostname** et relancez la commande **mount**.

`mount: ...: Not a directory`
: Le chemin d'accès à distance ou local n'est pas un répertoire. Vérifiez le libellé de la commande et lancez l'exécution sur chaque répertoire.

`mount: ...: You are not allowed`
: Vous devez disposer des droits d'utilisateur racine ou être membre du groupe système pour exécuter la commande **mount** sur votre machine, car cette commande affecte le système de fichiers pour tous les utilisateurs sur cette machine. Seuls les utilisateurs racine et les membres du groupe système sont habilités à effectuer des montages et des démontages NFS.

Problèmes de temps d'accès à NFS

Si l'accès aux fichiers distants semble anormalement lent, recherchez les causes possibles. Il peut s'agir par exemple d'un démon incontrôlable ou d'une ligne **tty** erronée.

Vérification des processus

Sur le serveur, entrez :

```
ps  -ef
```

Si le serveur fonctionne normalement et que d'autres utilisateurs obtiennent les réponses dans des délais satisfaisants, vérifiez que votre démon **biod** est actif. Procédez comme suit :

1. Exécutez la commande **ps –ef** et recherchez les démons **biod** dans la sortie.

   Si ces démons sont arrêtés ou bloqués, passez aux étapes 2 et 3.

2. Arrêtez les démons **biod** actifs :

   ```
   stopsrc -x biod -c
   ```

3. Lancez les démons **biod** :

   ```
   startsrc -s biod
   ```

Pour déterminer si les démons **biod** sont bloqués, exécutez la commande **ps** comme indiqué ci-dessus, copiez un fichier volumineux d'un système distant et relancez la commande **ps**. Si les démons **biod** n'accumulent pas du temps CPU, ils sont probablement bloqués.

Vérification des connexions réseau

Si les démons **biod** fonctionnent, contrôlez les connexions au réseau. La commande **nfsstat** vérifie si des paquets sont perdus. Utilisez les commandes **nfsstat –c** et **nfsstat –s** pour savoir si un client ou un serveur retransmet des blocs de grande taille. En effet, des retransmissions sont toujours possibles lorsque des paquets ont été perdus ou que les serveurs sont occupés. Un taux de retransmission de 5 % est considéré comme élevé.

La probabilité de retransmissions peut être réduite en modifiant les paramètres des files d'attente de transmission des cartes de communication. Pour cette opération, vous pouvez utiliser SMIT (System Management Interface Tool).

Les valeurs recommandées pour les serveurs NFS sont :

MTU (Maximum Transmission Unit) de la carte de communication et tailles des files d'attente de transmission		
Carte	*UTM*	*File d'attente de transmission*
anneau à jeton 4 Mo 16 Mo	1500 3900 1500 8500	50 40 (Augmentez la valeur si la commande **nfsstat** dépasse le délai imparti.) 40 (Augmentez la valeur si la commande **nfsstat** dépasse le délai imparti.) 40 (Augmentez la valeur si la commande **nfsstat** dépasse le délai imparti.)
Ethernet	1500	40 (Augmentez la valeur si la commande **nfsstat** dépasse le délai imparti.)

Les tailles UTM maximales pour chaque vitesse d'anneau à jeton réduisent l'utilisation du processeur et favorisent considérablement les opérations de lecture/écriture.

Remarques :

1. Appliquez ces valeurs aux clients NFS si les retransmissions se poursuivent.
2. Tous les nœuds d'un réseau doivent utiliser la même taille UTM.

Taille UTM

Pour définir la taille MTU, utilisez le raccourci Web-based System Manager, **wsm network**, ou le raccourci SMIT, **smit chif**. Sélectionnez la carte qui convient et indiquez une valeur UTM dans le champ Maximum IP Packet Size.

Vous pouvez également utiliser la commande **ifconfig** (qui est *obligatoire* pour fixer la taille UTM à 8500). Le format de la commande **ifconfig** est le suivant :

```
ifconfig trn NodeName up mtu MTUSize
```

tr*n* étant le nom de votre carte, `tr0`, par exemple.

Enfin, vous pouvez combiner les deux méthodes : SMIT et la commande **ifconfig**.

1. Ajoutez la commande **ifconfig** pour les anneaux à jeton, comme indiqué dans l'exemple précédent, au fichier /**etc**/**rc.bsdnet**.
2. Entrez le raccourci **smit setbootup_option**. Faites basculer le champ Utilisation d'une configuration rc de style BSD sur **oui.**

Tailles de files d'attente de transmission

La taille des files d'attente de transmission des cartes de communication se définit à l'aide de SMIT. Entrez le raccourci **smit chgtok**, sélectionnez la carte concernée et indiquez une taille de file d'attente dans le champ Transmit.

Intervention sur programmes bloqués

Si des programmes bloquent au cours d'un travail sur un fichier, le serveur NFS est peut être arrêté. Dans ce cas, le message d'erreur suivant s'affiche :

```
NFS server hostname not responding, still trying
```

Le serveur NFS (*hostname*) est en panne. Ceci révèle un problème avec le serveur NFS, la connexion réseau ou le serveur NIS.

Vérifiez les serveurs à partir desquels vous avez monté les systèmes de fichiers si votre machine est complètement bloquée. Si un ou plusieurs d'entre eux sont hors service, il n'y a pas lieu de s'inquiéter. Les programmes se poursuivront automatiquement dès la remise en service des serveurs. Aucun fichier n'est détruit.

Si un serveur en montage logiciel expire, les autres travaux ne sont pas concernés. Les programmes qui dépassent le délai en tentant d'accéder aux fichiers distants en montage logiciel n'aboutissent pas et le message `errno` s'affiche. Mais vous pouvez toujours accéder aux autres systèmes de fichiers.

Si tous les serveur fonctionnent, déterminez si les autres personnes utilisant les mêmes serveurs rencontrent également des difficultés. Si plusieurs machines sont dans ce cas, l'anomalie provient des démons **nfsd** du serveur. Dans ce cas, connectez-vous au serveur et exécutez la commande **ps** pour voir si le démon **nfsd** s'exécute et accumule du temps CPU. Sinon, tentez d'arrêter et de relancer le démon **nfsd**. Si le problème persiste, réamorcez le serveur.

Si les autres systèmes semblent en service et fonctionner normalement, vérifiez votre connexion réseau et la connexion du serveur.

Droits d'accès et authentification

Une fois les montages correctement effectués, vous pouvez rencontrer des difficultés de lecture, écriture ou création de fichiers ou répertoires distants. Ce type de difficultés est généralement dû à des problèmes de droits ou d'authentification. La cause de ces problèmes de droit ou d'authentification dépendent du NIS utilisé ou de la protection appliquée aux montages.

Dans le cas de figure le plus simple, les montages ne sont pas sécurisés et NIS n'est pas utilisé. Dans ce cas, les ID utilisateur (UID) et les ID groupe (GID) sont alors mappés par le seul biais des fichiers serveur et clients /**etc**/**passwd** et /**etc**/**group**, respectivement. Dans ce cas, pour qu'un utilisateur appelé `john` soit identifié comme `john` sur le client et sur le serveur, l'utilisateur `john` doit disposer dans le fichier /**etc**/**passwd** du même ID utilisateur. En voici un contre-exemple :

```
User  john  is  uid  200  on  client  foo.
User  john  is  uid  250  on  server  bar.
User  jane  is  uid  200  on  server  bar.
```

Le répertoire `/home/bar` est monté à partir du serveur `bar` sur le client `foo`. Si l'utilisateur `john` édite des fichiers sur le système de fichiers distant `/home/bar` du client `foo`, la sauvegarde des fichiers générera des confusions.

Pour le serveur `bar`, les fichiers appartiennent à `user jane`, car l'ID de `jane` est `200` sur `bar`. Si `john` se connecte directement à `bar` par la commande **rlogin**, il est probable qu'il ne pourra pas accéder aux fichiers qu'il vient de créer en travaillant sur le système de fichiers monté à distance. En revanche, `jane` peut y accéder car les machines gèrent les droits d'accès par UID et non par nom.

La seule solution pour résoudre ce problème durablement est de réaffecter des UID cohérents sur les deux machines. Par exemple, attribuez à `john` l'UID 200 sur le serveur `bar` ou 250 sur le client `foo`. Il faut alors appliquer aux fichiers appartenant à `john` la commande **chown** pour que les nouveaux ID leur soient attribués sur les machines correspondantes.

En raison des problèmes de maintien de mappages UID et GID cohérents sur toutes les machines d'un réseau, NIS ou NIS+ est souvent utilisé pour pallier ce type de problème. Reportez–vous au *AIX 4.3 NIS/NIS+ Guide* pour plus d'informations.

Résolution des noms sur un serveur NFS

Lorsqu'un serveur NFS prend en compte une requête de montage, il recherche le nom du client demandeur. Le serveur recherche, sur la base de l'adresse IP (Internet Protocol) du client, le nom hôte correspondant à cette adresse. Muni de ce nom, le serveur consulte la liste d'exportation du répertoire demandé et vérifie que le client est cité dans la liste d'accès au répertoire. S'il trouve une entrée relative au client qui corresponde exactement au résultat de la résolution de noms, l'authentification est accordée à ce niveau.

Si le serveur ne parvient pas à résoudre l'adresse IP en nom d'hôte, il rejette la demande de montage. Le serveur doit être en mesure de trouver une correspondance pour l'adresse IP du client demandeur. Si le répertoire est exporté avec une autorisation d'accès accordée à tous les clients, le serveur peut effectuer la résolution inverse pour accepter la demande de montage.

Le serveur doit également retrouver le nom exact du client. Considérons par exemple une entrée du fichier /**etc**/**exports** telle que :

```
/tmp      -access=silly:funny
```

A cette entrée correspondent, dans le fichier /**etc**/**hosts**, les entrées suivantes :

```
150.102.23.21        silly.domain.name.com
150.102.23.52        funny.domain.name.com
```

Remarquons que les noms ne correspondent pas exactement. Lorsque le serveur recherche les équivalences adresse IP– nom d'hôte pour les hôtes `silly` et `funny`, il ne retrouve pas exactement les mêmes chaînes de nom dans la liste d'accès d'exportation. Ce phénomène se produit généralement lorsque la résolution de noms est effectuée par le démon **named**. En effet, la plupart des bases de données du démon **named** contiennent des alias des noms complets des hôtes pour simplifier la tâche de l'utilisateur lors de la spécification des hôtes. Bien que des entrées noms hôte-adresses IP existent pour les alias, la recherche inversée peut ne pas être définie. La base de données pour la recherche inversée (adresse IP – nom hôte) contient généralement des entrées indiquant l'adresse IP et le nom complet de domaine (et non l'alias) de cet hôte. Parfois, les entrées d'exportation sont créées avec l'alias et le client rencontre des difficultés lorsqu'il tente d'effectuer un montage.

Limitation du nombre de groupes dans la structure NFS

Sur les systèmes qui utilisent NFS version 3.2, les utilisateurs ne peuvent pas, sans complications, être membres de plus de 16 groupes. (Les groupes sont définis via la commande **groups**.) Si un utilisateur dépend de 17 groupes, il ne sera pas autorisé à lire ou copier les fichiers du 17ème. Il faut alors modifier l'ordre de ces groupes pour lui permettre d'accéder à ces fichiers.

Montage à partir de serveurs équipés d'une version NFS antérieure

Lors du montage d'un système de fichiers à partir d'un serveur NFS de version antérieure à la 3 vers un client NFS version 3, l'utilisateur résidant sur le client rencontrera des difficultés de montage s'il est membre de plus de 8 groupes. En effet, certains serveurs, incapables de traiter correctement ce cas, refusent la demande de montage. La seule solution consiste à réduire le nombre de groupes auxquels appartient l'utilisateur concerné et de soumettre de nouveau la demande de montage. Le message d'erreur suivant est caractéristique de ce type de problème :

```
RPC:    Authentication  error;  why=Invalid  client  credential
```

Conséquences d'une extension de noyau NFS non chargée

Certaines commandes NFS ne s'exécutent pas correctement si l'extension de noyau NFS n'est pas chargée. Parmi ces commandes : **nfsstat**, **exportfs**, **mountd**, **nfsd** et **biod**. Lorsque NFS est installé sur le système, l'extension du noyau est placée dans le fichier **/usr/lib/drivers/nfs.ext**. Ce fichier est ensuite chargé comme extension de noyau lors de la configuration du système. Le script qui constitue cette extension charge le fichier **/etc/rc.net**. Ce script prévoit également, entre autres choses, le chargement de l'extension NFS. Remarquons à ce sujet, que l'extension de noyau TCP/IP (Transmission Control Protocol/Internet Protocol) doit être chargée avant l'extension de noyau NFS.

Remarque : La commande **gfsinstall** est utilisée pour charger l'extension NFS dans le noyau au démarrage initial du système. Cette commande peut être lancée plusieurs fois par amorçage sans générer de complications. Le système est actuellement livré avec la commande **gfsinstall**, présente à la fois dans le fichier **/etc/rc.net** et le fichier **/etc/rc.nfs**. Ce doublon est correct. Il est inutile de supprimer l'une ou l'autre de ces occurrences.

Informations de référence NFS

Liste des fichiers NFS (Network File System)

bootparams	Recense les clients qui peuvent être utilisés pour le démarrage des clients sans disque.
exports	Recense les répertoires qui peuvent être exportés vers des clients NFS.
networks	Contient des informations sur les réseaux du réseau Internet.
Fichier de configuration **pcnfsd.conf**	Fournit les options de configuration du démon **rpc.pcnfsd**.
rpc	Contient les informations de base de données pour les programmes RPC (Remote Procedure Call).
xtab	Recense les répertoires actuellement exportés.
/etc/filesystems	Répertorie tous les systèmes de fichiers qui sont montés au démarrage du système.

Liste des commandes NFS

chnfs	Lance un nombre donné de démons **biod** et **nfsd**.
mknfs	Configure le système pour qu'il exécute NFS et lance les démons NFS.
nfso	Configure les options de réseau NFS.
automount	Monte automatiquement un système de fichiers NFS.
chnfsexp	Modifie les attributs d'un répertoire exporté vers NFS.
chnfsmnt	Modifie les attributs d'un répertoire monté sur NFS.
exportfs	Exporte et annule l'exportation de répertoires vers des clients NFS.
lsnfsexp	Affiche les caractéristiques des répertoires exportés avec NFS.
lsnfsmnt	Affiche les caractéristiques des systèmes NFS montés.
mknfsexp	Exporte un répertoire en utilisant NFS.
mknfsmnt	Monte un répertoire en utilisant NFS.
rmnfs	Arrête les démons NFS.
rmnfsexp	Supprime les répertoires NFS exportés de la liste des exportations d'un serveur.
rmnfsmnt	Supprime les systèmes de fichiers NFS montés de la liste des montages d'un client.

Liste des démons NFS

Verrouillage des démons

lockd	Traite les requêtes de verrouillage par le biais du module RPC.
statd	Fournit des fonctions de reprise pour les services de verrouillage sur NFS.

Utilitaires et démons de service réseau

biod	Envoie les requêtes de lecture et d'écriture du client au serveur.
mountd	Répond aux requêtes des clients pour le montage de systèmes de fichiers.
nfsd	Lance le démon qui traite une requête de client concernant les opérations sur les systèmes de fichiers.
pcnfsd	Traite les requêtes de service des clients PC–NFS.
nfsstat	Affiche les informations concernant les possibilités pour une machine de recevoir les appels.
on	Exécute des commandes sur des machines distantes.
portmap	Mappe les numéros de programme RPC et les numéros de port Internet.
rexd	Accepte les requêtes d'exécution de programmes à partir de machines distantes.
rpcgen	Génère le code C afin d'implémenter le protocole RPC.
rpcinfo	Rend compte de l'état des serveurs RPC.
rstatd	Renvoie les statistiques de performance obtenues du noyau.
rup	Affiche l'état d'un hôte distant sur le réseau local.
rusers	Recense les utilisateurs connectés sur des machines distantes.
rusersd	Répond aux requêtes de la commande **rusers**.
rwall	Envoie des messages à tous les utilisateurs du réseau.
rwalld	Gère les requêtes de la commande **rwall**.
showmount	Affiche la liste de tous les clients ayant monté des systèmes de fichiers distants.
spray	Envoie un nombre spécifique de paquets à un hôte.
sprayd	Reçoit les paquets envoyés par la commande **spray**.

Utilitaires et démons de sécurité du réseau

chkey	Modifie la clé de chiffrement de l'utilisateur.
keyenvoy	Fournit un intermédiaire entre les processus utilisateur et le serveur de clé.
keylogin	Décrypte et enregistre la clé privée de l'utilisateur.
keyserv	Enregistre les clés publiques et les clés privées.
mkkeyserv	Lance le démon **keyserv** et annule la mise en commentaire des entrées appropriées dans le fichier /**etc**/**rc.nfs**.
newkey	Crée une nouvelle clé dans le fichier **publickey**.
rmkeyserv	Arrête le démon **keyserv** et met en commentaire l'entrée correspondant au démon **keyserv** dans le fichier /**etc**/**rc.nfs**.
ypupdated	Met à jour les informations des mappes NIS (Network Information Service).

Support des clients sans disque Sun

bootparamd	Fournit les informations nécessaires au démarrage des clients sans disque.

Sous–routines NFS

cbc_crypt, des_setparity ou ecb_crypt	Implémente les routines DES (Data Encryption Standard).

Chapitre 11. AIX Fast Connect pour Windows

AIX Fast Connect pour Windows

AIX Fast Connect pour Windows est un logiciel serveur qui permet aux serveurs et aux stations de travail AIX de partager des fichiers et des imprimantes avec des clients PC travaillant avec Windows NT, Windows 98, Windows 95, Windows For Workgroups ou des systèmes d'exploitation OS/2. Ce chapitre traite des sujets suivants :

Présentation de AIX Fast Connect pour Windows

AIX Fast Connect pour Windows utilise le protocole de réseau Microsoft. Les clients PC peuvent donc accéder aux fichiers et aux imprimantes AIX à l'aide de leur logiciel réseau natif. Les utilisateurs PC peuvent utiliser des sytèmes de fichiers AIX distants directement à partir de leurs machines comme s'ils étaient sauvegardés en local. De plus, ils peuvent imprimer des tâches sur des imprimantes dotées d'un système de spoulage AIX, visualiser celles qui sont disponibles et configurer une imprimante réseau.

Fast Connect offre ces services par la mise en œuvre du protocole de réseau SMB (Server Message Block) associé au NetBIOS (Network Basic Input/Output System) via le TCP/IP (Transmission Control Protocol/Internet Protocol), sur la base des RFC (Requêtes de commentaires) 1001 et 1002 de l'Internet Engineering Task Force.

Les principales fonctions de Fast Connect sont les suivantes :

- Intégration étroite avec AIX et exploitation de fonctions, telles que les routines, les E/S du noyau, le système de fichiers et la sécurité.
- Services de fichiers et d'impressions basés sur SMB
- Authentification du transit et de la connexion aux domaines NT.
- Protocole de navigation au sein des ressources
- Verrouillage opportuniste (oplock)
- WINS client et mandataire
- Prise en charge du B–node
- Prise en charge de l'interface de programmation d'application (API) Send File
- Fonctions de journalisation et de suivi
- Maintenance et administration avec l'interface utilisateur de votre choix : commandes, Web-based System Manager ou l'outil SMIT (System Management Interface Tool).
- Configuration rationalisée
- Prise en charge du mappage des noms de fichiers longs AIX vers des noms de fichiers DOS.
- Représentation Unicode de noms de répertoires, de fichiers, d'utilisateurs et de partages.

Concepts et termes courants

Vous trouverez ci–dessous l'explication de certains termes réseau courants :

Nœuds de diffusion (B–nodes)
: Un nœud de diffusion ou B–node est un type de nœud terminal NetBIOS qui prend en charge le service NetBIOS et contient des applications. Les B–nodes communiquent à l'aide de datagrammes UDP et de connexions TCP. Ces B–nodes interagissent librement au sein d'une zone de diffusion. Les autres nœuds terminaux standard sont les nœuds point à point (P–nodes) et les nœuds en mode mixte (M–nodes).

Navigation
: Cette fonction permet de visualiser les ressources disponibles sur un réseau. La liste de navigation d'un réseau Windows répertorie les autres hôtes et domaines disponibles. Windows met à jour cette liste. Par le biais d'une interface réseau conviviale, elle présente les autres serveurs offrant des services réseau. Ce faisant, les utilisateurs n'ont pas à mémoriser les noms des hôtes et services à distance. Windows 95, Windows 98 et Windows NT utilisent la liste de navigation pour définir la structure du réseau présenté dans Network Neighborhood et Windows Explorer. Cette liste est également accessible en tapant la commande **NET VIEW** au niveau de l'invite système.

Les domaines de Windows for Workgroups et de Windows NT mettent à jour la liste de navigation à partir d'un ordinateur appelé Master Browser (Navigateur maître). La première fois qu'un ordinateur offre un service réseau, il diffuse un paquet d'annonces serveur. Le Master Browser reçoit ce paquet et ajoute le nom de l'ordinateur à sa liste de navigation. En réponse, le Master Browser transmet au nouvel ordinateur une liste de navigateurs secondaires.

Chaque groupe de domaine ou NT contient au moins un navigateur secondaire. Une copie de la liste de navigation est mise à jour sur le navigateur secondaire afin d'éviter d'avoir à refaire cette liste en cas de défaillance du Master Browser.

CIFS
: CIFS est l'abréviation de Common Internet File System Protocol. Le CIFS offre une plate–forme croisée ouverte permettant aux systèmes client de demander des services de fichiers auprès des systèmes serveur du réseau. Il s'articule autour du protocole Server Message Block très utilisé par les PC et les stations de travail travaillant avec un grand nombre de systèmes d'exploitation. Il s'agit d'une ébauche soumise par Microsoft à l'Internet Engineering Task Force pour un accès transparent aux fichiers par le biais d'Internet.

NetBIOS
: NetBIOS ou Network Basic Input/Output System est une interface réseau non liée à un fournisseur. Elle était au départ conçue pour les systèmes PC IBM travaillant avec PC–DOS ou MS–DOS. NetBIOS est une interface logicielle, mais on ne peut pas parler d'un véritable protocole réseau. Elle précise les services disponibles sans émettre aucune restriction quant au protocole utilisé pour leur mise en place.

Il n'existe pas de norme NetBIOS officiellement définie. La version originale, telle que décrite par IBM en 1984 dans le *IBM PC Network Technical Reference Manual*, est considérée comme la norme de fait. Depuis son introduction, on a compté trois "moutures" de NetBIOS, assorties de leur protocole de transport spécifique : NetBEUI, NetBIOS over IPX et NetBIOS over TCP/IP.

Fast Connect utilise NetBIOS over TCP/IP.

Interface NetBIOS avec programmes d'application
: Sur les PC, NetBIOS comporte un ensemble de services ainsi qu'une interface programme répondant exactement à ces services. On distingue trois types de services NetBIOS :

  Service de noms
  : Les ressources NetBIOS sont identifiées par un nom. Les applications NetBIOS n'ont pas accès aux adresses de niveau inférieur. Une application représentant une ressource enregistre un ou plusieurs noms qu'elle souhaite utiliser.

    L'espace nom a une structure plate, non hiérarchisée. Il utilise 16 caractères alphanumériques. Les noms ne peuvent pas commencer par un astérisque (*).

L'enregistrement implique une demande d'utilisation d'un nom. La demande peut être formulée pour détenir la propriété exclusive (unique) ou partagée (groupe). Il y a confrontation en temps réel entre les différentes applications. Deux applications du réseau NetBIOS ne peuvent pas utiliser un nom unique à moins que l'application d'origine demande la suppression de son nom ou que l'hôte soit éteint ou réinitialisé.

Les trois opérations de base offertes par le service Noms sont les suivantes : **Add Name**, **Add Group Name** et **Delete Name**.

Service de sessions

Une session est un échange de messages en duplex intégral, fiable et structuré, intervenant entre deux applications NetBIOS. Les données sont organisées en messages.

Il peut exister plusieurs sessions entre deux applications. Les deux applications participant à la session ont accès au nom de l'application à distance. Il n'existe aucune directive quant à la résolution des requêtes de sessions d'un nom de groupe en connexion de données. Une application dispose d'un service de détection des échecs au niveau de la session.

Les opérations de base offertes par le service de sessions sont les suivantes : **Call**, **Listen**, **Hang Up**, **Send**, **Receive** et **Session Status**.

Services de datagrammes

Le service de datagrammes n'est pas un dispositif de communication fiable, structuré et sans connexion entre deux applications NetBIOS. Il s'apparente au service UDP sous TCP/IP.

Les datagrammes sont envoyés assortis d'un nom dûment enregistré par l'expéditeur. Ils peuvent être envoyés à une adresse spécifique ou diffusés de manière explicite.

Les datagrammes adressés à un nom en particulier sont réceptionnés par le destinataire exclusif. Les datagrammes adressés à un nom de groupe sont multi–destinataires. L'expéditeur ne fait pas la distinction entre noms de groupe et noms uniques. C'est pourquoi, il fait comme si tous les datagrammes non assortis d'une instruction de diffusion étaient multi–destinataires.

Comme avec le service de sessions, le destinataire du datagramme est informé des noms de l'expéditeur et du destinataire.

Les opérations de base du service de datagrammes sont les suivantes : **Send Datagram**, **Send Broadcast Datagram**, **Receive Datagram** et **Receive Broadcast Datagram**.

Résolution de noms NetBIOS

Cette fonction permet le mappage d'un nom NetBIOS vers son adresse IP. Les techniques couramment utilisées pour ce faire sont le Windows Internet Name Service (WINS), le fichier **LMHOSTS** et le système de noms de domaine (DNS). Ce système est expliqué dans la section Résolution de noms TCP/IP, page 3-103. Les autres techniques sont traitées ci–dessous :

WINS
: Lors de la mise à disposition d'un nouveau service réseau, tout comme lors de l'amorçage d'une machine Windows ou du démarrage de Fast Connect, le service doit être enregistré auprès d'un serveur WINS avant de pouvoir être accessible aux clients d'autres sous–réseaux. Le serveur WINS enregistre le nom de l'hôte, le domaine NT auquel l'hôte appartient ainsi que son adresse IP. Chaque fois qu'une machine tente de résoudre un nom d'hôte, elle interroge d'abord le serveur WINS. Si l'hôte n'y est pas enregistré, elle essaie de le trouver à l'aide d'un message de diffusion. Si l'hôte reste introuvable, un message d'erreur s'affiche (`a computer or sharename could not be found`). Fast Connect s'enregistre comme il se doit auprès d'un serveur WINS.

  Le WINS comporte également une méthode de réplication de sa base de données de noms d'hôtes avec d'autres serveurs WINS. Ce faisant, un serveur WINS secondaire est créé afin de recevoir des requêtes en cas d'indisponibilité du serveur WINS principal. Cela permet également de décongestionner les gros réseaux gênés par la lenteur des liaisons. Les serveurs sont ainsi placés plus près des clients et la résolution de noms se fait plus rapidement. (Le protocole WINS est la propriété de Microsoft).

LMHOSTS
: LMHOSTS est l'abréviation de LanManager Hosts. Il s'apparente au fichier /**etc**/**hosts** d'UNIX. Le fichier **LMHOSTS** permet le mappage des noms d'hôtes spécifiques vers les adresses IP. Il offre également une syntaxe de définition du domaine dans lequel l'hôte réside ainsi que de chargement d'un fichier **LMHOSTS** à partir du répertoire partagé d'un serveur.

  Pour plus d'informations sur le fichier **LMHOSTS**, reportez–vous au *Windows NT Networking Guide* ou au *Windows 95 Resource Kit*.

NetBIOS over TCP/IP
: NetBIOS over TCP/IP a été pour la première fois proposé dans les RFC 1001 et 1002, soumises à l'Internet Engineering Task Force en 1987. Ces RFC décrivent la mise en œuvre de NetBIOS à l'aide du TCP (Transmission Control Protocol) pour les services de sessions orientées–connexion et de l'UDP (User Datagram Protocol) pour les services de datagrammes.

Cette conception présente des avantages considérables par rapport à NetBEUI et NetBIOS over IPX. Premièrement, elle utilise des protocoles TCP/IP existants et peut donc être acheminée sur Internet à l'échelle globale ainsi que sur tous les autres grands réseaux. Deuxièmement, la mise en place logicielle de l'interface NetBIOS peut être faite avec la structure TCP/IP existante sans avoir à ajouter de nouveaux pilotes réseau. Le TCP/IP étant déjà pris en charge par la plupart des systèmes d'exploitation, la prise en charge de NetBIOS devrait se faire sans grande difficulté.

NetBIOS Scope
: NetBIOS Scope est l'ensemble des ordinateurs au sein duquel le nom NetBIOS est enregistré. Les opérations de datagrammes multi–destinataires et de diffusion NetBIOS doivent porter sur l'ensemble de NetBIOS.

Commande **net**
: La commande **net** et ses sous–commandes peuvent être utilisées pour configurer et gérer le serveur Fast Connect Server à partir de la ligne de

commande. Par ailleurs, le Web-based System Manager et le SMIT offrent des interfaces pilotées par menu permettant d'effectuer les mêmes tâches. Pour plus d'informations sur la commande **net**, reportez–vous au *AIX Commands Reference, Volume 4*.

Authentification du transit
: L'authentification du transit est un mécanisme employé par le serveur Fast Connect afin de valider les autorisations utilisateur auprès d'un contrôleur de domaine, et en cas de validation, d'autoriser l'accès de l'utilisateur à une ressource du serveur Fast Connect. Pour plus d'informations sur l'authentification du transit, reportez–vous à l'ébauche Internet, *CIFS Login and Passthrough Authentication, Prelim Draft, Jan 3, 1997* élaborée par Leach and Naik de Microsoft.

SMB
: SMB est l'abréviation de Server Message Block. Il s'agit du protocole utilisé en supplément de NetBIOS pour la mise mise en œuvre des services d'impression et de partage des fichiers de Windows.

Avec ce protocole, les clients échangent des messages (appelés blocs de messages serveur) avec un serveur afin d'accéder à ses ressources. Tous les messages SMB ont un format commun : ils comportent un en–tête de taille fixe suivi d'un composant de données et d'un paramètre de taille variable.

On peut distinguer quatre types de messages SMB :

- Les messages de contrôle de session génèrent, authentifient et terminent des sessions.
- Les messages d'impression et de fichiers contrôlent respectivement l'accès à l'imprimante et aux fichiers.
- Les commandes de messages permettent à une application d'envoyer ou de recevoir des messages à destination ou en provenance d'un autre hôte.

Lorsqu'un client SMB négocie une connexion avec un serveur du même nom, les deux parties décident d'un protocole de communication commun. Cette fonctionnalité permet les extensions de protocole mais accroît la complexité du SMB.

Partages
: Les partages sont des ressources partagées par le serveur Fast Connect. Les deux types de partages pris en charge par Fast Connect sont les imprimantes et les fichiers AIX.

Groupes de travail
: Un groupe de travail est un ensemble logique de stations de travail et de serveurs qui n'appartiennent pas à un domaine. Dans un groupe de travail, chaque ordinateur enregistre sa copie des informations relatives aux comptes utilisateurs et groupes. C'est pourquoi, au sein des groupes de travail, les utilisateurs ne peuvent se connecter directement qu'aux machines sur lesquelles ils disposent d'un compte. Les membres d'un groupe de travail peuvent visualiser et utiliser les ressources d'autres systèmes. Pour ce faire, les ressources sont partagées au sein du groupe de travail et les utilisateurs réseau sont validés par la machine disposant de la ressource.

Limitations relatives à AIX Fast Connect pour Windows

Les limitations suivantes s'appliquent à AIX Version 4.3.3 ainsi qu'aux versions antérieures de Fast Connect :

- Fast Connect ne permet pas plusieurs partages du même nom de file d'attente d'impresssion. En d'autres termes, si une imprimante partage déjà une file d'attente d'impression, vous ne pouvez pas en créer une autre (avec un nom "net" différent). Si vous passez outre cette recommandation, un message d'erreur s'affiche **Operation could not be performed**.
- Les utilisateurs d'OS/2 ou d'autres clients ne prenant pas en charge l'unicode doivent s'assurer de la correspondance entre les données locales client et serveur.
- Les ACL AIX ne sont ni reconnus ni pris en charge. Les règles explicites d'accès ou de refus d'accès utilisateur/groupe ne sont pas prises en compte.
- L'audit de sécurité ne porte pas sur les actions individuelles de l'utilisateur par le biais d'un client SMB. Si la fonction d'audit est activée, certains événements du journal d'audit auront l'identité racine.
- Le quota disque et le ulimit d'un utilisateur ne sont pas contrôlés. Un utilisateur peut remplir le système de fichiers partagé.
- Il n'existe pas de prise en charge des autorisations DCE/DFS ou des systèmes de fichiers. Les systèmes de fichiers DCE/DFS ne peuvent pas être partagés.
- Il n'existe pas d'informations de journalisation permettant d'identifier les utilisateurs connectés au serveur AIX par le biais de AIX Fast Connect pour Windows.
- Certains pilotes d'imprimante AIX ajoutent des commandes au fichier en cours d'impression, d'autres non. Toutefois, les clients Windows émettent toujours dans un format ne nécessitant aucune commande. C'est pourquoi, si le pilote d'imprimante AIX est de ce type, vous devez définir les options correspondantes **–o –dp** lors de la création du partage d'imprimante.

AIX Fast Connect pour Windows Caractéristiques

Cette section traite des caractéristiques matérielles et logicielles pour le serveur AIX et ses clients PC.

Caractéristiques matérielles du serveur

AIX Fast Connect pour Windows fonctionne sur toutes les machines prenant en charge le système d'exploitation AIX à l'exception des machines sans disque ou sans données. La machine doit être dotée d'un adaptateur de réseau pris en charge par TCP/IP et être connectée physiquement à un réseau. Le système doit avoir au moins 32 Mo de RAM (64 Mo de préférence) et 50 Mo d'espace disque disponible.

Caractéristiques logicielles du serveur

Les caractéristiques logicielles du serveur pour AIX Fast Connect pour Windows sont les suivantes :

- AIX Version 4.3.2 ou ultérieure
- La taille de /**var** doit être suffisamment importante pour enregistrer temporairement le fichier le plus gros pouvant être imprimé par le service correspondant.
- Les fichiers **bos.net.tcp.client** version 4.3.2.0 ou ultérieure doivent être installés et configurés.
- Les fichiers **bos.rte.loc** version 4.3.2.2 ou ultérieure doivent être installés et configurés.
- AIX Version 4.3.2 APAR IX85388 est nécessaire à la prise en charge de sendfile par l'API.

Caractéristiques du matériel client

Chaque PC client doit avoir un adaptateur LAN installé et être physiquement connecté à un réseau.

Caractéristiques du logiciel client

Pour utiliser Fast Connect, tous les clients doivent disposer des éléments suivants :

- Un navigateur web avec prise en charge de masques (Netscape, par exemple) afin de pouvoir utiliser l'outil Web-based System Manager.

et un des systèmes d'exploitation suivants :

- Windows NT 4.0
- Windows 98
- Windows 95 avec service pack version 1 ou ultérieure
- Windows for Workgroups version 3.11 ou ultérieure
- OS/2 Warp 4.0 ou ultérieure

AIX Fast Connect pour Windows Pack produit et installation

Cette section traite des caractéristiques des images du pack produit et de l'installation de AIX Fast Connect pour Windows.

Pack produit

Le pack produit Fast Connect comporte les images suivantes :

Image	Description
cifs.base	Utilitaires serveur Fast Connect
cifs.msg	Messages serveur Fast Connect
cifs.basic	Serveur Fast Connect (Windows uniquement)
ou	
cifs.advanced	Serveur évolué Fast Connect (Windows et OS2)

Ces images contiennent les fichiers suivants :

Image	Fichiers	Description des fichiers
cifs.base	cifs.base.websm	Prise en charge de Web-based System Manager de Fast Connect
	cifs.base.smit	Prise en charge SMIT Fast Connect
	cifs.base.cmd	Commandes Fast Connect
cifs.msg	cifs.msg	Messages serveur Fast Connect (la langue est indiquée par l'extension de fichier)
cifs.basic	cifs.basic.rte	Serveur Fast Connect (Windows uniquement)
cifs.advanced	cifs.advanced.rte	Fichiers du serveur évolué Fast Connect (Windows et OS2)

Installation

AIX Fast Connect pour Windows est installé sur AIX Version 4.3.2 ou une version ultérieure. Les fichiers suivants doivent déjà être installés et configurés :

- **bos.net.tcp.client** version 4.3.2.0 ou ultérieure
- **bos.rte.loc** version 4.3.2.2. ou ultérieure

De plus, AIX Version 4.3.2 IX85388 est nécessaire à la prise en charge de **sendfile** par l'API.

Outre ces caractéristiques logicielles, Fast Connect nécessite environ 50 Mo d'espace disque supplémentaire. Pour plus d'informations, reportez–vous au *AIX 4.3 Installation Guide*.

Une fois l'installation terminée, les fichiers suivants apparaissent sur le système :

Fichier	Type	Chemin d'accès	Description
cifsServer	binaire	**/usr/sbin**	Démon du serveur Fast Connect
cifsServerAdv	binaire	**/usr/sbin**	Démon du serveur évolué Fast Connect
cifsPrintServer	binaire	**/usr/sbin**	Démon du serveur de fichiers d'impression Fast Connect

Fichier	Type	Chemin d'accès	Description
net	binaire	**/usr/sbin**	Commande d'administration Fast Connect
rc.cifs	Script	**/etc**	Script shell de marche/arrêt Fast Connect pour **inittab**
cifsConfig	ASCII	**/etc/cifs**	Fichier de configuration Fast Connect
cifsPasswd	ASCII	**/etc/cifs**	Fichier de configuration utilisateur Fast Connect
README	ASCII	**/etc/cifs**	Documentation supplémentaire sur Fast Connect
cifsLog	ASCII	**/var/cifs**	Fichier de journalisation Fast Connect
cifsTrace*	ASCII	**/var/cifs**	Fichier de suivi Fast Connect
sm_smb.cat	Catalogue de messages	**/usr/lib/nls/msg**	Catalogue de messages Fast Connect (langue indiquée dans l'extension de nom de fichier)

Remarque : une fois l'installation terminée, le fichier **cifsTrace** n'apparaît pas sur le système.

AIX Fast Connect pour Windows Configuration

Vous pouvez utiliser Web-based System Manager, le SMIT, la commande **net** ou une combinaison de ces méthodes pour configurer le serveur Fast Connect de votre site.

Paramètres configurables

Fast Connect est conçu pour faciliter la gestion sans pour autant sacrifier la personnalisation nécessaire du système. Par conséquent, il n'est possible d'accéder qu'à un petit nombre de paramètres configurables.

Remarque : la plupart de ces paramètres sont configurables de manière dynamique et ne nécessitent pas l'arrêt ni le redémarrage du serveur afin que les modifications soient prises en compte.

Vous trouverez ci–dessous une brève description de ces paramètres :

Paramètre	Description	Type	Valeur (par défaut, min, max)	S/D[1]
autodisconnect	Délai (en minutes) des sessions inactives	int	120, 0, 65535	D
backup_passthrough _authentication_server	Adresse IP du serveur d'authentification de transit secondaire	Chaîne	n/a	D
comment	Commentaire du serveur	Chaîne	n/a	D
domainname	Domaine du serveur	Chaîne	n/a	S
dosattrmapping	Assortis d'une valeur de 1, les attributs Archive, System et Hidden sont alors mappés vers les bits d'exécution User, Group et Other. Dans le cas contraire, ces attributs ne sont pas pris en charge.	int	(1, 0, 1)	D
dosfilenamemapchar	Caractère utilisé pour mapper les noms de fichiers longs vers le format 8,3. Les valeurs reconnues sont la tilde (~) et l'accent circonflexe (^). La tilde (~) est la valeur par défaut.	char	~	D
dosfilenamemapping	Assortis d'une valeur de 1, les noms de fichiers longs sont mappés vers le format 8,3. Dans le cas contraire, ces noms sont tronqués. Pour plus d'informations, reportez–vous à la section Mappage de noms de fichiers AIX longs vers des noms de fichiers DOS, page 11-16.	int	(1, 0, 1)	D

Paramètre	Description	Type	Valeur (par défaut, min, max)	S/D[1]
encrypt_passwords	Assorti d'une valeur de 0, le mot de passe est constitué de texte en clair. Avec une valeur autre que 0, négociation avec le client.	int	(1, 0, 2)	S
filenamematchinglevel	Avec une valeur fixée à 0, correspondance sans distinction des majuscules et des minuscules. Avec une valeur de 1, correspondance avec distinction des majuscules et des minuscules.	int	(1, 0, 1)	S
guestlogonsupport	Autorisation d'accès donnée ou non à un "invité".	int	(0, 0, 1)	D
guestname	Identification de l'invité.	Chaîne	n/a	D
maxconnections[2]	Nombre maximum de connexions ouvertes sur le serveur.	int	0, 0, 1000	D
maxconnections[2]	Nombre maximum de fichiers ouverts sur le serveur.	int	0, 0, 1000	D
maxsearches[2]	Nombre maximum de recherches ouvertes sur le serveur	int	0, 0, 1000	D
maxusers[2]	Nombre maximum de sessions utilisateur autorisé.	int	0, 0, 1000	D
nbns	Avec une valeur de 1, le serveur fonctionne comme un serveur de noms NETBIOS.	int	1, 0, 1	S
oplockfiles	Prise en charge ou non de oplocks sur les fichiers.	Y/N (oui/non)	oui, non, oui	S
oplocktimeout	Délai exprimé en secondes pour **oplock**.	int	35, 35, 640	S
os2compatible	Avec une valeur de 0, READONLY fait référence à tous les fichiers accessibles en lecture mais pas en écriture. Avec une valeur de 1, READONLY fait référence à tous les fichiers accessibles en lecture.	int	1, 0, 1	D
passthrough_authentication_server	Adresse IP du serveur d'authentification de transit	Chaîne	n/a	D
wins_proxy	Fonctionnement ou non du serveur comme mandataire WINS.	int	(0, 0, 1)	D
primary_wins_ipaddr	Adresse IP de l'adresse WINS principale.	Chaîne	n/a	D
secondary_wins_ipaddr	Adresse IP de l'adresse WINS secondaire.	Chaîne	n/a	D

Paramètre	Description	Type	Valeur (par défaut, min, max)	S/D[1]
send_file_api	Activation ou désactivation de l'API send file.	int	(1, 0, 1)	D
send_file_cache_size	Si la valeur de send_file_api est fixée à 1 et que la taille de lecture SMB requise est inférieure à la valeur de ce paramètre, send_file API met le fichier dans le cache. La valeur par défaut est zéro. En d'autres termes, send_file API ne met pas le fichier dans le cache.	int	(0, 0, 4194304)	D
send_file_size	Si la valeur de send_file_api est fixée à 1 et que la taille de lecture SMB requise est supérieure à la valeur de ce paramètre, send_file API est utilisé avec SMB.	int	(4096, 1, 4194304)	D
servername	Nom du serveur.	Chaîne	n/a	S
umask	AIX umask.	octal	(022, 0, 0777)	D

Remarque :

1. S signifie statique et D dynamique. Toute modification des paramètres statiques nécessite l'arrêt puis le redémarrage du serveur afin que ces changements soient pris en compte.
2. Pour maxusers, maxconnections, maxopens et maxsearches, une valeur minimum ou par défaut de zéro signifie illimité (sans restrictions).

Configuration du partage d'imprimantes et de fichiers

Il existe deux types de partages pouvant être configurés par Fast Connect : le partage de fichiers et le partage d'imprimantes. Lors du premier démarrage du serveur, un partage de fichiers avec netname `HOME` est créé et chargé par défaut. L'administrateur peut ajouter d'autres partages de fichiers ou d'imprimantes à l'aide de Web-based System Manager, du SMIT ou de la commande **net**.

Remarque : Les partages par défaut HOME, IBMLAN$ et ADMIN$ ne peuvent être ni changés ni supprimés.

Configuration utilisateur

Les comptes utilisateur peuvent être configurés sur le serveur à l'aide de Web-based System Manager, du SMIT ou de la commande **net**. Chaque utilisateur Fast Connect défini doit l'être également dans AIX. Fast Connect prend en charge l'authentification du niveau utilisateur à l'aide de mots de passe (texte en clair). L'accès aux ressources est autorisé sur la base des droits d'accès de l'utilisateur AIX authentifié.

L'accès "invité" est contrôlé à l'aide des paramètres de configuration **guest** et **guestname**. Si ces paramètres sont activés, Fast Connect permet l'accès d'un invité aux ressources réseau lorsque l'ID utilisateur reçue dans la configuration de la session serveur ne correspond à aucun des utilisateurs définis sur le serveur et diffère également de la valeur du paramètre **guestname** configuré sur le serveur.

Remarque : Si **encrypt_passwords** est assorti de la valeur 0, le mot de passe utilisateur ne peut pas comporter à la fois des majuscules et des minuscules. Si **encrypt_passwords** est assorti de la valeur 1 ou 2, ajoutez des noms d'utilisateur à la base de données utilisateurs de Fast Connect à l'aide de Web-based System Manager, du SMIT ou de la commande **net**. La base de données utilisateurs de Fast Connect est un sous–ensemble de la base de données utilisateurs AIX.

Configuration d'interfaces réseau

Fast Connect répond aux exigences du protocole SMB stipulant l'utilisation du protocole NetBIOS over TCP/IP, telles qu'énoncées dans les normes IETF RFC1001 et RFC1002. Il utilise toutes les interfaces réseau définies et opérationnelles pour AIX TCP/IP.

Configuration initiale

Sur un serveur Fast Connect nouvellement installé, les paramètres de configuration initiale sont les suivants :

Server Name — Nom d'hôte TCP/IP du serveur.

Server Description — Serveur Fast Connect sur *hostname*

Default Shares (Partages par défaut)

`HOME`, avec les attributs suivants :

- Network Name — HOME
- AIX directory — Répertoire initial de l'utilisateur tel que défini dans le profil utilisateur.

Les autres paramètres du serveur sont définis par défaut.

AIX Fast Connect pour Windows Administration

Vous pouvez utiliser Web-based System Manager, le SMIT ou la commande **net** pour gérer et administrer le serveur Fast Connect. Ces tâches se répartissent en trois catégories : contrôle du serveur, modification de sa configuration et collecte d'informations sur ce serveur.

Administration de AIX Fast Connect pour Windows		
Web-based System Manager: raccourci **wsm pc** (application services PC) –OU–		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Démarrage du serveur	**smit smbadminstart**	**net start**
Arrêt du serveur	**smit smbadminstop**	**net stop**
Mise en pause du serveur	—	**net pause**
Remise en marche du serveur	—	**net resume**
Modification des paramètres	**smit smbcfghatt**	**net config**
Modification des ressources	**smit smbcfgresi**	**net config**
Ajout d'utilisateurs	**smit smbcfgusradd**	**net user**
Modification des utilisateurs	**smit smbchgusrlis**	**net user**
Modification du mot de passe utilisateur	**smit smbusrpwd**	**net user**
Retrait d'un utilisateur	**smit smbrmusrlis**	**net user**
Configuration de nbns	**smit smbwcfgn**	—
Adjonction d'un nom NetBIOS	**smit smbwcfgadd**	**net nbaddname** ou **net nbaddgroup** ou **net nbaddmulti**
Suppression d'un nom NetBIOS	**smit smbwcfgdel**	**net nbdelname**
Suppression d'un nom NetBIOS (nom et adresse)	**smit smbwcfdadd**	**net nbdeladdr**
Sauvegarde d'une table de noms NetBIOS	**smit smbwcfgbak**	**net nbbackup**
Restauration d'une table de noms NetBIOS	**smit smbwcfgres**	**net nbrestore**
Liste de tous les partages	**smit smbsrvlisall**	**net share**
Liste de tous les partages de fichiers	**smit smbsrvfilist**	**net share**
Ajout d'un partage de fichiers	**smit smbsrvfiladd**	**net share**
Modification d'un partage de fichiers	**smit smbsrvfilchg**	**net share**
Suppression d'un partage de fichiers	**smit smbsrvfilrm**	**net share**

Administration de AIX Fast Connect pour Windows		
Ajout d'un partage d'imprimantes	**smit smbsrvprtadd**	**net share**
Modification d'un partage d'imprimantes	**smit smbsrvprchg**	**net share**
Suppression d'un partage d'imprimantes	**smit ssrvprtrm**	**net share**
Affichage de l'état du serveur	**smit smbadminstatu**	**net status**
Affichage de la configuration	**smit smbcfg**	**net config**
Affichage de statistiques	**smit smbadminstats**	**net statistics**
Affichage des partages	**smit smbsrvlisall**	**net share**
Aide	**smit**, puis sélectionnez Aide	**net help**

Mappage de noms de fichiers AIX longs vers des noms de fichiers DOS

Les systèmes d'exploitation PC plus anciens, tels que Windows for Workgroups 3.11, ne prennent pas en charge les noms de fichiers longs. Cette restriction requiert le mappage des noms de fichiers AIX longs vers des noms de fichiers DOS. Dans la plupart des cas, tronquer le nom ne suffit pas car de nombreux noms de fichiers sont mappés de manière identique si les 8 premiers caractères sont les mêmes. En outre, cette fonction est utilisée pour bon nombre d'applications (16 bits) plus anciennes fonctionnant avec Windows 95, Windows 98 et Windows NT.

Fast Connect mappe les noms de fichiers AIX (AFN) vers les noms de fichiers DOS (DFN) tout en veillant à affecter des noms de fichiers uniques. Il procède à cette opération en utilisant la méthode de mappage de noms de Microsoft Windows NT. En d'autres termes, les conflits de noms sont gérés en utilisant un caractère de délimitation suivi d'un chiffre unique pour que le nom le soit aussi).

Fast Connect génère un nom mappé dans le cas où l'AFN doit être transmis à un client DOS.

Les DFN générés par Fast Connect ne sont pas repris lors des redémarrages du serveur. Toutefois, les mappages demeurent cohérents pendant toute la durée de vie du serveur Fast Connect.

Il prend en charge les recherches efficaces de DFN et d'AFN donnés.

Fast Connect est doté d'une option de configuration pour désactiver le mappage. Lors de sa désactivation, les noms longs sont simplement tronqués dans le respect de la méthode d'affectation des noms de fichiers DOS.

Le caractère de délimitation utilisé est également configurable.

Remarque : Le mappage AFN vers DFN ne se déroulera pas correctement si le serveur est réamorcé. A titre d'exemple, prenez deux fichiers du répertoire racine d'un partage SMB exporté : `LongFileName1.txt` et `LongFileName2.txt`. Supposez qu'un client Windows 3.11 monte ce partage et fasse une recherche dans ce répertoire. Le résultat de la recherche est le suivant :

`LONGFI~1.TXT` pour `LongFileName1.txt`

`LONGFI~2.TXT` pour `LongFileName2.txt`

L'utilisateur humain de ce client note ce nom de fichier (`LONGFI~1.TXT`) et l'ouvre pour le modifier. Les modifications sont enregistrées dans ce fichier. Puis, le serveur s'arrête. Quelqu'un retire ensuite `LongFileName1.txt` du système des fichiers serveur. Une fois le fonctionnement du serveur rétabli, l'utilisateur du client modifie à nouveau `LONGFI~1.TXT`. Cette fois–ci ce nom 8,3 mappe vers `LongFileName2.txt`, et pas vers le nom de fichier préalablement supprimé ! Par conséquent, le client se retrouve à modifier le mauvais fichier. C'est pourquoi, si l'unité réseau est reconnectée après réamorçage du serveur, il faut récupérer de nouvelles listes de fichiers avant d'accéder aux noms mappés.

Connexion de clients PC à AIX Fast Connect pour Windows

Les étapes reprises dans les sections suivantes sont nécessaires à la connexion d'un client PC au serveur Fast Connect.

Configuration TCP/IP

Pour accéder au serveur Fast Connect, chaque client PC doit être configuré pour NetBIOS over TCP/IP (RFC1001/1002). Pour ce faire, consultez les sections suivantes.

Clients Windows 95, Windows 98

1. A partir du bouton Start (Démarrer), sélectionnez **Settings (Paramètres)–>Control_Panel (Panneau de configuration)–>Network (Réseau)**.
2. Sur l'écran de configuration comportant des onglets (affiché au départ), vérifiez l'existence des entrée suivantes :
   - Entrée pour la carte réseau (pilote matériel)
   - TCP/IP (protocole)
   - Client for Microsoft Networks (client)

   Récupérez toute entrée manquante à partir des disquettes Windows 95.
3. Cliquez sur l'entrée TCP/IP, puis sélectionnez Propriétés. La boîte de dialogue Propriétés TCP/IP a plusieurs onglets. Vérifiez les éléments suivants :

Adresse IP	Configurez comme il convient. (Pour le premier test, il peut vous sembler préférable de spécifier manuellement des adresses IP uniques pour chaque PC).
Onglet Liens	Sélectionnez Client for Microsoft Networks.

   En outre, vous pouvez activer la prise en charge WINS, DNS et/ou GATEWAY pour chaque client. Si tel est le cas, configurez chaque option comme il convient.
4. TESTEZ la configuration TCP/IP du client par interrogation (**ping**) des adresses IP à partir de l'invite DOS du client PC vers le serveur Fast Connect et vice versa.

Clients Windows NT

Remarque : vous devez vous connecter comme administrateur.

1. A partir du bouton Start (Démarrer), sélectionnez **Settings (Paramètres)–>Control_Panel (Panneau de configuration)–>Network (Réseau)**.
2. Au niveau de l'onglet Services, vérifiez l'existence d'entrées pour les services suivantes :
   - Navigateur de l'ordinateur
   - Interface NetBIOS
   - Station de travail

   Récupérez toute entrée manquante à partir du CD Windows NT.
3. Au niveau de l'onglet Protocoles, ajoutez TCP/IP (si cette option est manquante), puis sélectionnez Propriétés.

   La boîte de dialogue Propriétés TCP/IP a plusieurs onglets. Vérifiez les éléments suivants :

Adresse IP	Configurez comme il convient. (Pour le premier test, il peut vous sembler préférable de spécifier manuellement des adresses IP uniques pour chaque PC).

Il se peut que vous vouliez également configurer DNS, l'adresse WINS et le routage.

4. Testez la configuration TCP/IP du client par interrogation (**ping**) des adresses adresse IP à partir de l'invite DOS du client PC vers le serveur Fast Connect et vice versa.

Clients Windows For Workgroups (Windows 3.11)

1. A partir du groupe Réseau (au sein du Gestionnaire de programmes), lancez l'option Network Setup (Configuration du réseau).
2. Vérifiez l'existence des éléments suivants :
   - Microsoft Windows Network (version 3.11) (réseau)
   - Entrée de carte d'adaptateur LAN (pilote d'unité)
   - Microsoft TCP/IP–32 3.11b (protocole)

   Il se peut que vous deviez installer le protocole TCP/IP. TCP/IP n'est pas inclus dans le support d'installation de Windows 3.11. Vous pouvez télécharger une copie de Microsoft TCP/IP–32 3.11b à partir du site web de Microsoft **www.microsoft.com**.)

   Pour configurer TCP/IP, cliquez deux fois sur Microsoft TCP/IP–32 3.11b. Configurez l'adresse IP, le masque de sous–réseau, la passerelle par défaut, le(s) serveur(s) WINS), DNS ainsi que d'autres options, si nécessaire. (l'activation de **LMHOSTS** et DNS sont des options avancées).
3. Testez la configuration TCP/IP du client par interrogation (**ping**) des adresses IP à partir de l'invite DOS du client PC vers le serveur Fast Connect et vice versa.

Clients OS/2

1. Installez la prise en charge TCP/IP et NetBIOS au cours de l'installation de OS/2.
2. Utilisez le programme Configuration de TCP/IP pour vérifier et configurer TCP/IP.
3. Utilisez le programme MPTS (Multi–Protocol Transport Services) afin de vérifier et de configurer les protocoles suivants pour l'adaptateur réseau :
   - IBM OS/2 TCP/IP
   - IBM OS/2 NetBIOS OVER TCP/IP

   Ces protocoles doivent avoir le même numéro d'adaptateur LAN qui doit correspondre à l'interface TCP/IP.

   Remarque : l'installation par défaut est `IBM OS/2 NetBIOS`. Ajoutez `IBM OS/2 NetBIOS OVER TCP/IP` s'il n'est pas encore répertorié).
4. Testez la configuration TCP/IP du client par interrogation (**ping**) des adresses IP à partir de l'invite DOS du client PC vers le serveur Fast Connect et vice versa.

Fonction d'administration et d'authentification de l'utilisateur

Prise en charge des méthodes d'authentification de l'utilisateur ci–dessous :

- Authentification de l'utilisateur basée sur AIX à l'aide de mots de passe CIFS (texte en clair).
- Protocole de chiffrement du mot de passe CIFS LM (LAN Manager)
- Authentification de transit du domaine NT

La fonction d'administration de l'utilisateur dépend de la méthode d'authentification sélectionnée par l'administrateur Fast Connect. Chaque type a ses avantages et ses inconvénients. La méthode que vous choisissez dépend de votre environnement, de votre politique d'administration et du type le plus simple à administrer et à utiliser, selon vos critères.

Authentification utilisateur basée sur AIX

Cette méthode d'authentification basée sur AIX AIX utilise les définitions et les mots de passe utilisateur. Une fois configurée, la session Fast Connect récupère les autorisations d'accès utilisateur AIX validées (UID, GID et groupes secondaires).

Caractéristiques

1. Les clients doivent pouvoir négocier des mots de passe avec texte en clair. Cela peut passer par l'activation des mots de passe avec texte en clair et la mise à jour des entrées de registre requises pour clients Windows NT, 95 et 98.
2. Fast Connect doit être activé pour utiliser des mots de passe avec texte en clair à l'aide du SMIT, de Web-based System Manager ou de la commande **net**.

Avantages

1. Réduction du temps de gestion administrative du système (utilisation des informations utilisateur AIX existantes).
2. Possibilité d'utilisation d'outils AIX de gestion des utilisateurs.

Désavantages

1. Une mise à jour des registres Windows peut s'avérer nécessaire.
2. Windows peut demander une nouvelle saisie des mots de passe et de l'ID utilisateur.
3. Les mots de passe avec texte en clair sont acheminés sur le réseau.

Protocole de chiffrement de mots de passe CIFS LM (LAN Manager)

La méthode de protocole CIFS LM utilise des définitions utilisateur Fast Connect et des mots de passe à chiffrement aux fins d'authentification de l'utilisateur. Celui–ci doit également être défini comme utilisateur AIX et partager le même nom. Fast Connect procède au chiffrement des mots de passe et les sauvegarde dans ses fichiers pour les utiliser lors de la configuration de la session. Une fois configurée, la session Fast Connect récupère les autorisations d'accès utilisateur validées (UID, GID et groupes secondaires).

Caractéristiques

1. Les utilisateurs doivent être définis dans Fast Connect à l'aide du SMIT, de Web-based System Manager ou de la commande **net**.
2. AIX Fast Connect pour Windows doit être activé pour les mots de passe à chiffrement à l'aide du SMIT, de Web-based System Manager ou de la commande **net**.
3. Les mots de passe de connexion utilisateur Windows ou OS/2 doivent être les mêmes que ceux de Fast Connect. Ces mots de passe ne sont pas nécessairement identiques au mot de passe de connexion à AIX.
4. Vous devez être utilisateur racine (root) pour pouvoir modifier les mots de passe.

Avantages

1. Vous n'avez besoin d'aucune autre connexion en dehors de celle qui a été établie avec la station de travail Windows ou OS/2.
2. Les mots de passe avec texte en clair ne sont pas acheminés sur le réseau, ce qui offre une sécurité accrue.

Désavantages

1. La charge administrative est plus importante pour les utilisateurs Fast Connect.
2. L'administrateur doit intervenir pour la mise à jour des mots de passe.

Authentification de transit des domaines NT

Cette méthode d'authentification utilise des définitions utilisateur AIX ainsi qu'une authentification utilisateur au niveau de NT Server. Chaque utilisateur doit également être défini comme utilisateur AIX. La fonction d'authentification de transit est activée à l'aide du SMIT, de Web-based System Manager ou de la commande **net** en indiquant l'authentification de transit *NTserver IPaddress*.

Lors de la configuration de la session, Fast Connect transmet la demande de configuration de session au serveur NT. Si ce serveur authentifie l'utilisateur, Fast Connect autorise l'accès. Une fois configurée, la session Fast Connect récupère les autorisations d'accès utilisateur validées (UID, GID et groupes secondaires).

Caractéristiques

1. L'utilisateur doit être défini sur le serveur d'authentification de transit.
2. AIX Fast Connect pour Windows doit être activé aux fins d'authentification de transit à l'aide du SMIT, de Web-based System Manager ou de la commande **net** pour définir l'adresse IP du serveur NT.
3. Le nom d'utilisateur NT doit correspondre au nom d'utilisateur AIX, bien que les mots de passe puissent différer.

Avantages

1. Vous n'avez besoin d'aucune autre connexion en dehors de celle qui a été établie avec la station de travail Windows ou OS/2.
2. Les mots de passe avec texte en clair ne sont pas acheminés sur le réseau, ce qui offre une sécurité accrue.
3. L'utilisation de la définition utilisateur NT réduit le temps de gestion administrative nécessaire.

Désavantages

1. Nécessité d'un serveur NT.

NetBIOS Name Service (NBNS)

NetBIOS Name Service (NBNS) for AIX Fast Connect pour Windows offre des services de résolution de noms. Il prend également en charge certaines fonctions de Windows Internet Name Service (WINS), telles que l'enregistrement de noms multihomed et de noms de groupe Internet.

Pour activer NBNS, 'nbns' dans le fichier **cifsConfig** doit être assorti de la valeur `1` (valeur par défaut), puis redémarrez le serveur Fast Connect.

Pour désactiver NBNS, entrez `nbns = 0` dans le fichier **cifsConfig**.

Administration des tâches NBNS		
Tâche	*Raccourci SMIT*	*Commande ou fichier*
Liste de noms dans la table de noms NetBIOS	**smit smb**	**net nblistnames**
Ajout d'un nom NetBIOS	**smit smb**	**et nbaddname /name:*NetBIOS Name* /ipaddress:*ip address* [/subcode:*00–ff*]***
Suppression d'un nom NetBIOS dans la table correspondante	**smit smb**	**net nbdelname /name:*NetBIOS Name* [/subcode:*00–ff*]**
Suppression de l'adresse et du nom	**smit smb**	**net nbdeladdr /name:*NetBIOS Name* /ipaddress:*ipaddress****

Administration des tâches NBNS		
Sauvegarde de la table de noms NetBIOS dans un fichier	**smit smb**	**net nbbackup [/file:*file name*]**
Restauration d'une table de noms NetBIOS à partir d'un fichier de sauvegarde	**smit smb**	**net nbrestore [/file:*file name*]**

Remarque : La valeur de *ip address* peut être un chiffre dans la gamme d'adresses IP.

Groupes de travail, domaines et comptes utilisateur

Dans un souci de simplification, les clients PC devraient se trouver dans le même groupe de travail Windows ou domaine NT que le serveur Fast (ou vice versa). Windows 3.11, Windows 95, Windows NT utilisent tous `WORKGROUP` comme nom de groupe de travail par défaut. Le serveur Fast Connect s'initialise également pour utiliser `WORKGROUP`. Si votre réseau utilise l'authentification de connexion au domaine NT, vous pouvez configurer le serveur Fast Connect afin qu'il vérifie son accès via les serveurs d'authentification de domaine NT.

Que vous utilisiez des groupes de travail ou des domaines NT, l'accès à Fast Connect est géré par la sécurité utilisateur. Vous devez configurer les comptes utilisateur AIX pour chaque utilisateur Windows accédant à Fast Connect. C'est de loin le plus simple, si les comptes utilisateur (et mots de passe) sur AIX correspondent aux comptes client (et mots de passe) Windows ou domaine NT.

- Sur le serveur Fast Connect, utilisez le raccourci SMIT :

  ```
  smit smbcfghatt
  ```

  Pour utiliser Workgroups, entrez le nom du groupe de travail dans le champ Nom de domaine.

  Pour utiliser la validation de domaine NT, entrez les adresses IP pour le(s) serveur(s) d'authentification de ce domaine dans les champs Passthrough Authentication Server (Serveur d'authentification de transit) et Backup Passthrough Authentication Server (Serveur secondaire d'authentification de transit).

- Sur les clients PC fonctionnant avec Windows 95 ou Windows 98, sélectionnez le **bouton Start (Démarrer) –> Settings (Paramètres) –> Control_Panel (Panneau de configuration) –> Network (Réseau)**. Sur l'écran d'identification, entrez le nom de votre PC.

  Pour utiliser Workgroups, entrez le nom du groupe de travail dans le champ Workgroup.

  Pour utiliser la validation de domaine NT, allez dans l'onglet Configuration, sélectionnez Client for Microsoft Networks (Clients pour réseaux Microsoft), puis cliquez sur Propriétés. Cochez la case Domaine NT, puis entrez le nom de celui–ci.

- Sur les clients PC fonctionnant avec Windows NT, assurez–vous que vous êtes connecté comme Administrateur. Puis :

  a. Sélectionnez le **bouton Start (Démarrer) –> Settings (Paramètres) –> Control_Panel (Panneau de configuration) –> Network (Réseau)**.

  b. Sur l'écran d'identification, sélectionnez le bouton **Change... (Modifier)** .

  c. Entrez le nom de ce PC.

  d. Entrez le groupe de travail ou le nom de domaine, comme il convient.

- Sur les clients PC fonctionnant avec Windows for Workgroups, la configuration du groupe de travail intervient au cours de l'installation et de la configuration de Windows 3.11, mais peut être modifiée dans le fichier **SYSTEM.INI**, si nécessaire.

- Sur les clients PC fonctionnant avec OS/2, la configuration du groupe de travail intervient lors de l'installation d'OS/2, mais peut être modifiée dans le paramètre DOMAIN de **IBMLAN.INI**, si nécessaire.

Remarque : utilisez la commande OS/2 **LOGON** pour utiliser les services NetBIOS, tels que la navigation sur le réseau, NET VIEW et NET USE.

Utilisation de mots de passe (texte en clair) avec Windows 98 ou Windows NT 4.0 (Service Pack 3)

Pour des raisons de sécurité, Microsoft a désactivé la prise en charge de mots de passe réseau sans chiffrement (texte en clair) dans Windows 98 et Windows NT 4.0 (livré avec Service Pack 3). Pour utiliser des mots de passe avec texte en clair sur votre réseau, ces clients doivent être mis à niveau avec les options de registre suivantes.

Pour installer l'option Enable Plain Text Passwords (Activation des mots de passe avec texte en clair) de Windows 98, procédez comme suit :

1. Utilisez **EDIT** ou le BLOC–NOTES pour créer le fichier de texte suivant **W98plain.reg**, comme un fichier local sur la machine Windows 98 :

```
REGEDIT4

; Registry file to allow plaintext passwords on Windows 98

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP]
"EnablePlainTextPassword"=dword:00000001
```

2. A l'aide de l'Explorateur Windows, cliquez deux fois sur le nom de fichier **W98plain.reg** dans le répertoire dans lequel vous l'avez sauvegardé. Cette opération met à jour le registre Windows de ce client permettant la saisie de mots de passe avec texte en clair.
3. Arrêtez et réamorcez la machine Windows 98. (l'arrêt et le redémarrage du système est nécessaire pour que cette option soit prise en compte).

Pour installer l'option Enable Plain Text Passwords (Activation des mots de passe avec texte en clair) de Windows NT 4.0, procédez comme suit :

1. Utilisez **EDIT** ou le BLOC–NOTES pour créer le fichier de texte suivant **NT4plain.reg**, comme un fichier local sur la machine Windows NT :

```
REGEDIT4

; Registry file to allow plaintext passwords on Windows NT 4.0, SP3

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters]
EnablePlainTextPassword=dword:00000001
```

2. A l'aide de l'Explorateur Windows, cliquez deux fois sur le nom de fichier **NT4plain.reg** dans le répertoire dans lequel vous l'avez sauvegardé. Cette opération met à jour le registre Windows de ce client permettant la saisie de mots de passe avec texte en clair.
3. Arrêtez et redémarrez la machine Windows NT. (l'arrêt et le redémarrage du système est nécessaire pour que cette option soit prise en compte).

Remarque : Même avec l'option précédente installée, tous les clients Windows NT 4.0 demandent à l'utilisateur la saisie de son mot de passe la première fois qu'il se connecte au serveur Fast Connect (en utilisant l'option de navigation, en mappant les unités, etc.). Une fois connecté, d'autres opérations de navigation ou de mappage d'unités peuvent intervenir sans aucun problème. L'affichage du message **Password Invalid** (mot de passe non valable) au tout début s'explique par le fait que Windows NT 4.0 essaie d'utiliser des mots de passe à chiffrement pour se connecter à Fast Connect, au lieu de mots de passe avec texte en clair.

Navigation sur le réseau

AIX Fast Connect pour Windows prend en charge des opérations de navigation, telles que Network Neighborhood et NET VIEW. Ces opérations présentent à l'utilisateur une liste de partages de fichiers et d'imprimantes exportée pour chaque serveur.

Network Neighborhood peut également être utilisé comme mode de mappage des unités. (Cliquez sur un nom de partage de fichiers à l'aide du bouton droit de la souris, puis sélectionnez Map Network Drive (Mapper unité réseau) dans le menu déroulant).

Toutefois, tenez compte des limitations suivantes quant à la navigation sur le réseau :

- Pour visualiser le serveur Fast Connect dans Network Neighborhood, un client PC doit pouvoir visualiser le Master Brower (Navigateur principal) pour le groupe de travail ou le domaine pour lequel le serveur Fast Connect est configuré. (Fast Connect ne fonctionne pas comme un navigateur principal, mais les clients Windows 95, Windows 98 ou Windows NT de ce groupe de travail/domaine peuvent jouer ce rôle).

  La navigation réseau fonctionne généralement mieux si le client PC et le serveur Fast Connect sont dans le même groupe de travail/domaine.

- La base de données de liste de navigation gérée par le Master Browser n'est pas toujours à jour. La liste peut afficher des noms de serveurs Fast Connect qui sont actuellement en panne, ne fonctionnent pas, sont physiquement déconnectés voire inaccessibles. Le Master Browser ne supprime pas un serveur de la liste de navigation tant que le délai de rafraîchissement de ce nom de serveur n'a pas expiré (ce qui peut prendre plusieurs jours). Si un utilisateur essaie tout de même d'accéder à ce nom de serveur (en navigant au sein des noms de partages, en mappant des unités, etc.), un serveur Fast Connect déconnecté sera identifié comme inaccessible.

Mappage d'unités

Normalement, les clients PC doivent définir des mappages d'unités pour utiliser les partages de fichiers Fast Connect exportés. Ces mappages peuvent se faire à partir de l'invite DOS ou Windows.

Vous pouvez utiliser les mécanismes suivants pour définir ou non des mappages entre des lettres d'unité PC et des partages de fichiers Fast Connect. Pour les besoins des exemples suivants, supposons que le nom de serveur NetBIOS est `cifs01` et que les partages de fichiers `apps` et `pcdata` sont définis.

A partir de DOS :

```
DOS> net help                        (help info for DOS)
DOS> net use H: \\cifs01\home      (pre-defined Fast Connect share)
DOS> net use F: \\cifs01\apps
DOS> copy F:\oldfile H:\newfile    (uses previous drive-mappings)
DOS> net use F: /delete            (delete the drive-mapping)
```

A partir de Windows :

1. Accédez à la boîte de dialogue Map Network Drive (Mappage d'unité réseau).
   - Sélectionnez **Windows Explorer –> Tools (Outils) –> Map Network Drive (Mapper unité réseau)**.

     ou

   - Cliquez sur Network Neighborhood à l'aide du bouton droit de la souris et sélectionnez **Map Network Drive (Mapper unité réseau)**.
2. Sélectionnez l'unité souhaitée (par exemple, F:) à partir de la liste déroulante Unités, puis
   - utilisez le chemin d'accès suivant : (par exemple, `\\cifs01\apps`).

     ou

– utilisez les Shared Directories (Répertoires partagés) pour sélectionner le partage de réseau souhaité.

Utilisation d'imprimantes Fast Connect

Pour l'impression, les mappages DOS et Windows diffèrent quelque peu. Pour les besoins des exemples suivants, supposons que le serveur Fast Connect `cifs01` a défini les partages d'imprimantes `netprint1` et `pscolor`.

Pour les applications DOS, il est possible d'utiliser les mappages d'unité simples présentés ci–dessous :

```
DOS> net use LPT1: \\cifs01\netprint1
DOS> net use LPT2: \\cifs01\pscolor
```

Toutefois, pour la prise en charge de l'impression à partir d'applications Windows, il est nécessaire d'installer un pilote d'imprimante Windows et de le mapper vers l'imprimante réseau, comme suit :

1. Sélectionnez **Start (Démarrer) –> Settings (Paramètres) –> Printers (Imprimantes) –> Add Printer (Ajouter imprimante)**.
2. Sélectionnez l'option **Network Printer (Imprimante réseau)**.
3. Entrez le nom de partage d'imprimantes Fast Connect (par exemple, **cifs01****netprint1**) ou utilisez la liste de navigation pour sélectionner le partage d'imprimantes souhaité.
4. Sélectionnez le pilote d'imprimante Windows correspondant à cette imprimante réseau (par exemple, IBM 4039 imprimante laser PS), installé à partir des disquettes Windows.

Pour Windows 3.11, installez le pilote d'imprimante souhaité à partir du Panneau de configuration, puis utilisez le bouton Connecter... pour le mapper vers le partage d'imprimantes Fast Connect.

AIX Fast Connect pour Windows Identification des problèmes

Suivi

Le serveur Fast Connect est doté d'une fonction de création de fichiers de suivi AIX afin d'identifier les problèmes. Lorsque cette fonction est activée, les informations relatives aux événements sélectionnés sont consignées dans le fichier de suivi. Pour accéder à ces fichiers de suivi, la commande trace (suivi) doit être installée sur votre machine. Cette commande se trouve dans le module **bos.sysmgt.trace**.

Les suivis d'erreurs suivants sont utilisés par le serveur Fast Connect :

2EE	CIFS Enter
2EF	CIFS Exit
2F0	CIFS–FSS
2F1	CIFS–LOGON
2F2	CIFS–NET
2F3	CIFS–SMB PARSER
2F4	CIFS–PSS
2F5	CIFS–SMS

Les fichiers de suivi peuvent être créés en utilisant l'interface SMIT ou à partir de la ligne de commande.

A partir de la ligne de commande :

1. Entrez :

   ```
   trace -a -j 2EE,2EF,2F0,2F1,2F2,2F3,2F4,2F5 -o /tmp/cifs.trace
   ```

   Le fichier de suivi **cifs.trace** est créé dans le répertoire /**tmp**.
2. Recréez le problème.
3. Entrez :

   ```
   trcstop
   ```
4. Entrez :

   ```
   trcrpt -t /etc/trcfmt /tmp/cifs.trace
   ```

   La commande trcrpt formate le fichier de suivi en texte lisible et produit un rapport au format standard.

A partir de l'interface SMIT :

1. Entrez le raccourci SMIT :

   ```
   smit trcstart
   ```
2. Sélectionnez les suivis d'erreurs CIFS pour ID d'événement ADDITIONAL, puis quittez le SMIT. Le fichier de suivi **trcfile** est créé dans le répertoire (par défaut) /**var**/**adm**/**ras**.
3. Recréez le problème.
4. Entrez :

   ```
   smit trcstop
   ```

   puis quittez le SMIT.
5. Entrez :

   ```
   smit trcrpt
   ```

   puis sélectionnez le format de sortie. Le fichier de suivi s'affiche dans un format lisible.

Journaux

Le serveur Fast Connect consigne des messages d'information et d'erreur dans le fichier **cifsLog** dans /**var**/**cifs**.

Problèmes courants et solutions

Problèmes de connexion

Impossible de se connecter au serveur.

Vérifiez que la fonction passthrough_authentication_server est activée sur le serveur.

```
access is denied

password is invalid

password is not correct

not authorized to login
```

Lorsque l'un de ces messages d'erreur s'affiche sur le client PC, procédez comme suit :

- Entrez le mot de passe correct.
- Vérifiez l'ID de connexion utilisateur et son mot de passe sur les clients disposant normalement d'un compte sur le serveur AIX. Déconnectez–vous et reconnectez–vous sur les clients avec le mot de passe/ID utilisateur correct.
- Pour les clients avec Window NT et Service Pack 3, la commande NET VIEW affiche le message `access is denied`. Reportez–vous à la section Utilisation de Windows NT 4.0 avec le Service Pack 3, page 11-23 pour plus d'informations.

  Remarque : Fast Connect ne prend pas en charge les mots de passe comportant des lettres majuscules et minuscules.

```
System error 53 has occurred.

The network path was not found.
```

Lorsque ce message d'erreur s'affiche sur le client PC, procédez comme suit :

- Vérifiez le nom NetBIOS du serveur Fast Connect.
- Vérifiez l'état du serveur.
- Reportez–vous à la section Procédure de vérification de la connexion, page 11-27.

```
System error 51 has occurred.

The remote computer is not available.
```

Lorsque ce message d'erreur s'affiche sur le client PC, vérifiez l'état du serveur. Il se peut qu'il soit en pause.

Procédure de vérification de la connexion

1. Interrogez (**ping**) le serveur Fast Connect par adresse IP. En cas de dépassement de délai, vérifiez les éléments suivants :
   - le câble de connexion physique
   - l'état de la machine AIX
   - la configuration TCP/IP sur les clients et sur le serveur AIX

2. Interrogez (**ping**) le serveur Fast Connect avec son nom NetBIOS. En cas d'échec, reportez–vous à la section Résolution de noms NetBIOS, page 11-4 pour plus d'informations.
3. Vérifiez l'état du serveur sur la machine AIX à l'aide des commandes **net config**, **net status** et **net statistics**.

Index

Symboles

Nombres

A

B

C

D

E

F

G

I

L

M

N

S

T

U

V

W

X

Vos remarques sur ce document / Technical publication remark form

Titre / Title : AIX 4.3 Guide de gestion du système Communications et réseaux

Nº Reférence / Reference Nº : 86 F2 31JX 02

Daté / Dated : Octobre 1999

ERREURS DETECTEES / ERRORS IN PUBLICATION

AMELIORATIONS SUGGEREES / SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Vos remarques et suggestions seront examinées attentivement.
Si vous désirez une réponse écrite, veuillez indiquer ci-après votre adresse postale complète.

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please furnish your complete mailing address below.

NOM / NAME : _____ Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

Remettez cet imprimé à un responsable BULL ou envoyez-le directement à :

Please give this technical publication remark form to your BULL representative or mail to:

BULL ELECTRONICS ANGERS
CEDOC
34 Rue du Nid de Pie – BP 428
49004 ANGERS CEDEX 01
FRANCE

Technical Publications Ordering Form
Bon de Commande de Documents Techniques

To order additional publications, please fill up a copy of this form and send it via mail to:
Pour commander des documents techniques, remplissez une copie de ce formulaire et envoyez-la à :

BULL ELECTRONICS ANGERS
CEDOC
ATTN / MME DUMOULIN
34 Rue du Nid de Pie – BP 428
49004 ANGERS CEDEX 01
FRANCE

Managers / Gestionnaires :
Mrs. / Mme : **C. DUMOULIN** +33 (0) 2 41 73 76 65
Mr. / M : **L. CHERUBIN** +33 (0) 2 41 73 63 96

FAX : +33 (0) 2 41 73 60 19
E–Mail / Courrier Electronique : srv.Cedoc@franp.bull.fr

Or visit our web site at: / Ou visitez notre site web à:
`http://www-frec.bull.com` (PUBLICATIONS, Technical Literature, Ordering Form)

CEDOC Reference # Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
__ __ _____ _ [__]		__ __ _____ _ [__]		__ __ _____ _ [__]	
[__] : **no revision number means latest revision** / pas de numéro de révision signifie révision la plus récente					

NOM / NAME : _____ Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

TELEPHONE / PHONE : _____ FAX : _____

E–MAIL : _____

For Bull Subsidiaries / Pour les Filiales Bull :
Identification: _____

For Bull Affiliated Customers / Pour les Clients Affiliés Bull :
Customer Code / Code Client : _____

For Bull Internal Customers / Pour les Clients Internes Bull :
Budgetary Section / Section Budgétaire : _____

For Others / Pour les Autres :
Please ask your Bull representative. / Merci de demander à votre contact Bull.

PLACE BAR CODE IN LOWER LEFT CORNER

BULL ELECTRONICS ANGERS
CEDOC
34 Rue du Nid de Pie – BP 428
49004 ANGERS CEDEX 01
FRANCE

REFERENCE
86 F2 31JX 02

Bull

Utiliser les marques de découpe pour obtenir les étiquettes.
Use the cut marks to get the labels.

AIX 4.3
Guide de gestion
du système

Communications
et réseaux

86 F2 31JX 02

AIX 4.3
Guide de gestion
du système

Communications
et réseaux

86 F2 31JX 02

AIX 4.3
Guide de gestion
du système

Communications
et réseaux

86 F2 31JX 02