Gestion de réseaux série à l'aide d'UUCP et de PPP dans Oracle® Solaris 11.2

Référence: E53884
Juillet 2014

ORACLE®

Table des matières

Utilisation de la présente documentation

- **Présentation** : décrit la procédure à effectuer pour activer les services PPP et UUCP pour assurer la mise en réseau série.
- **Public visé** : administrateurs système.
- **Connaissances requises** : Compétences de base et avancées en matière d'administration.

Bibliothèque de documentation du produit

Les informations de dernière minute et les problèmes connus pour ce produit sont inclus dans la bibliothèque de documentation accessible à l'adresse http://www.oracle.com/pls/topic/lookup?ctx=E36784.

Accès aux services de support Oracle

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

Commentaires en retour

Faites part de vos commentaires sur cette documentation à la page suivante : http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPITRE 1

A propos du protocole Solaris Point-to-Point 4.0

Cette section est consacrée à la mise en réseau série. La mise en réseau série fait référence à l'utilisation d'une interface série (un port RS-232 ou V.35, par exemple) pour relier deux ordinateurs ou plus dans le cadre du transfert de données. Contrairement aux interfaces LAN, telles qu'Ethernet, ces interfaces série permettent de connecter des systèmes très éloignés. Pour mettre en oeuvre la mise en réseau série, vous disposez des technologies PPP (Point-to-Point Protocol) et UUCP (UNIX-to-UNIX CoPy). Lorsqu'une interface série est configurée pour la mise en réseau, elle devient disponible à plusieurs utilisateurs, tout comme n'importe quelle autre interface réseau, notamment Ethernet.

Ce chapitre présente Solaris PPP 4.0. Cette version de PPP permet à deux ordinateurs situés à différents emplacements physiques de communiquer en utilisant PPP sur une large gamme de médias. Solaris PPP 4.0 est inclus dans l'installation de base.

Il aborde les sujets suivants :

Notions de base de Solaris PPP 4.0

Solaris PPP 4.0 met en oeuvre le protocole de liaison de données PPP (Point-to-Point Protocol, protocole point à point) qui fait partie de la suite de protocoles TCP/IP. PPP décrit la façon dont les données sont transmises entre deux machines, au moyen de médias de communication tels que des lignes téléphoniques.

Depuis le début des années 1990, PPP est un standard Internet fréquemment utilisé pour l'envoi de datagrammes par la biais d'une liaison de communication. Le standard PPP est décrit dans le document RFC 1661 par le groupe de travail du Protocole Point à Point de l'IETF (Internet Engineering Task Force). PPP est couramment utilisé lorsque des ordinateurs distants appellent un fournisseur de service Internet (FAI) ou un serveur d'entreprise configuré pour recevoir des appels entrants.

Solaris PPP 4.0 est basé sur l'ANU (Australian National University) PPP–2.4 public et met en oeuvre le standard PPP. Les liaisons PPP synchrones et asynchrones sont toutes deux prises en charge.

Compatibilité de Solaris PPP 4.0

Diverses versions du standard PPP sont disponibles et couramment utilisées par la communauté Internet. ANU PPP-2.4 est plébiscité pour Linux, Tru64 UNIX et les trois principales variantes de BSD :

- FreeBSD
- OpenBSD
- NetBSD

Solaris PPP 4.0 apporte les fonctions hautement configurables d'ANU PPP-2.4 aux machines qui exécutent le système d'exploitation Oracle Solaris. Les machines exécutant Solaris PPP 4.0 peuvent configurer facilement des liaisons PPP à toutes les machines exécutant une mise en oeuvre du standard PPP.

Parmi les implémentations PPP non basées sur l'ANU qui interopèrent avec Solaris PPP 4.0, citons :

- Solaris PPP, également appelée `asppp`, disponible avec les versions Solaris 2.4 à 8
- Solstice™ PPP 3.0.1
- Microsoft Windows 98 DUN
- Cisco IOS 12.0 (synchrone)

Quelle version de Solaris PPP utiliser

Solaris PPP 4.0 est l'implémentation PPP prise en charge. Les versions Solaris 9 et ultérieures n'incluent pas le logiciel Asynchronous Solaris PPP (`asppp`) antérieur. Pour plus d'informations, reportez-vous au Chapitre 9, Migration de Solaris PPP vers Solaris PPP 4.0 (tâches).

Pourquoi utiliser Solaris PPP 4.0 ?

Si vous utilisez actuellement `asppp`, envisagez de migrer vers Solaris PPP 4.0 . Notez les différences entre les deux technologies Solaris PPP :

- **Modes de transfert**

  `asppp` prend en charge les communications asynchrones uniquement. Solaris PPP 4.0 prend en charge les communications asynchrones et les communications synchrones.

- **Processus de configuration**

  La configuration de `asppp` nécessite la configuration du fichier de configuration `asppp.cf`, de trois fichiers UUCP et de la commande `ipadm`. En outre, vous devez préconfigurer les interfaces de tous les utilisateurs susceptibles de se connecter à une machine.

  La configuration de Solaris PPP 4.0 requiert de définir des options pour les fichiers de configuration PPP ou d'exécuter la commande `pppd` avec des options. Vous pouvez également utiliser à la fois le fichier de configuration et la ligne de commande. Solaris PPP crée et supprime des interfaces de manière dynamique. Il n'est pas nécessaire de configurer directement les interfaces PPP de chaque utilisateur.
- **Fonctionnalités de Solaris PPP 4.0 non disponibles à partir de asppp**
  - Authentification MS-CHAPv1 et MS-CHAPv2
  - PPPoE (PPP over Ethernet) pour la prise en charge des ponts ADSL
  - Authentification PAM
  - Modules de plug-in
  - Adressage IPv6
  - Compression de données utilisant l'algorithme BSD ou Deflate
  - Prise en charge de la fonction de rappel côté client de Microsoft

Chemin de mise à niveau de Solaris PPP 4.0

Si vous convertissez une configuration `asppp` en Solaris PPP 4.0, vous pouvez utiliser le script de conversion fourni avec cette version. La section “Conversion de `asppp` à Solaris PPP 4.0” à la page 157 contient les instructions complètes à ce sujet.

Sources d'informations sur PPP

De nombreuses ressources sur PPP sont disponibles en ligne et sous forme de documentation imprimée. Les sous-sections suivantes offrent quelques suggestions.

Ouvrages de référence professionnelle à propos de PPP

Pour plus d'informations sur les implémentations PPP courantes, notamment ANU PPP, reportez-vous aux ouvrages suivants :

- Carlson, James. *PPP Design, Implementation, and Debugging*. 2è éd. Addison-Wesley, 2000.
- Sun, Andrew. *Using and Managing PPP*. O'Reilly & Associates, 1999.

Documents RFC sur PPP

Voici quelques documents RFC utiles sur PPP :

- 1661 et 1662 décrivent les caractéristiques principales de PPP
- 1334 décrit les protocoles d'authentification, tels que PAP (Password Authentication Protocol) et CHAP (Challenge-Handshake Authentication Protocol)
- 1332 est un RFC international qui décrit PPPoE (PPP over Ethernet)

Pour obtenir des copies des RFC PPP, spécifiez le numéro du document sur la page Web IETF RFC http://www.ietf.org/rfc.html .

Pages de manuel sur PPP

Pour des détails techniques sur la mise en oeuvre de Solaris PPP 4.0, reportez-vous aux pages de manuel suivantes :

- `pppd`(1M)
- `chat`(1M)
- `pppstats`(1M)
- `pppoec`(1M)
- `pppoed`(1M)
- `sppptun`(1M)
- `snoop`(1M)

Consultez en outre la page de manuel de `pppdump`(1M). Vous trouverez les pages de manuel sur PPP à l'aide de la commande `man`.

Configurations et terminologie PPP

Cette section présente les configurations PPP. Elle définit également les termes utilisés dans ce guide.

Solaris PPP 4.0 prend en charge différentes configurations.

- Configurations commutées ou à accès *commuté*
- Configurations câblées ou de *ligne spécialisée*

FIGURE 1-1 Composants de la liaison PPP

La figure précédente illustre une liaison PPP de base. La liaison est constituée des composants suivants :

- Deux machines, situées habituellement à des emplacements physiques distincts, appelées *pairs*. Un pair peut être un ordinateur personnel, une station de travail d'ingénierie, un serveur de grande taille ou même un routeur commercial, selon les exigences du site.
- Interface série sur chaque pair. Sur des machines Oracle Solaris, cette interface peut être `cua`, `hihp` ou une autre interface, selon que vous configurez une liaison PPP synchrone ou asynchrone.
- Liaison physique, telle qu'un câble série, une connexion modem ou une ligne spécialisée d'un fournisseur réseau (ligne T1 ou T3, par exemple).

Présentation de la liaison commutée PPP

La configuration PPP la plus fréquente est la *liaison commutée*. Dans une liaison commutée, le pair local *appelle* le pair distant pour établir la connexion et exécuter PPP. Au cours du processus de commutation, le pair local compose le numéro de téléphone du pair distant afin d'initialiser la liaison.

Un ordinateur domestique qui appelle un pair situé chez un FAI, configuré pour recevoir des appels entrants, constitue un scénario de commutation courant. Un autre scénario est un site d'entreprise où une machine locale transmet des données via une liaison PPP à un pair situé dans un autre bâtiment.

Dans ce guide, le pair local qui initialise la connexion commutée est appelé la *machine d'appel sortant*. Le pair qui reçoit l'appel entrant est désigné comme le *serveur d'appel entrant*. Cette

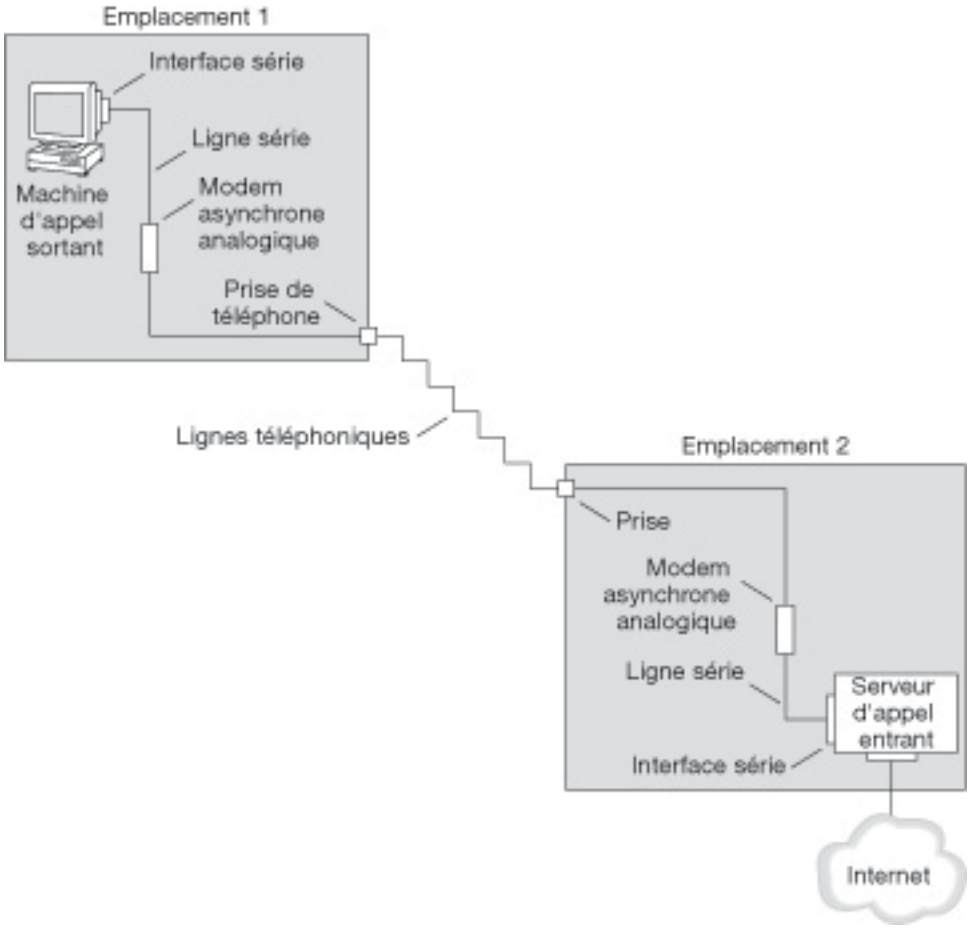
machine est en réalité le pair cible de la machine d'appel sortant et n'est pas nécessairement un vrai serveur.

PPP n'est pas un protocole client-serveur. Certains documents PPP emploient les termes "client" et "serveur" dans le contexte de l'établissement d'un appel téléphonique. Un serveur d'appel entrant n'est pas un vrai serveur, comme un serveur de fichiers ou un serveur de noms. Le terme "serveur d'appel entrant" est répandu parce que les machines d'appel entrant "servent" plusieurs machines d'appel sortant auxquelles elles offrent l'accès au réseau. Néanmoins, le serveur d'appel entrant représente le pair cible de la machine d'appel sortant.

Composants de la liaison PPP commutée

Reportez-vous au schéma ci-après.

FIGURE 1-2 Liaison PPP commutée analogique de base



La configuration de l'emplacement 1 (côté appel sortant de la liaison) se compose des éléments suivants :

- Machine d'appel sortant, généralement un ordinateur personnel ou une station de travail au domicile d'un utilisateur.
- Interface série sur la machine d'appel sortant. L'interface `/dev/cua/a` ou `/dev/cua/b` est l'interface série standard pour les appels sortants sur des machines exécutant le logiciel Oracle Solaris.
- Modem asynchrone ou adaptateur de terminal RNIS connecté à une prise téléphonique.
- Lignes et services téléphoniques d'un opérateur de téléphonie.

La configuration de l'emplacement 2 (côté appel entrant de la liaison) se compose des éléments suivants :

- Prise téléphonique (ou connecteur similaire) connectée au réseau téléphonique.
- Modem asynchrone ou adaptateur de terminal RNIS
- Interface série sur le serveur d'appel entrant, `ttya` ou `ttyb` pour les appels entrants
- Serveur d'appel entrant connecté à un réseau, tel qu'un intranet d'entreprise, ou dans le cas d'un FAI, Internet

Utilisation d'adaptateurs de terminal RNIS avec une machine d'appel sortant

Les adaptateurs de terminal RNIS externes sont plus rapides que les modems, mais ils se configurent plus ou moins de la même manière. La principale différence dans la configuration d'un adaptateur de terminal RNIS réside dans le script de discussion, qui requiert les commandes spécifiques du fabricant de l'adaptateur. La section “Script de discussion pour adaptateur de terminal RNIS externe” à la page 129 contient des informations sur les scripts de discussion pour les adaptateurs de terminal.

Description des communications commutées

Les fichiers de configuration PPP à la fois sur les pairs entrants et sortants contiennent les instructions pour la configuration de la liaison. Le processus suivant s'effectue lors de l'initialisation de la liaison commutée.

1. L'utilisateur ou le processus sur la machine d'appel sortant exécute la commande `pppd` pour démarrer la liaison.
2. La machine d'appel sortant lit les fichiers de configuration PPP. La machine d'appel sortant envoie ensuite des instructions via la ligne série à son modem, y compris le numéro de téléphone du serveur d'appel entrant.
3. Le modem compose le numéro de téléphone pour établir une connexion téléphonique avec le modem du serveur d'appel entrant.

   La série de chaînes de texte que la machine d'appel sortant envoie au modem et au serveur d'appel entrant est contenue dans un fichier appelé *script de discussion*. Si nécessaire, la machine d'appel sortant envoie des commandes au serveur d'appel entrant pour appeler PPP sur le serveur.
4. Le modem connecté au serveur d'appel entrant entame la négociation de liaison avec le modem connecté à la machine d'appel sortant.
5. A l'issue de la négociation entre les modems, le modem connecté à la machine d'appel sortant indique "CONNECT".
6. La liaison PPP sur les deux pairs entre dans la phase *Establish* où le protocole LCP (Link Control Protocol) négocie les paramètres de liaison de base et l'utilisation de l'authentification.

7. Si nécessaire, les pairs s'authentifient mutuellement.
8. Les NCP (Network Control Protocol) de PPP négocient l'utilisation de protocoles réseau, tels que IPv4 ou IPv6.

La machine d'appel sortant peut alors exécuter `telnet` ou une commande similaire au niveau d'un hôte accessible via le serveur d'appel entrant.

Présentation de la liaison PPP de ligne spécialisée

Une configuration PPP câblée de *ligne spécialisée* implique deux pairs reliés par le biais d'une liaison. Cette liaison constitue un service numérique commuté ou non commuté, loué auprès d'un fournisseur. Solaris PPP 4.0 fonctionne sur tous les supports de ligne spécialisée point à point et duplex intégral. En règle générale, une société loue une liaison câblée auprès d'un fournisseur réseau pour se connecter à un fournisseur d'accès Internet ou à un autre site distant.

Comparaison des liaisons commutées et des liaisons de ligne spécialisées

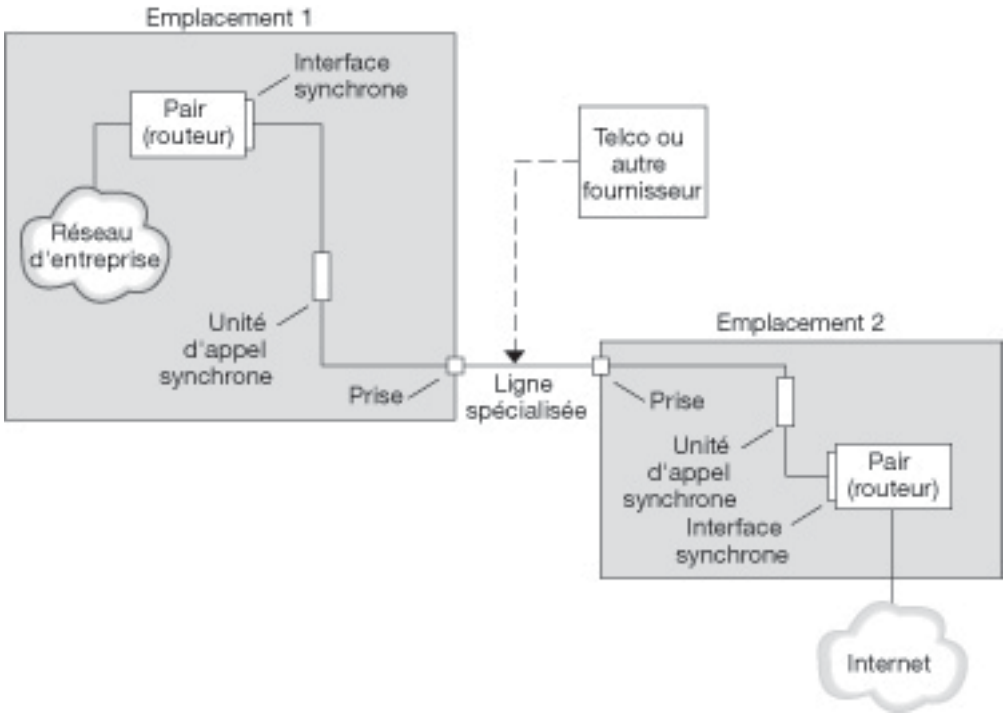
Les deux types de liaison, commutée et spécialisée, impliquent deux pairs connectés par un support de communication. Le tableau suivant récapitule les différences entre les types de liaison.

Ligne spécialisée	Ligne commutée
Toujours connectée, à moins qu'un administrateur système ou une coupure d'alimentation ne l'interrompe.	Lancée sur demande, lorsqu'un utilisateur tente d'appeler un pair distant.
Utilise les communications synchrones et asynchrones. Un modem longue distance est souvent utilisé pour les communications asynchrones.	Utilise les communications asynchrones.
Louée auprès d'un fournisseur.	Utilise des lignes téléphoniques existantes.
Requiert des unités synchrones.	Utilise des modems moins coûteux.
Nécessite des ports synchrones, courants sur la plupart des systèmes SPARC. Cependant, les ports synchrones ne sont pas fréquents sur les systèmes x86 et les systèmes SPARC plus récents.	Utilise les interfaces série standard incluses sur la plupart des ordinateurs.

Composants de la liaison PPP de ligne spécialisée

Reportez-vous au schéma ci-après.

FIGURE 1-3 Configuration de la ligne spécialisée de base



La liaison de ligne spécialisée est constituée des composants suivants :

- **Deux pairs**, chacun situé à l'une des extrémités de la liaison. Les pairs peuvent être une station de travail ou un serveur. Le pair fonctionne souvent comme un routeur entre son réseau, ou Internet, et le pair opposé.
- **Une interface synchrone sur chaque pair**. Certaines machines exécutant le logiciel Oracle Solaris exigent l'acquisition d'une carte d'interface synchrone, telle que HSI/P, pour la connexion à une ligne spécialisée. D'autres machines, comme les stations de travail UltraSPARC®, intègrent des interfaces synchrones.
- **Une unité numérique synchrone CSU/DSU sur chaque pair**, qui relie le port synchrone à la ligne spécialisée.

  En fonction de votre environnement linguistique, une CSU peut être intégrée à la DSU, être louée auprès d'un fournisseur ou vous appartenir. La DSU offre une interface série synchrone standard à la machine Oracle Solaris. Avec Frame Relay, le périphérique FRAD (Frame Relay Access Device) réalise l'adaptation de l'interface série.
- **Une ligne spécialisée**, offrant des services numériques commutés ou non commutés. C'est le cas de SONET/SDH, Frame Relay PVC et T1.

Description des communications de ligne spécialisée

Sur la plupart des types de lignes spécialisées, les pairs ne s'appellent pas. Une société acquiert plutôt un service de ligne spécialisée pour connecter explicitement deux emplacements fixes. Il arrive que les deux pairs à chaque extrémité de la ligne spécialisée soient situés à différents emplacements physiques de la même société. Une société qui définit un routeur sur une ligne spécialisée connectée à un FAI constitue un autre scénario.

Les lignes spécialisées sont moins courantes que les liaisons commutées, bien qu'elles soient plus faciles à configurer. Elles ne nécessitent pas de scripts de discussion. L'authentification n'est généralement pas utilisée, car les deux pairs se connaissent lorsqu'une ligne est louée. Une fois initialisée par les deux pairs, la liaison PPP reste active. Une liaison de ligne spécialisée reste active, sauf en cas de panne de la ligne ou si l'un des pairs met explicitement fin à la liaison.

Les pairs de ligne spécialisée exécutant Solaris PPP 4.0 utilisent la plupart des fichiers de configuration qui définissent une liaison commutée.

Le processus suivant a lieu pour lancer la communication sur la ligne spécialisée :

1. Chaque pair exécute la commande `pppd` dans le cadre du processus d'initialisation ou d'un autre script d'administration.
2. Les pairs lisent leurs fichiers de configuration PPP.
3. Les pairs négocient les paramètres de communication.
4. Une liaison IP est établie.

Authentification PPP

L'authentification est le processus qui permet de vérifier qu'un utilisateur est bien celui qu'il dit être. La séquence de connexion UNIX est une forme simple d'authentification :

1. La commande `login` invite l'utilisateur à spécifier un nom et un mot de passe.
2. `login` tente alors d'authentifier l'utilisateur en recherchant le nom d'utilisateur et le mot de passe entrés dans la base de données de mots de passe.
3. Si la base de données contient le nom d'utilisateur et le mot de passe en question, l'utilisateur est *authentifié* et se voit autoriser à accéder au système. Si la base de données ne contient pas le nom d'utilisateur et le mot de passe, l'accès au système est refusé à l'utilisateur.

Par défaut, Solaris PPP 4.0 n'exige pas l'authentification sur les machines qui ne disposent pas d'une route par défaut spécifiée. Par conséquent, une machine locale sans route par défaut n'authentifie pas les appelants distants. A l'inverse, si elle possède une route par défaut définie, la machine authentifie toujours les appelants distants.

Vous pouvez utiliser les protocoles d'authentification PPP pour vérifier l'identité des appelants qui tentent de configurer une liaison PPP sur votre machine. A l'inverse, vous devez configurer

des informations d'authentification PPP, si votre machine locale doit appeler des pairs qui authentifient des appelants.

Authentificateurs et authentifiés

Sur une liaison PPP, la machine à l'origine de l'appel est considérée comme l'*authentifié*, car elle doit prouver son identité au pair distant. Le pair est considéré comme l'*authentificateur*. L'authentificateur recherche l'identité de l'appelant dans les fichiers PPP correspondant au protocole de sécurité et authentifie ou non l'appelant.

Généralement, vous configurez une authentification PPP pour une liaison commutée. Au début de l'appel, la machine d'appel sortant est l'authentifié. Le serveur d'appel sortant est l'authentificateur. Le serveur possède une base de données sous forme de fichier de *secrets*. Ce fichier répertorie tous les utilisateurs autorisés à configurer une liaison PPP vers le serveur. Considérez ces utilisateurs comme des *appelants de confiance*.

Certaines machines d'appel sortant demandent aux pairs distants de fournir des informations d'authentification lorsqu'ils répondent à leurs appels. Leurs rôles sont ensuite inversés : le pair distant devient l'authentifié et la machine d'appel sortant l'authentificateur.

Remarque - Bien que PPP 4.0 n'empêche pas l'authentification par les pairs de ligne spécialisée, l'authentification n'est pas fréquente dans ce type de liaison. La nature des contrats de lignes spécialisées implique généralement que les deux participants à chaque extrémité de la ligne se connaissent. Il s'agit souvent de participants de confiance. Toutefois, étant donné que l'authentification PPP n'est pas très difficile à gérer, vous devriez sérieusement envisager de mettre en oeuvre l'authentification pour les lignes spécialisées.

Protocoles d'authentification PPP

Les protocoles d'authentification PPP sont les protocoles PAP (Password Authentication Protocol) et CHAP (Challenge-Handshake Authentication Protocol). Chaque protocole utilise une base de données de *secrets* qui contient des informations d'identification, ou *informations d'identification de sécurité*, pour chaque appelant autorisé à se connecter à la machine locale. Pour une explication détaillée de PAP, reportez-vous à la section “Protocole d'authentification par mot de passe (PAP)” à la page 133. Pour une explication de CHAP, reportez-vous à la section “Protocole CHAP (Challenge-Handshake Authentication Protocol)” à la page 136.

Raisons de l'utilisation de l'authentification PPP

Fournir l'authentification sur une liaison PPP est facultatif. En outre, bien que l'authentification vérifie qu'un pair est digne de confiance, l'authentification PPP ne garantit pas la confidentialité

des données. Pour assurer la confidentialité, utilisez des logiciels de chiffrement, tels que IPsec, PGP, SSL, Kerberos et Secure Shell.

Remarque - Solaris PPP 4.0 ne met pas en oeuvre le protocole ECP (Encryption Control Protocol) PPP, décrit dans le document RFC 1968.

Envisagez la mise en oeuvre de l'authentification PPP dans les situations suivantes :

- Votre société accepte les appels entrants provenant d'utilisateurs sur le réseau téléphonique commuté public.
- La stratégie de sécurité de votre entreprise exige que les utilisateurs distants fournissent des informations d'authentification lorsqu'ils accèdent à votre réseau à travers un pare-feu d'entreprise ou lorsqu'ils se livrent à des transactions sécurisées.
- Vous voulez authentifier les appelants par rapport à une base de données de mots de passe UNIX standard, telle que `/etc/passwd`, NIS, LDAP ou PAM. Utilisez une authentification PAP pour ce scénario.
- Les serveurs d'appel entrant de votre société fournissent également la connexion Internet du réseau. Utilisez une authentification PAP pour ce scénario.
- La ligne série est moins sûre que la base de données de mots de passe sur la machine ou les réseaux à chaque extrémité de la liaison. Utilisez une authentification CHAP pour ce scénario.

Prise en charge des utilisateurs DSL via PPPoE

De nombreux fournisseurs réseau et utilisateurs qui travaillent à domicile ont recours à la technologie DSL (Digital Subscriber Line, ligne d'abonné numérique) pour accélérer l'accès au réseau. Pour prendre en charge les utilisateurs DSL, Solaris PPP 4.0 intègre la fonction PPPoE (PPP over Ethernet). La technologie PPPoE permet à plusieurs hôtes d'exécuter des sessions PPP sur une liaison Ethernet vers une ou plusieurs destinations.

Si l'un des facteurs suivants s'applique à votre situation, vous devez utiliser le protocole PPPoE :

- Vous prenez en charge les utilisateurs DSL, y compris éventuellement vous-même. Votre fournisseur de services DSL peut demander aux utilisateurs de configurer un tunnel PPPoE pour recevoir des services sur la ligne DSL.
- Votre site est un FAI qui envisage de proposer PPPoE à ses clients.

Cette section présente les termes associés à la technologie PPPoE et une vue d'ensemble d'une topologie PPPoE de base.

Présentation PPPoE

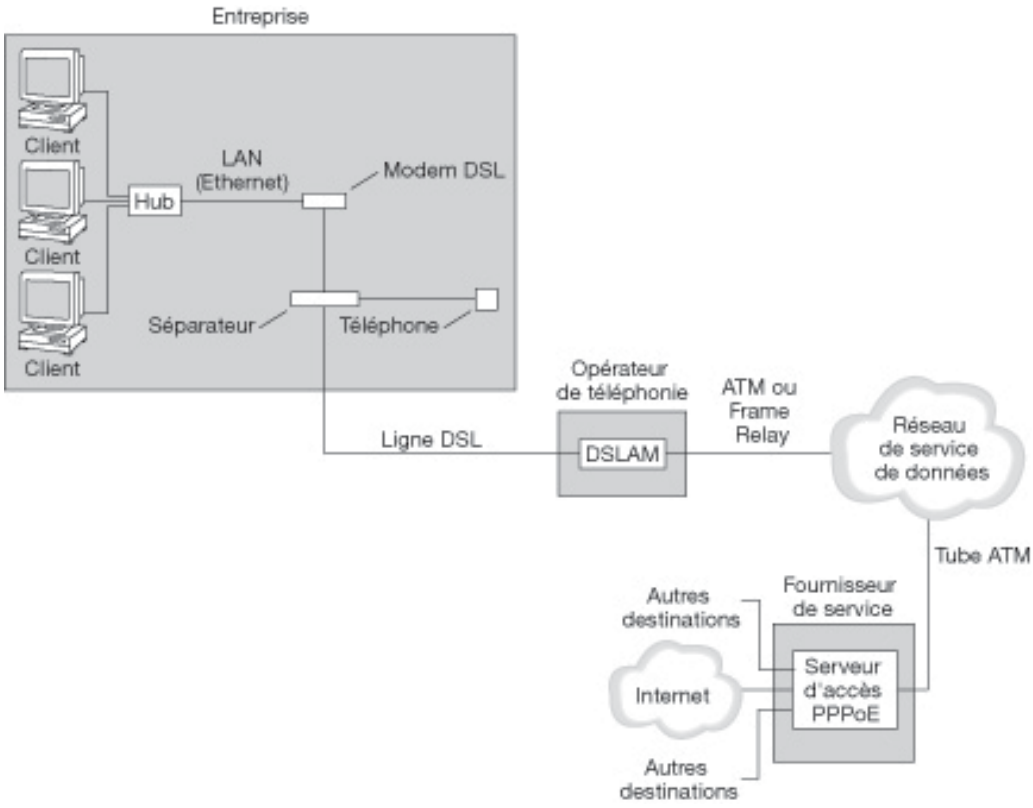
PPPoE est un protocole propriétaire de RedBack Networks. Plus qu'une autre version du protocole PPP standard, PPPoE est un protocole de découverte. Dans un scénario PPPoE, une machine qui lance des communications PPP doit d'abord repérer, ou *découvrir* , un pair qui exécute PPPoE. Le protocole PPPoE utilise des paquets de diffusion Ethernet pour localiser le pair.

Une fois le processus de détection terminé, PPPoE configure un tunnel Ethernet reliant l'hôte initiateur (*client PPPoE*) au pair (*serveur d'accès PPPoE*). La *mise en tunnel* consiste à exécuter un protocole sur un autre. A l'aide du protocole PPPoE, Solaris PPP 4.0 met en tunnel PPP sur Ethernet IEEE 802.2, deux protocoles de liaison de données. La connexion PPP obtenue se comporte comme une liaison dédiée entre le client PPPoE et le serveur d'accès. Pour des informations détaillées sur PPPoE, reportez-vous à la section “Création de tunnels PPPoE pour la prise en charge DSL ” à la page 141.

Composants d'une configuration PPPoE

Trois participants sont impliqués dans une configuration PPPoE : un consommateur, un opérateur de téléphonie et un fournisseur de service, comme illustré dans la figure suivante.

FIGURE 1-4 Participants à un tunnel PPPoE



Consommateurs PPPoE

En tant qu'administrateur système, vous pouvez aider les consommateurs à réaliser leur configuration PPPoE. Une personne ayant besoin d'exécuter PPPoE sur une ligne DSL est un consommateur PPPoE typique. Un autre consommateur PPPoE est une société qui acquiert une ligne DSL par le biais de laquelle ses employés peuvent exécuter des tunnels PPPoE, comme illustré dans la figure précédente.

Offrir des communications PPP par le biais d'un périphérique DSL haut débit à un nombre d'hôtes est la principale raison qui incite un consommateur professionnel à utiliser PPPoE. Souvent, un client PPPoE possède son propre *modem DSL*. Plusieurs clients sur un hub peuvent aussi partager un modem DSL également connecté au hub par une ligne Ethernet.

Remarque - Techniquement, les périphériques DSL sont des ponts, pas des modems. Cependant, ces périphériques étant couramment appelés des modems, ce guide utilise le terme "modem DSL".

PPPoE exécute PPP via un tunnel sur la ligne Ethernet connectée au modem DSL. Cette ligne est connectée à un séparateur, qui à son tour se connecte à une ligne téléphonique.

PPPoE côté opérateur de téléphonie

L'entreprise téléphonique correspond à la couche intermédiaire du scénario PPPoE. Il divise le signal reçu via la ligne téléphonique à l'aide d'un périphérique appelé *multiplexeur DSLAM (Digital Subscriber Line Access Multiplexer, multiplexeur d'accès de ligne d'abonné numérique)*. Le multiplexeur DSLAM décompose les signaux analogiques sur différents câbles, câbles analogiques pour le service téléphonique et câbles numériques pour PPPoE. Depuis le multiplexeur DSLAM, les câbles numériques prolongent le tunnel sur un réseau de données ATM jusqu'au FAI.

PPPoE côté fournisseur de service

Le FAI reçoit la transmission PPPoE du réseau de données ATM via un pont. Au niveau du fournisseur d'accès Internet, un serveur d'accès exécutant PPPoE fonctionne tout comme le pair de la liaison PPP. Le serveur d'accès fonctionne de manière très similaire au serveur d'appel entrant présenté à la Figure 1-2, “Liaison PPP commutée analogique de base”, à ceci près que le serveur n'utilise pas de modems. Le serveur d'accès convertit chaque session PPPoE en trafic IP régulier, un accès à Internet par exemple.

Si vous êtes l'administrateur système d'un fournisseur d'accès Internet, vous pouvez être chargé de la configuration et de la gestion d'un serveur d'accès.

Sécurité d'un tunnel PPPoE

Le tunnel PPPoE est par nature non sécurisé. Vous pouvez utiliser PAP ou CHAP afin de fournir l'authentification de l'utilisateur pour la liaison PPP en cours d'exécution sur le tunnel.

♦ ♦ ♦ CHAPITRE 2

Planification de la liaison Point-to-Point Protocol

Définir une liaison PPP implique un ensemble de tâches distinctes, qui inclut la planification et d'autres activités qui ne sont pas liées à PPP. Ce chapitre explique comment planifier les liaisons PPP les plus courantes, l'authentification et PPPoE.

Les chapitres qui suivent le Chapitre 2, Planification de la liaison Point-to-Point Protocol utilisent des exemples de configuration pour illustrer comment configurer une liaison donnée. Ces exemples de configuration sont présentés dans ce chapitre.

Voici la liste des sujets abordés :

Planification PPP générale (liste des tâches)

PPP requiert des tâches de planification avant que la liaison puisse être configurée. En outre, si vous souhaitez utiliser la mise en tunnel PPPoE, vous devez d'abord configurer la liaison PPP, puis assurer la mise en tunnel. La liste des tâches suivante répertorie les principales tâches de planification abordées dans ce chapitre. Il se peut que la tâche générale suffise à configurer votre type de liaison. Il se peut aussi que les tâches de liaison, authentification et peut-être PPPoE soient nécessaires.

TABLEAU 2-1 Liste des tâches de planification PPP

Tâche	Description	Pour obtenir des instructions
Planification d'une liaison PPP commutée	Rassemblez les informations nécessaires à la configuration d'une machine d'appel sortant ou d'un serveur d'appel entrant.	"Planification d'une liaison PPP commutée" à la page 30
Planification d'une liaison de ligne spécialisée	Rassemblez les informations nécessaires à la configuration d'un client sur une ligne spécialisée.	"Planification d'une liaison de ligne spécialisée" à la page 33
Planification de l'authentification sur une liaison PPP	Rassemblez les informations nécessaires à la configuration de l'authentification PAP ou CHAP sur la liaison PPP.	"Planification de l'authentification sur une liaison" à la page 36

Tâche	Description	Pour obtenir des instructions
Planification d'un tunnel PPPoE	Rassemblez les informations nécessaires à la configuration d'un tunnel PPPoE sur lequel une liaison PPP peut s'exécuter.	“Planification de la prise en charge DSL sur un tunnel PPPoE” à la page 41

Planification d'une liaison PPP commutée

Parmi les liaisons PPP, les liaisons commutées sont les plus courantes. Cette section contient les informations suivantes :

- Informations de planification d'une liaison commutée
- Explication de l'exemple de liaison à utiliser au Chapitre 3, Configuration d'une liaison Point-to-Point Protocol

En général, vous configurez uniquement la machine située à l'une des extrémités de la liaison PPP commutée : la machine d'appel sortant ou le serveur d'appel entrant. Pour une présentation de la liaison PPP commutée, reportez-vous à la section “Présentation de la liaison commutée PPP” à la page 17.

Avant de configurer la machine d'appel sortant

Avant de configurer une machine d'appel sortant, rassemblez les informations répertoriées dans le tableau ci-dessous.

Remarque - Les informations de planification contenues dans cette section n'incluent pas les informations à rassembler sur l'authentification ou PPPoE. Pour plus d'informations sur la planification de l'authentification, reportez-vous à la section “Planification de l'authentification sur une liaison” à la page 36. Pour la planification PPPoE, reportez-vous à la section “Planification de la prise en charge DSL sur un tunnel PPPoE” à la page 41.

TABLEAU 2-2 Informations pour une machine d'appel sortant

Données	Intervention
Vitesse maximale du modem	Reportez-vous à la documentation fournie par le fabricant du modem.
Commandes de connexion du modem (commandes AT)	Reportez-vous à la documentation fournie par le fabricant du modem.
Nom à attribuer au serveur d'appel entrant situé à l'autre extrémité de la liaison	Créez un nom vous permettant d'identifier le serveur d'appel entrant.
Séquence de connexion requise par le serveur d'appel entrant	Contactez l'administrateur du serveur d'appel entrant ou consultez la documentation du FAI si le serveur d'appel entrant se trouve chez le FAI.

Avant de configurer le serveur d'appel entrant

Avant de configurer un serveur d'appel entrant, rassemblez les informations répertoriées dans le tableau ci-dessous.

Remarque - Les informations de planification contenues dans cette section n'incluent pas les informations à rassembler sur l'authentification ou PPPoE. Pour plus d'informations sur la planification de l'authentification, reportez-vous à la section “Planification de l'authentification sur une liaison” à la page 36. Pour la planification PPPoE, reportez-vous à la section “Planification de la prise en charge DSL sur un tunnel PPPoE” à la page 41.

TABLEAU 2-3 Informations pour un serveur d'appel entrant

Données	Intervention
Vitesse maximale du modem	Reportez-vous à la documentation fournie par le fabricant du modem.
Noms des utilisateurs autorisés à appeler le serveur d'appel entrant	Obtenez le nom des utilisateurs potentiels avant de configurer leurs répertoires personnels, comme indiqué à la section “Configuration des utilisateurs du serveur d'appel entrant ” à la page 55.
Adresse IP dédiée aux communications PPP	Obtenez l'adresse de la personne responsable au sein de votre société de la délégation des adresses IP.

Exemple de configuration d'une liaison PPP commutée

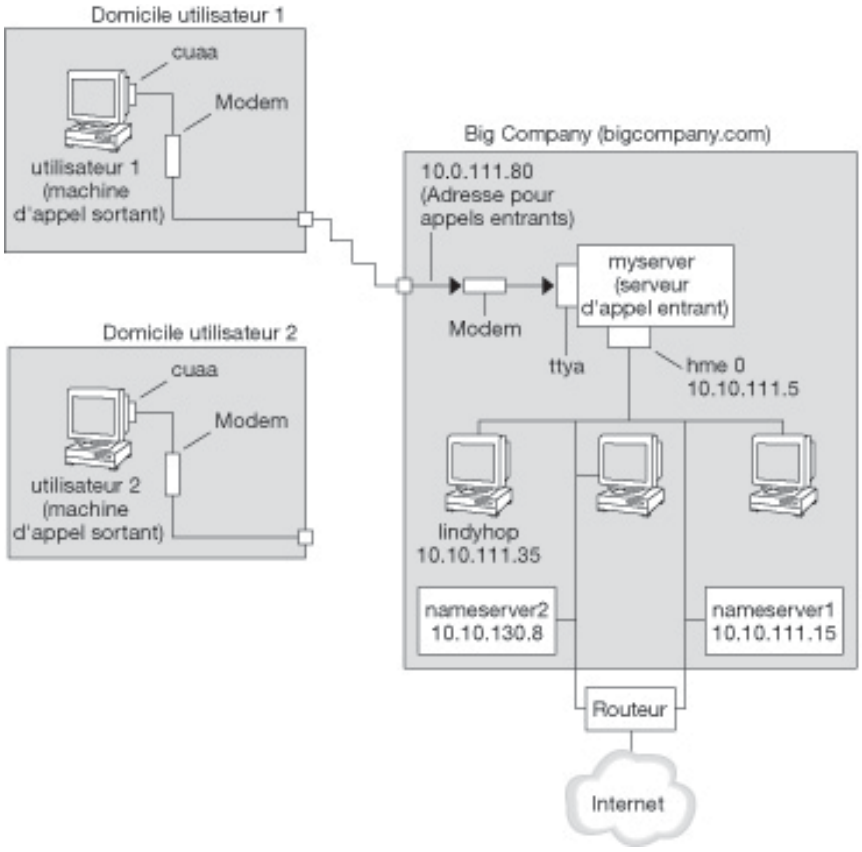
Les tâches pésentées au Chapitre 3, Configuration d'une liaison Point-to-Point Protocol mettent en oeuvre la demande d'une petite entreprise de laisser les employés travailler depuis chez eux quelques jours par semaine. Le SE Oracle Solaris doit être installé sur l'ordinateur que les employés utilisent chez eux. Ceux-ci doivent également se connecter à distance à leur machine de travail sur l'intranet de l'entreprise.

Les tâches permettent de configurer une liaison commutée de base aux caractéristiques suivantes :

- Les machines *d'appel sortant* sont situées chez les employés qui doivent appeler l'intranet de l'entreprise.
- Le serveur *d'appel entrant* est une machine située sur l'intranet de l'entreprise, configurée pour recevoir les appels entrants des employés.
- Une connexion de type UNIX est utilisée pour authentifier la machine d'appel sortant. Des méthodes d'authentification Solaris PPP 4.0 plus strictes ne sont pas requises par la politique de sécurité de l'entreprise.

La figure suivante illustre la liaison créée au Chapitre 3, Configuration d'une liaison Point-to-Point Protocol.

FIGURE 2-1 Exemple de liaison commutée



Dans cette figure, un hôte distant lance un appel sortant par le biais de son modem via les lignes téléphoniques à l'intranet de Big Company. Un autre hôte est configuré pour pouvoir établir une connexion à Big Company mais est actuellement inactif. Les appels provenant d'utilisateurs distants sont traités dans l'ordre selon lequel ils sont reçus par le modem connecté au serveur d'appel entrant au sein de Big Company. Une connexion PPP est établie entre les pairs. La machine d'appel sortant peut ensuite se connecter à distance à une machine hôte sur l'intranet.

Sources d'informations sur la liaison PPP commutée

Reportez-vous aux sections suivantes :

- Pour configurer une machine d'appel sortant, reportez-vous au Tableau 3-2, “Liste des tâches de la configuration de la machine d'appel sortant”.
- Pour configurer une machine d'appel entrant, reportez-vous au Tableau 3-3, “Liste des tâches de la configuration du serveur d'appel entrant ”.
- Pour obtenir un aperçu des liaisons commutées, reportez-vous à la section “Présentation de la liaison commutée PPP” à la page 17.
- Pour obtenir des informations détaillées sur les commandes et fichiers PPP, reportez-vous à la section “Utilisation des options PPP dans les fichiers et sur la ligne de commande ” à la page 111.

Planification d'une liaison de ligne spécialisée

Configurer une liaison de ligne spécialisée consiste à configurer le pair situé à une extrémité d'un service commuté ou non commuté, loué à un fournisseur.

Cette section contient les informations suivantes :

- Informations de planification d'une ligne spécialisée
- Explication de l'exemple de liaison illustré à la Figure 2-2, “Exemple d'une configuration de ligne spécialisée”

Pour une présentation des liaisons de ligne spécialisée, reportez-vous à la section “Présentation de la liaison PPP de ligne spécialisée” à la page 21. Pour connaître les tâches de configuration d'une ligne spécialisée, reportez-vous au Chapitre 4, Configuration d'une liaison Point-to-Point Protocol de ligne spécialisée.

Avant de configurer une liaison de ligne spécialisée

Lorsque votre société loue une liaison de ligne spécialisée à un fournisseur réseau, vous ne configurez généralement que le système à votre extrémité de la liaison. Le pair situé à l'autre extrémité de la liaison est géré par un autre administrateur. Il peut s'agir d'un administrateur système situé à un emplacement distant au sein de votre société ou d'un administrateur système chez le fournisseur d'accès Internet.

Matériel nécessaire à une liaison de ligne spécialisée

Outre le média de la liaison, votre extrémité de la liaison nécessite le matériel suivant :

- Interface synchrone pour votre système
- Unité synchrone (CSU/DSU)
- Votre système

L'équipement des locaux d'abonné (CPE, customer premises equipment) de certains fournisseurs de services réseau inclut un routeur, une interface synchrone et une CSU/DSU. Cependant, l'équipement nécessaire varie en fonction du fournisseur et des restrictions gouvernementales liées à votre environnement linguistique. Le fournisseur réseau peut vous fournir des informations sur l'unité nécessaire, si cet équipement n'est pas fourni avec la ligne spécialisée.

Informations à rassembler pour la liaison de ligne spécialisée

Avant de configurer le pair local, il vous faudra peut-être rassembler les éléments répertoriés dans le tableau suivant.

TABLEAU 2-4 Planification d'une liaison de ligne spécialisée

Données	Intervention
Nom de périphérique de l'interface	Reportez-vous à la documentation de la carte d'interface.
Instructions de configuration de la carte d'interface synchrone	Reportez-vous à la documentation de la carte d'interface. Vous avez besoin de ces informations pour configurer l'interface HSI/P. Il n'est peut-être pas nécessaire de configurer d'autres types de cartes d'interface.
(Facultatif) Adresse IP du pair distant	Reportez-vous à la documentation du fournisseur de service. Vous pouvez également contacter l'administrateur système du pair distant. Ces informations sont nécessaires uniquement si l'adresse IP n'est pas négociée entre les deux pairs.
(Facultatif) Nom du pair distant	Reportez-vous à la documentation du fournisseur de service. Vous pouvez également contacter l'administrateur système du pair distant.
(Facultatif) Vitesse de la liaison	Reportez-vous à la documentation du fournisseur de service. Vous pouvez également contacter l'administrateur système du pair distant.
(Facultatif) Compression utilisée par le pair distant	Reportez-vous à la documentation du fournisseur de service. Vous pouvez également contacter l'administrateur système du pair distant.

Exemple de configuration d'une liaison de ligne spécialisée

Les tâches du Chapitre 4, Configuration d'une liaison Point-to-Point Protocol de ligne spécialisée décrivent la mise en oeuvre de l'objectif d'une entreprise de taille moyenne (LocalCorp) de fournir un accès Internet à ses employés. A présent, les ordinateurs des employés sont connectés au réseau privé de l'entreprise (intranet).

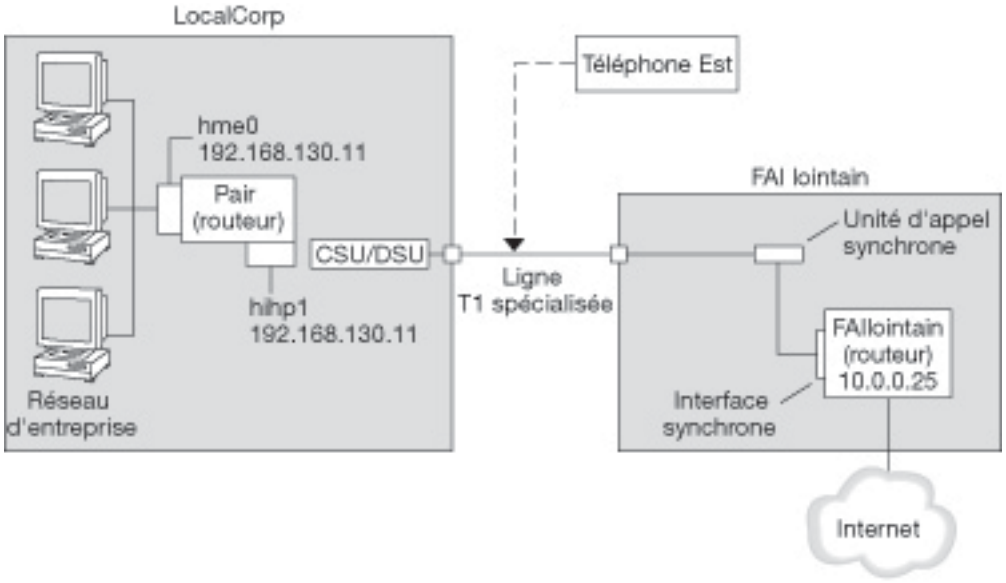
LocalCorp a besoin d'accélérer les transactions et l'accès aux nombreuses ressources disponibles sur Internet. La société signe un contrat avec le fournisseur d'accès Internet FAI lointain, ce qui

lui permet de définir sa propre ligne spécialisée avec FAI lointain. Ensuite, LocalCorp loue une ligne T1 à Téléphone Est, un opérateur de téléphonie. Téléphone Est installe la ligne spécialisée entre LocalCorp et le FAI lointain. Téléphone Est fournit ensuite une CSU/DSU déjà configurée à LocalCorp.

Les tâches permettent de configurer une liaison de ligne spécialisée dotée des caractéristiques suivantes :

- LocalCorp a configuré un système sous forme de routeur de passerelle, qui transmet les paquets à des hôtes sur Internet via la ligne spécialisée.
- Le FAI lointain a également défini un pair comme routeur auquel des lignes spécialisées de clients sont connectées.

FIGURE 2-2 Exemple d'une configuration de ligne spécialisée



Dans la figure, un routeur est configuré pour PPP au sein de LocalCorp. Le routeur se connecte à l'intranet de l'entreprise par l'intermédiaire de son interface `hme0`. La deuxième connexion relie l'interface HSI/P (hihp1) de la machine à l'unité numérique CSU/DSU. La CSU/DSU se connecte alors à la ligne spécialisée installée. L'administrateur de LocalCorp configure

l'interface HSI/P et fichiers PPP. L'administrateur tape ensuite `/etc/init.d/pppd` pour initialiser la liaison entre LocalCorp et le FAI lointain.

Sources d'informations sur les lignes spécialisées

Reportez-vous aux sections suivantes :

- Chapitre 4, Configuration d'une liaison Point-to-Point Protocol de ligne spécialisée
- “Présentation de la liaison PPP de ligne spécialisée” à la page 21

Planification de l'authentification sur une liaison

Cette section contient les informations de planification pour fournir l'authentification sur la liaison PPP. Le Chapitre 5, Configuration de l'authentification Point-to-Point Protocol contient les tâches permettant de mettre en oeuvre l'authentification PPP sur votre site.

PPP offre deux types d'authentification : PAP, qui est décrite en détail à la section “Protocole d'authentification par mot de passe (PAP)” à la page 133 et CHAP, qui est décrite à la section “Protocole CHAP (Challenge-Handshake Authentication Protocol)” à la page 136.

Avant de configurer l'authentification sur une liaison, vous devez choisir le protocole d'authentification qui répond le mieux à la stratégie de sécurité de votre site. Ensuite, vous configurez le fichier des secrets et les fichiers de configuration PPP pour les machines d'appel entrant ou les machines d'appel sortant des appelants, ou les deux types de machines. Pour plus d'informations sur le choix du protocole d'authentification qui convient à votre site, reportez-vous à la section “Raisons de l'utilisation de l'authentification PPP” à la page 24.

Cette section contient les informations suivantes :

- Informations de planification pour les authentifications PAP et CHAP
- Explications des exemples de scénario d'authentification présentés à la Figure 2-3, “Exemple d'un scénario d'authentification PAP (travail à domicile) ” et à la Figure 2-4, “Exemple d'un scénario d'authentification CHAP (appel d'un réseau privé) ”

Pour connaître les tâches de configuration de la fonction d'authentification, reportez-vous au Chapitre 5, Configuration de l'authentification Point-to-Point Protocol.

Avant de configurer l'authentification PPP

La configuration de l'authentification sur votre site doit faire partie intégrante de votre stratégie PPP générale. Avant de mettre en oeuvre l'authentification, vous devez monter le matériel, configurer le logiciel et tester la liaison.

TABLEAU 2-5 Prérequis à la configuration de l'authentification

Données	Pour obtenir des instructions
Tâches de configuration d'une liaison commutée	Chapitre 3, Configuration d'une liaison Point-to-Point Protocol.
Tâches relatives au test de la liaison	Chapitre 7, Dépannage de problèmes courants du Point-to-Point Protocol.
Exigences en matière de sécurité pour votre site	Stratégie de sécurité de votre entreprise. Si vous ne disposez pas d'une stratégie de sécurité, la configuration de l'authentification PPP vous offre l'occasion d'en créer une.
Suggestions à propos de l'utilisation du protocole PAP ou CHAP sur votre site	"Raisons de l'utilisation de l'authentification PPP" à la page 24. Pour obtenir des informations plus détaillées sur ces protocoles, reportez-vous à la section "Authentification des appelants sur une liaison" à la page 133

Exemples de configuration d'authentification PPP

Cette section contient des exemples de scénarios d'authentification à utiliser dans les procédures décrites au Chapitre 5, Configuration de l'authentification Point-to-Point Protocol.

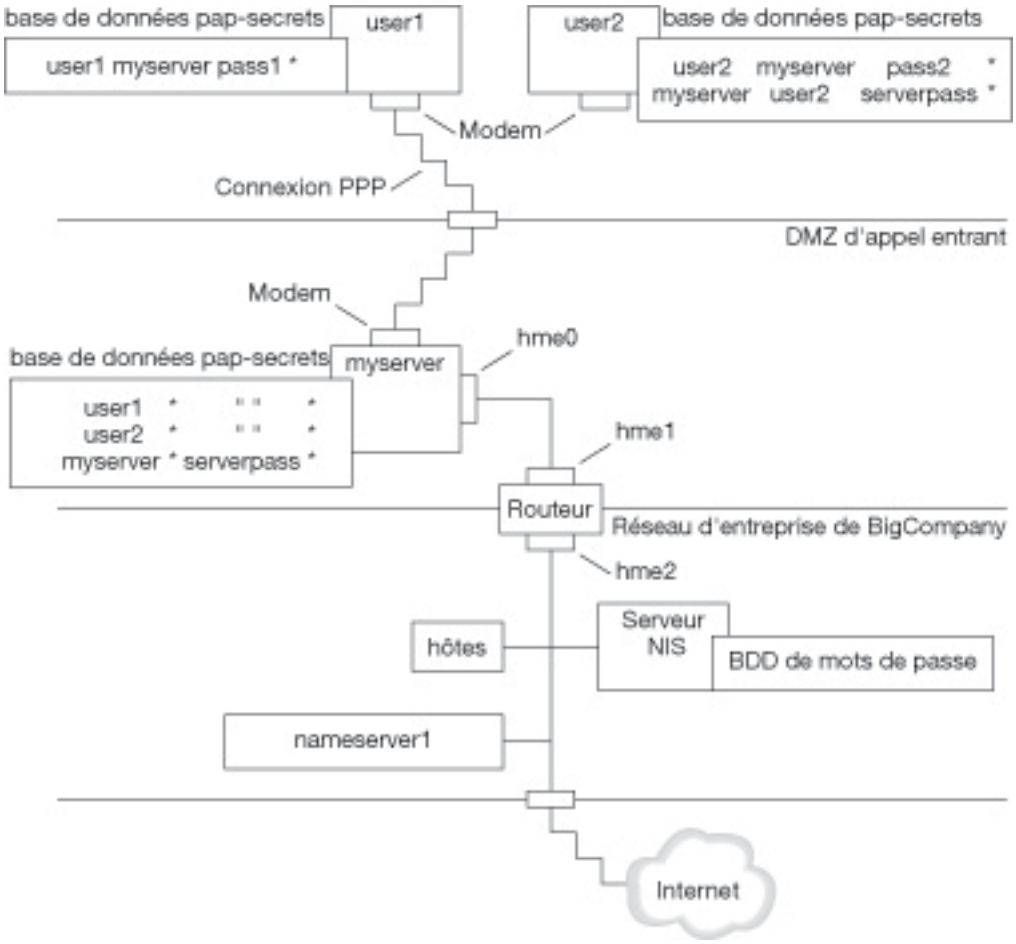
- "Exemple de configuration utilisant une authentification PAP " à la page 37
- "Exemple de configuration utilisant l'authentification CHAP" à la page 39

Exemple de configuration utilisant une authentification PAP

Les tâches décrites à la section "Configuration de l'authentification PAP" à la page 68 montrent comment configurer une authentification PAP sur la liaison PPP. Les procédures utilisent comme exemple un scénario PAP créé pour la société fictive Big Company dans l'"Exemple de configuration d'une liaison PPP commutée" à la page 31.

Big Company veut permettre à ses utilisateurs de travailler à domicile. Les administrateurs système veulent une solution sûre pour les lignes série reliées au serveur d'appel entrant. La connexion de type UNIX qui fait appel aux bases de données de mots de passe NIS a convenu au réseau de Big Company par le passé. Les administrateurs système veulent un modèle d'authentification UNIX pour les appels entrant sur le réseau via la liaison PPP. Par conséquent, ils peuvent appliquer le scénario suivant qui a recours à l'authentification PAP.

FIGURE 2-3 Exemple d'un scénario d'authentification PAP (travail à domicile)



Le administrateurs système créent une DMZ d'appel entrant dédiée et séparée du reste du réseau d'entreprise par un routeur. L'acronyme DMZ provient du terme militaire anglais "demilitarized zone" (zone démilitarisée). La DMZ est un réseau isolé, configuré pour des raisons de sécurité. La DMZ contient généralement les ressources qu'une société offre au public, telles que des serveurs Web, des serveurs FTP anonymes, des bases de données et des serveurs modem. Les concepteurs de réseaux placent souvent la DMZ entre un pare-feu et une connexion Internet de l'entreprise.

Les seuls occupants de la DMZ décrite à la Figure 2-3, “Exemple d'un scénario d'authentification PAP (travail à domicile) ” sont le serveur d'appel entrant `monserveur` et le routeur. Le serveur d'appel entrant exige des appelants qu'ils fournissent leurs informations

d'identification PAP, notamment leurs nom d'utilisateur et mot de passe, lors de la configuration de la liaison. En outre, le serveur d'appel entrant utilise l'option `login` de PAP. Ainsi, les noms d'utilisateur et mots de passe PAP des appelants doivent correspondre exactement à leurs noms d'utilisateur et mots de passe UNIX dans la base de données de mots de passe du serveur d'appel entrant.

Une fois la liaison PPP établie, les paquets de l'appelant sont transmis au routeur. Le routeur fait suivre la transmission à sa destination sur le réseau de l'entreprise ou sur Internet.

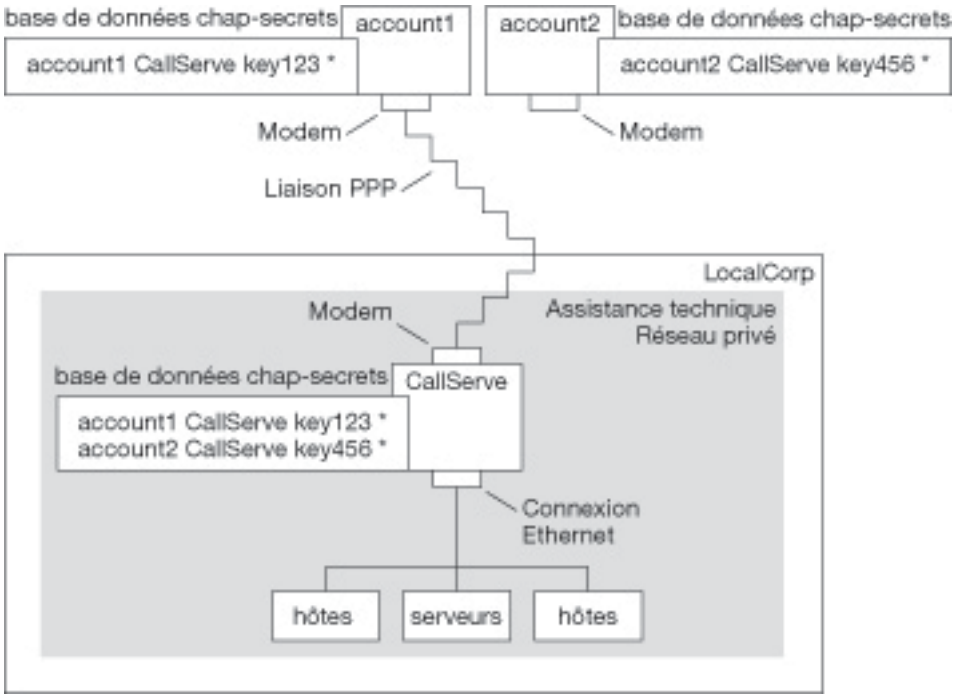
Exemple de configuration utilisant l'authentification CHAP

Les tâches décrites à la section “Configuration de l'authentification CHAP” à la page 76 montrent comment configurer l'authentification CHAP. Les procédures utilisent comme exemple un scénario CHAP à créer pour la société fictive LocalCorp présentée à l'“Exemple de configuration d'une liaison de ligne spécialisée” à la page 34.

LocalCorp fournit la connexion à Internet via une ligne spécialisée à un FAI. Le service d'assistance technique de LocalCorp génère un trafic réseau important. Par conséquent, il a besoin d'un réseau privé isolé. Les techniciens du service voyagent beaucoup et ont besoin d'accéder à distance au réseau de l'assistance technique pour obtenir des informations leur permettant de résoudre des problèmes. Pour protéger les informations confidentielles contenues dans la base de données du réseau privé, les appelants distants doivent être authentifiés avant d'être autorisés à se connecter.

Par conséquent, les administrateurs système mettent en oeuvre le scénario d'authentification CHAP suivant pour une configuration PPP commutée.

FIGURE 2-4 Exemple d'un scénario d'authentification CHAP (appel d'un réseau privé)



Le seul lien entre le réseau de l'assistance technique et le monde extérieur est la ligne série vers l'extrémité du serveur d'appel entrant de la liaison. Les administrateurs système configurent l'ordinateur portable de chaque représentant du service pour une liaison PPP dotée de la sécurité CHAP, comprenant un secret CHAP. La base de données des secrets CHAP située sur le serveur d'appel entrant contient les informations d'identification CHAP pour toutes les machines qui sont autorisées à appeler le réseau de l'assistance technique.

Sources d'informations sur l'authentification

Vous disposez des ressources suivantes :

- Voir “Configuration de l'authentification PAP” à la page 68.
- Voir “Configuration de l'authentification CHAP” à la page 76.
- Voir “Authentification des appelants sur une liaison” à la page 133 et la page de manuel `pppd`(1M).

Planification de la prise en charge DSL sur un tunnel PPPoE

Certains fournisseurs DSL vous demandent de configurer la mise en tunnel PPPoE de votre site pour exécuter PPP sur leurs réseaux numériques haut débit et lignes DSL. Pour une présentation de PPPoE, reportez-vous à la section “Prise en charge des utilisateurs DSL via PPPoE ” à la page 25.

Un tunnel PPPoE implique trois participants : un consommateur, un opérateur de téléphonie et un fournisseur d'accès Internet. Vous configurez PPPoE pour des consommateurs (des clients PPPoE au sein de votre entreprise ou des particuliers à domicile, par exemple) ou sur un serveur auprès d'un fournisseur d'accès Internet.

Cette section contient les informations de planification pour l'exécution PPPoE sur les clients et les serveurs d'accès. Il aborde les sujets suivants :

- Informations de planification pour le serveur d'accès et l'hôte PPPoE
- Explication du scénario PPPoE présenté à la section “Exemple de configuration d'un tunnel PPPoE ” à la page 43

Le Chapitre 6, Configuration d'un tunnel PPP Over Ethernet décrit les tâches de configuration d'un tunnel PPPoE.

Avant de configurer un tunnel PPPoE

Les activités précédant la configuration varient en fonction du côté du tunnel que vous configurez, client ou serveur. Dans les deux cas, vous ou votre entreprise devez conclure un contrat avec un opérateur de téléphonie. Celui-ci fournit les lignes DSL aux clients, ainsi qu'une passerelle et éventuellement un tube ATM aux serveurs d'accès. La plupart des contrats stipulent qu'il incombe à l'opérateur de téléphonie de monter son équipement sur votre site.

Avant de configurer un client PPPoE

Généralement, l'implémentation du client PPPoE inclut l'équipement suivant :

- Ordinateur personnel ou autre système utilisé par un particulier ;
- Modem DSL généralement installé par l'opérateur de téléphonie ou le fournisseur d'accès Internet ;
- (Facultatif) Hub, si plusieurs clients sont impliqués, ce qui est le cas des consommateurs DSL d'entreprises ;
- (Facultatif) Séparateur, généralement installé par le fournisseur

De nombreuses configurations DSL sont possibles, en fonction des besoins de l'utilisateur ou de la société, ainsi que des services proposés par le fournisseur.

TABLEAU 2-6 Planification pour les clients PPPoE

Données	Intervention
Si vous configurez un client PPPoE à domicile pour un particulier ou pour vous-même, rassemblez les informations de configuration figurant hors du champ d'application de PPPoE.	Demandez les procédures de configuration requises à l'opérateur de téléphonie ou au fournisseur d'accès Internet (FAI).
Si vous configurez des clients PPPoE au niveau d'un site d'entreprise, rassemblez le nom des utilisateurs auxquels sont affectés les systèmes client PPPo E. Si vous configurez des clients PPPoE distants, la responsabilité de fournir aux utilisateurs des informations relatives à l'ajout d'équipements DSL à domicile peut vous incomber.	Demandez une liste des utilisateurs autorisés à la direction de votre entreprise.
Recherchez les interfaces disponibles sur le client PPPoE.	Exécutez la commande `ipadm show-addr` sur chaque machine pour les noms d'interface.
(Facultatif) Obtenez le mot de passe du client PPPoE.	Demandez aux utilisateurs les mots de passe qu'ils préfèrent. Ou affectez des mots de passe aux utilisateurs. Notez que ce mot de passe est utilisé pour l'authentification de liaison, non pour la connexion UNIX.

Avant de configurer un serveur PPPoE

La planification d'un serveur d'accès PPPoE implique une collaboration avec l'opérateur de téléphonie qui vous fournit la connexion à son réseau de service de données. L'opérateur de téléphonie installe ses lignes, souvent des tubes ATM, sur votre site, et fournit une passerelle à votre serveur d'accès. Vous devez configurer les interfaces Ethernet qui ont accès aux services offerts par votre société. Par exemple, vous devez configurer des interfaces pour l'accès à Internet, ainsi que les interfaces Ethernet du pont de l'opérateur de téléphonie

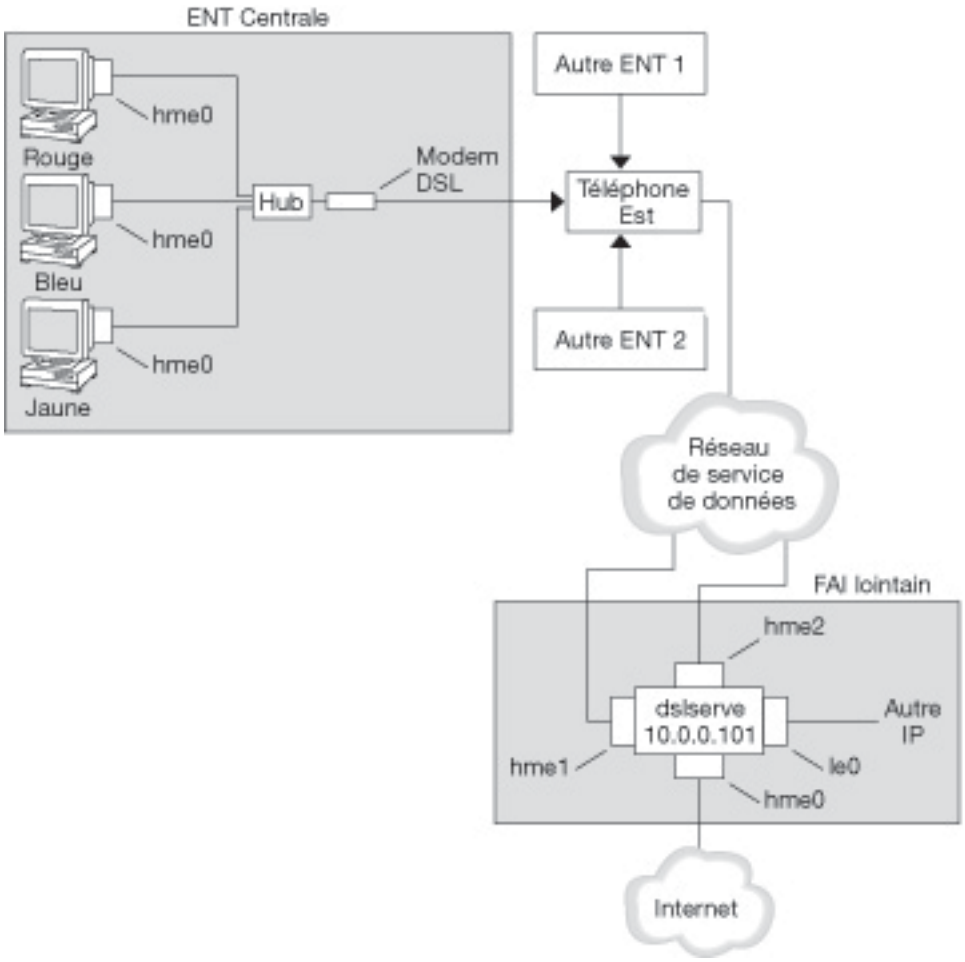
TABLEAU 2-7 Planification d'un serveur d'accès PPPoE

Données	Intervention
Interfaces utilisées pour les lignes du réseau de service de données	Exécutez la commande `ipadm show-addr` pour identifier des interfaces.
Types de services à fournir à partir du serveur PPPo E	Demandez à la direction et aux planificateurs de réseau qu'ils vous fournissent leurs exigences et suggestions.
(Facultatif) Types de services à fournir aux consommateurs	Demandez à la direction et aux planificateurs de réseau qu'ils vous fournissent leurs exigences et suggestions.
(Facultatif) Noms d'hôte et mots de passe des clients distants	Demandez aux planificateurs de réseau et aux autres personnes responsables sur votre site de la négociation des contrats. Les noms d'hôte et mots de passe sont utilisés pour l'authentification PAP ou CHAP, non pour la connexion UNIX.

Exemple de configuration d'un tunnel PPPoE

Cette section contient un exemple d'un tunnel PPPoE qui sert d'illustration des tâches décrites au Chapitre 6, Configuration d'un tunnel PPP Over Ethernet. Bien que l'illustration indique tous les participants au tunnel, vous administrez uniquement une extrémité, le côté client ou le côté serveur.

FIGURE 2-5 Exemple de tunnel PPPoE



Dans l'exemple, ENT Centrale souhaite fournir un accès Internet haut débit à ses employés. ENT Centrale acquiert un package DSL auprès de Téléphone Est, qui, à son tour, passe un

contrat avec le fournisseur d'accès Internet FAI lointain. Le FAI lointain offre un accès Internet et d'autres services IP aux clients qui achètent un package DSL à Téléphone Est.

Exemple de configuration client PPPoE

ENT Centrale acquiert un package auprès de Téléphone Est qui fournit une ligne DSL au site. L'offre comprend une connexion authentifiée dédiée au FAI pour les clients PPPoE d'ENT Centrale. L'administrateur système connecte les clients PPPoE potentiels à un hub. Les techniciens de Téléphone Est connectent le hub à leur équipement DSL.

Exemple de configuration d'un serveur PPPoE

Dans le cadre de l'application de l'accord commercial entre le FAI ISP lointain et Téléphone est, l'administrateur système du FAI configure le serveur d'accès `dslserve`. Ce serveur possède quatre interfaces :

- `eri0` : interface du réseau principal qui se connecte au réseau local
- `hme0` : interface par le biais de laquelle le FAI lointain fournit un service Internet à ses clients
- `hme1` : interface contractée par ENT Centrale pour les tunnels PPPoE authentifiés
- `hme2` : interface contractée par d'autres clients pour leur tunnel PPPoE

Sources d'informations sur PPPoE

Vous disposez des ressources suivantes :

- Voir “Configuration du client PPPoE” à la page 84.
- Voir “Configuration d'un serveur d'accès PPPoE” à la page 87.
- Reportez-vous à la section “Création de tunnels PPPoE pour la prise en charge DSL ” à la page 141 et aux pages de manuel `pppoed`(1M), `pppoec`(1M) et `sppptun`(1M).

♦ ♦ ♦ CHAPITRE 3

Configuration d'une liaison Point-to-Point Protocol

Ce chapitre explique les tâches de la configuration de la liaison PPP la plus courante, la liaison commutée. Les sections principales sont les suivantes :

Tâches principales de la configuration de la liaison PPP commutée (liste des tâches)

Pour configurer la liaison PPP commutée, vous devez configurer des modems, modifier des fichiers de base de données et modifier les fichiers de configuration PPP décrits dans le Tableau 8-1, “Récapitulatif des fichiers de configuration et des commandes PPP”.

Le tableau suivant répertorie les principales tâches de la configuration des deux côtés d'une liaison PPP commutée. En général, vous configurez une seule extrémité de la liaison, c'est-à-dire la machine d'appel sortant ou le serveur d'appel entrant.

TABLEAU 3-1 Liste des tâches de la configuration de la liaison PPP commutée

Tâche	Description	Pour obtenir des instructions
1. Collecte des informations de préconfiguration.	Rassemblez les données qui sont nécessaires avant de procéder à la configuration de la liaison : noms d'hôte des pairs, numéros de téléphone cible et vitesse des modems.	“Planification d'une liaison PPP commutée” à la page 30
2. Configuration de la machine d'appel sortant	Configurez le protocole PPP sur la machine qui effectue l'appel via la liaison.	“Tâches de configuration de la machine d'appel sortant (liste des tâches) ” à la page 46
3. Configuration du serveur d'appel entrant	Configurez le protocole PPP sur la machine qui reçoit les appels entrants.	“Tâches de configuration du serveur d'appel entrant (liste des tâches) ” à la page 53

Tâche	Description	Pour obtenir des instructions
4. Appel du serveur d'appel entrant	Tapez la commande `pppd` pour initialiser les communications.	“Appel du serveur d'appel entrant” à la page 58

Configuration de la machine d'appel sortant

Les tâches de cette section expliquent comment configurer une machine d'appel sortant. Le scénario d'appel entrant à partir du domicile présenté à la Figure 2-1, “Exemple de liaison commutée” sert d'exemple. Vous pouvez effectuer les tâches dans votre société avant de remettre la machine à un utilisateur potentiel. Vous pouvez également indiquer aux utilisateurs expérimentés comment configurer leur machine chez eux. Pour configurer une machine d'appel sortant, il est impératif de posséder l'autorisation racine sur cette machine.

Tâches de configuration de la machine d'appel sortant (liste des tâches)

TABLEAU 3-2 Liste des tâches de la configuration de la machine d'appel sortant

Tâche	Description	Pour obtenir des instructions
1. Collecte des informations de préconfiguration.	Rassemblez les données qui sont nécessaires avant de procéder à la configuration de la liaison : noms d'hôte des pairs, numéros de téléphone cible et vitesse des modems.	“Planification d'une liaison PPP commutée” à la page 30
2. Configuration du modem et du port série	Configurez le modem et le port série.	“Configuration du modem et du port série (machine d'appel sortant)” à la page 48
3. Configuration de la communication via la ligne série	Configurez les caractéristiques de la transmission via la ligne série.	“Définition des communications sur la ligne série ” à la page 49
4. Définition de la conversation entre la machine d'appel sortant et le pair	Rassemblez les données de communication à utiliser lorsque vous créez le script de discussion.	“Création des instructions pour l'appel d'un pair” à la page 50
5. Configuration des informations concernant un pair particulier	Configurez les options PPP pour l'appel d'un serveur d'appel entrant donné.	“Définition de la connexion à un pair donné” à la page 51
6. Appel du pair	Tapez la commande `pppd` pour initialiser les communications.	“Appel du serveur d'appel entrant” à la page 58

Fichiers modèles de liaison PPP commutée

Solaris PPP 4.0 fournit des fichiers modèles. Chaque modèle contient des options courantes pour un fichier de configuration PPP particulier. Le tableau suivant répertorie les exemples de modèles qui peuvent être utilisés pour la configuration d'une liaison commutée et leurs fichiers Solaris PPP 4.0 équivalents.

Fichier de modèle	Fichier de configuration PPP	Pour obtenir des instructions
`/etc/ppp/options.tmpl`	`/etc/ppp/options`	“Modèle `/etc/ppp/options.tmpl`” à la page 116
`/etc/ppp/options.ttya.tmpl`	`/etc/ppp/options.`*ttyname*	“Fichier modèle `options.ttya.tmpl`” à la page 118
`/etc/ppp/myisp-chat.tmpl`	Fichier portant le nom de votre choix pour contenir le script de discussion	“Modèle de script de discussion `/etc/ppp/myisp-chat.tmpl`” à la page 125
`/etc/ppp/peers/myisp.tmpl`	`/etc/ppp/peers/`*peer-name*	“Fichier modèle `/etc/ppp/peers/myisp.tmpl`” à la page 121

Si vous décidez d'utiliser l'un des fichiers modèles, veillez à le renommer comme le fichier de configuration PPP équivalent. La seule exception est le fichier de discussion modèle `/etc/ppp/myisp-chat.tmpl`. Vous pouvez nommer le script de discussion à votre convenance.

Configuration des périphériques sur la machine d'appel sortant

La première tâche du processus de configuration d'une machine PPP d'appel sortant consiste à configurer les périphériques sur la ligne série, c'est-à-dire le modem et le port série.

Remarque - Les tâches qui s'appliquent à un modem s'appliquent généralement à un adaptateur de terminal RNIS.

Avant d'effectuer la procédure ci-dessous, vous devez avoir effectué les opérations suivantes :

- Installation de la version de Oracle Solaris sur la machine d'appel sortant
- Identification de la vitesse optimale du modem
- Choix du port série à utiliser sur la machine d'appel sortant
- Obtention du mot de passe root pour la machine d'appel sortant

Pour plus d'informations sur la planification, reportez-vous à la section “Avant de configurer la machine d'appel sortant” à la page 30.

▼ Configuration du modem et du port série (machine d'appel sortant)

1. **Programmez le modem.**

   Bien qu'il existe une grande variété de types de modems, la plupart est livrée avec les paramètres appropriés pour Solaris PPP 4.0. La liste suivante présente les paramètres de base pour les modems qui utilisent Solaris PPP 4.0.

   - **DCD :** suivre les instructions de la porteuse
   - **DTR :** définir sur un niveau faible pour que le modem raccroche et accrocher le modem
   - **Contrôle de flux :** définir sur RTS/CTS pour un contrôle de flux matériel duplex intégral
   - **Séquences d'ttention :** désactiver

   Si vous rencontrez des problèmes pour configurer la liaison et pensez que le modem est défectueux, consultez d'abord la documentation du fabricant du modem. En outre, un certain nombre de sites Web se proposent de vous aider à programmer votre modem. Enfin, vous pouvez trouver des suggestions permettant de résoudre des problème liés au modem à la section “Diagnostic des problèmes de modem ” à la page 101.

2. **Branchez les câbles du modem au port série de la machine d'appel sortant et à la prise de téléphone.**

3. **Connectez-vous en tant qu'administrateur à la machine d'appel sortant.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

4. **Définissez la direction du modem pour les appels sortants uniquement.**

Configuration des communications sur la machine d'appel sortant

Les procédures décrites dans cette section expliquent comment configurer les communications transitant par la ligne série de la machine d'appel sortant. Avant de pouvoir appliquer ces procédures, vous devez configurer le modem et le port série, comme décrit à la section “Configuration du modem et du port série (machine d'appel sortant)” à la page 48.

Les tâches suivantes indiquent comment activer la machine d'appel sortant pour établir les communications avec le serveur d'appel entrant. L'amorce des communications est définie par les options contenues dans les fichiers de configuration PPP. Vous devez créer les fichiers suivants :

- `/etc/ppp/options`

- `/etc/ppp/options.`*ttyname*
- Script de discussion
- `/etc/ppp/peers/`*peer-name*

Solaris PPP 4.0 fournit des modèles pour les fichiers de configuration PPP, que vous pouvez ensuite adapter à vos besoins. Pour des informations détaillées sur ces fichiers, reportez-vous à la section “Fichiers modèles de liaison PPP commutée ” à la page 47.

▼ Définition des communications sur la ligne série

1. **Connectez-vous en tant qu'administrateur à la machine d'appel sortant.**
   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Créez un fichier appelé `/etc/ppp/options` avec l'entrée suivante :**

   ```
   lock
   ```

   Le fichier `/etc/ppp/options` permet de définir les paramètres généraux qui s'appliquent à toutes les communications sur la machine locale. L'option `lock` permet le verrouillage de type UUCP de la forme `/var/spool/locks/LC.xxx.yyy.zzz` .

   Remarque - Si la machine d'appel sortant ne dispose pas d'un fichier `/etc/ppp/options`, seul le superutilisateur peut exécuter la commande `pppd`. Toutefois, le fichier `/etc/ppp/options` peut être vide.

   Pour une description complète de `/etc/ppp/options`, reportez-vous à “Fichier de configuration `/etc/ppp/options`” à la page 115.

3. **(Facultatif) Créez un fichier appelé `/etc/ppp/options.`*ttyname* pour définir la manière dont les communications doivent être lancées à partir d'un port série spécifique.**
   L'exemple suivant illustre un fichier `/etc/ppp/options.` *ttyname* pour le port dont le nom de périphérique est `/dev/cua/a`.

   ```
   # cat /etc/ppp/options.cua.a
   crtscts
   ```

   L'option PPP `crtscts` indique au démon `pppd` d'activer le contrôle de flux matériel du port série a.
   Pour plus d'informations sur le fichier `/etc/ppp/options.ttyname`, reportez-vous à la section “Fichier de configuration`/etc/ppp/options.`*ttyname*” à la page 117.

4. **Définissez la vitesse du modem, comme décrit à la section “Définition de la vitesse du modem ” à la page 54.**

▼ Création des instructions pour l'appel d'un pair

Avant que la machine d'appel sortant puisse initialiser une liaison PPP, vous devez rassembler les informations concernant le serveur d'appel entrant qui doit devenir le pair. Elles vous permettent de créer le script de discussion, qui décrit la conversation réelle entre la machine d'appel sortant et le pair.

1. **Déterminez la vitesse à laquelle le modem de la machine d'appel sortant doit s'exécuter.**

   Pour plus d'informations, reportez-vous à la section “Configuration de la vitesse du modem pour une liaison commutée ” à la page 123.

2. **Recherchez les informations suivantes sur le site du serveur d'appel entrant :**

   - Numéro de téléphone du serveur
   - Protocole d'authentification utilisé, le cas échéant ;
   - Séquence de connexion requise par le pair pour le script de discussion.

3. **Recherchez les nom et adresse IP des serveurs de noms sur le site du serveur d'appel entrant.**

4. **Dans un script de discussion, fournissez les instructions permettant d'initialiser des appels vers un pair donné.**

   Par exemple, vous pouvez être amené à créer le script de discussion suivant, `/etc/ppp/mychat`, pour appeler le serveur d'appel entrant `myserver`.

```
SAY "Calling the peer\n"
        TIMEOUT 10
        ABORT BUSY
        ABORT 'NO CARRIER'
        ABORT ERROR
        REPORT CONNECT
        "" AT&F1&M5S2=255
        TIMEOUT 60
        OK ATDT1-123-555-1234
        CONNECT \c
        SAY "Connected; logging in.\n"
        TIMEOUT 5
        ogin:--ogin: pppuser
        TIMEOUT 20
        ABORT 'ogin incorrect'
        ssword: \qmypassword
```

```
"% " \c
SAY "Logged in.  Starting PPP on peer system.\n"
ABORT 'not found'
"" "exec pppd"
~ \c
```

Le script contient des instructions pour appeler un serveur d'appel entrant Oracle Solaris nécessitant une séquence de connexion. Vous trouverez la description de chaque instruction à la section “Script de discussion de base amélioré pour une connexion de type UNIX ” à la page 127. Pour plus de détails sur la création d'un script de discussion, reportez-vous à la section “Définition de la conversation sur la liaison commutée ” à la page 123.

Remarque - Vous n'appelez pas le script de discussion directement. Vous utilisez plutôt le nom de fichier du script de discussion en tant qu'argument de la commande `chat`, qui appelle le script.

Si un pair exécute Oracle Solaris ou un système d'exploitation similaire, envisagez d'utiliser le script de discussion précédent comme modèle pour les machines d'appel sortant.

▼ Définition de la connexion à un pair donné

1. **Connectez-vous en tant qu'administrateur à la machine d'appel sortant.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Mettez à jour les informations de référentiel pour les services du commutateur du service de noms et DNS.**

```
# svccfg
svc:> select network/dns/client
svc:/network/dns/client> setprop config/domain = astring: "example.com"
svc:/network/dns/client> setprop config/nameserver = net_address: "10.10.111.15"
svc:/network/dns/client> addpropval config/nameserver "10.10.130.8"
svc:/network/dns/client> select network/dns/client:default
svc:/network/dns/client:default > refresh
svc:/network/dns/client:default > validate
svc:/network/dns/client:default > select system/name-service/switch
svc:/system/name-service/switch > setprop config/host = astring: "files dns"
 svc:/system/name-service/switch:default > select system/name-service/switch:default
svc:/system/name-service/switch:default > refresh
svc:/system/name-service/switch:default > validate
# svcadm enable network/dns/client
# svcadm refresh system/name-service/switch
```

3. **Créez un fichier pour le pair.**

Par exemple, vous devez créer le fichier suivant pour définir le serveur d'appel entrant `myserver` :

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
noauth
connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
```

/dev/cua/a	Spécifie que le périphérique `/dev/cua/un` doit être utilisé en tant qu'interface série des appels vers `myserver`.
57600	Définit la vitesse de la liaison.
noipdefault	Spécifie que pour les transactions avec le pair `myserver`, la machine d'appel sortant possède au départ l'adresse IP 0.0.0.0. `myserver` affecte une adresse IP à la machine d'appel sortant pour chaque session commutée.
idle 120	Indique que la liaison doit expirer après une période d'inactivité de 120 secondes.
noauth	Spécifie qu'il n'est pas nécessaire que le pair `myserver` fournisse des informations d'authentification lorsqu'il négocie la connexion avec la machine d'appel sortant.
connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"	Spécifie l'option `connect` et ses arguments, y compris le numéro de téléphone du pair, et le script de discussion `/etc/ppp/mychat` avec les instructions d'appel.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- Pour configurer une autre machine d'appel sortant, reportez-vous à la section “Configuration du modem et du port série (machine d'appel sortant)” à la page 48.
- Pour tester la connectivité modem par appel sortant vers une autre machine, reportez-vous aux pages de manuel `cu`(1C) et `tip`(1). Ces utilitaires peuvent vous aider à vérifier que votre modem est configuré correctement. Ils vous permettent également de vérifier que vous pouvez établir une connexion à une autre machine.
- Pour en savoir plus sur les fichiers de configuration et les options, reportez-vous à la section “Utilisation des options PPP dans les fichiers et sur la ligne de commande ” à la page 111.

- Pour configurer un serveur d'appel entrant, reportez-vous à la section “Configuration des périphériques sur le serveur d'appel entrant ” à la page 53.

Configuration du serveur d'appel entrant

Les tâches décrites dans cette section permettent de configurer le serveur d'appel entrant. Le serveur d'appel entrant est un pair qui reçoit l'appel de la machine d'appel sortant via la liaison PPP. Ces tâches indiquent comment configurer le serveur d'appel entrant `myserver` présenté à la Figure 2-1, “Exemple de liaison commutée”.

Tâches de configuration du serveur d'appel entrant (liste des tâches)

TABLEAU 3-3 Liste des tâches de la configuration du serveur d'appel entrant

Tâche	Description	Pour obtenir des instructions
1. Collecte des informations de préconfiguration.	Rassemblez les données qui sont nécessaires avant de procéder à la configuration de la liaison : noms d'hôte des pairs, numéros de téléphone cible et vitesse des modems.	“Planification d'une liaison PPP commutée” à la page 30
2. Configuration du modem et du port série	Configurez le modem et le port série.	“Configuration du modem et du port série (serveur d'appel entrant)” à la page 54
3. Configuration des informations d'appel du pair	Configurez les environnements utilisateur et les options PPP pour toutes les machines d'appel sortant autorisées à appeler le serveur d'appel entrant.	“Configuration des utilisateurs du serveur d'appel entrant ” à la page 55
4. Configuration de la communication en ligne série	Configurez les caractéristiques de la transmission via la ligne série.	“Définition des communications sur la ligne série (serveur d'appel entrant) ” à la page 56

Configuration des périphériques sur le serveur d'appel entrant

La procédure suivante explique comment configurer le modem et le port série sur le serveur d'appel entrant.

Avant d'effectuer la procédure suivante, vous devez effectuer les activités suivantes sur le serveur d'appel entrant pair :

- Installation de la version Oracle Solaris
- Identification de la vitesse optimale du modem
- Choix du port série à utiliser

Configuration du modem et du port série (serveur d'appel entrant)

1. **Programmez le modem, comme indiqué dans la documentation du fabricant.**

   Pour d'autres suggestions, reportez-vous à la section “Configuration du modem et du port série (machine d'appel sortant)” à la page 48.

2. **Branchez le modem au port série sur le serveur d'appel entrant.**

3. **Connectez-vous en tant qu'administrateur au serveur d'appel entrant.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

4. **Définissez la direction du modem pour les appels entrants uniquement.**

Définition de la vitesse du modem

La procédure suivante explique comment définir la vitesse du modem pour un serveur d'appel entrant. La section “Configuration de la vitesse du modem pour une liaison commutée ” à la page 123 contient des suggestions à propos des vitesses à utiliser avec les ordinateurs Sun Microsystems.

1. **Connectez-vous au serveur d'appel entrant.**

2. **Utilisez la commande `tip` pour atteindre le modem.**

   Vous trouverez des instructions d'utilisation de la commande `tip` pour définir la vitesse du modem à la page de manuel `tip` (1).

3. **Configurez le modem pour une vitesse DTE fixe.**

4. **Verrouillez le port série pour cette vitesse à l'aide de `ttymon`.**

Voir aussi La liste ci-après fournit les références à des informations connexes.

- “Configuration du modem et du port série (serveur d'appel entrant)” à la page 54
- “Configuration des utilisateurs du serveur d'appel entrant ” à la page 55

Configuration des utilisateurs du serveur d'appel entrant

Le processus de configuration d'un serveur d'appel entrant consiste en partie à configurer des informations sur chaque appelant distant connu.

Avant de commencer les procédures décrites dans cette section, vous devez effectuer les opérations suivantes :

- Obtention des noms d'utilisateur UNIX pour tous les utilisateurs qui sont autorisés à se connecter à partir de machines distantes d'appel sortant
- Configuration du modem et de la ligne série, comme décrit dans la section “Configuration du modem et du port série (serveur d'appel entrant)” à la page 54.
- Définition d'une adresse IP dédiée à affecter aux appels entrants provenant d'utilisateurs distants. Envisagez de créer une adresse IP entrante dédiée si le nombre d'appelants potentiels dépasse le nombre de modems et de ports série sur le serveur d'appel entrant. Pour obtenir des informations complètes sur la création d'adresses IP dédiées, reportez-vous à la section “Création d'un schéma d'adressage IP pour appelants ” à la page 139.

▼ Configuration des utilisateurs du serveur d'appel entrant

1. **Connectez-vous en tant qu'administrateur au serveur d'appel entrant.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Créez un compte sur le serveur d'appel entrant pour chaque utilisateur PPP distant.**

   Pour obtenir des instructions sur la création d'un utilisateur, reportez-vous à la section “ Configuration et gestion des comptes utilisateur avec l’interface de ligne de commande ” du manuel “ Gestion des comptes utilisateur et des environnements utilisateur dans Oracle Solaris 11.2 ”.

3. **Pour chaque appelant, créez un fichier `$HOME/.ppprc` qui contient diverses options spécifiques à la session PPP de l'utilisateur.**

   Par exemple, vous pouvez créer le fichier `.ppprc` suivant pour `pppuser`.

```
# cat /export/home/pppuser/.ppprc
noccp
```

L'option `noccp` désactive le contrôle de compression sur la liaison.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- “Configuration des utilisateurs du serveur d'appel entrant ” à la page 55.
- “Définition des communications sur la ligne série (serveur d'appel entrant) ” à la page 56.

Configuration de la communication sur le serveur d'appel entrant

La tâche suivante indique comment activer le serveur d'appel entrant pour ouvrir les communications avec toutes les machines d'appel sortant. Les options définies dans les fichiers de configuration PPP suivants déterminent la manière dont les communications sont établies.

- `/etc/ppp/options`
- `/etc/ppp/options.`*ttyname*

Pour obtenir des informations détaillées sur ces fichiers, reportez-vous à la section “Utilisation des options PPP dans les fichiers et sur la ligne de commande ” à la page 111.

Avant de continuer, vous devez effectuer les opérations suivantes :

- Configuration du port série et du modem sur le serveur d'appel entrant, comme décrit à la section “Configuration du modem et du port série (serveur d'appel entrant)” à la page 54
- Configuration des informations sur les utilisateurs potentiels du serveur d'appel entrant, comme décrit à la section “Configuration des utilisateurs du serveur d'appel entrant ” à la page 55

▼ Définition des communications sur la ligne série (serveur d'appel entrant)

1. **Connectez-vous en tant qu'administrateur au serveur d'appel entrant.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Créez le fichier `/etc/ppp/options` avec l'entrée suivante.**

nodefaultroute

`nodefaultroute` indique qu'aucune session `pppd` sur le système local peut établir une route par défaut sans privilèges `root`.

Remarque - si le serveur d'appel entrant ne dispose pas d'un fichier `/etc/ppp/options`, seul le superutilisateur peut exécuter la commande `pppd`. Toutefois, le fichier `/etc/ppp/options` peut être vide.

---

3. **Créez le fichier `/etc/options.`*ttyname* pour définir la façon dont les appels reçus via le port série *ttyname* doivent être traités.**

   Le fichier `/etc/options.ttya` suivant définit la façon dont le port série `/dev/ttya` du serveur d'appel entrant doit traiter les appels entrants.

   ```
   :10.0.0.80
   xonxoff
   ```

`:10.0.0.80`	Affecte l'adresse IP 10.0.0.80 à tous les pairs qui appellent via le port série `ttya`.
`xonxoff`	Autorise la ligne série à traiter les communications en provenance des modems avec le contrôle de flux logiciel activé.

Voir aussi Si vous avez suivi l'ensemble des procédures décrites dans ce chapitre, vous avez terminé la configuration de la liaison commutée. La liste ci-après fournit les références à des informations connexes.

- Pour tester la connectivité modem par appel sortant vers une autre machine, reportez-vous aux pages de manuel `cu`(1C) et `tip`(1). Ces utilitaires peuvent vous aider à vérifier que votre modem est configuré correctement. Ils vous permettent également de vérifier que vous pouvez établir une connexion à une autre machine.
- Pour configurer des options supplémentaires pour le serveur d'appel entrant, reportez-vous à la section “Configuration du serveur d'appel entrant” à la page 53.
- Pour configurer plusieurs machines d'appel sortant, reportez-vous à la section “Configuration de la machine d'appel sortant” à la page 46.
- Pour que l'ordinateur distant appelle le serveur d'appel entrant, reportez-vous à la section “Appel du serveur d'appel entrant ” à la page 57.

Appel du serveur d'appel entrant

Pour établir une liaison PPP commutée, il suffit que la machine d'appel sortant appelle le serveur d'appel entrant. Vous pouvez demander à la machine d'appel sortant d'appeler le serveur

en spécifiant l'option `demand` dans les fichiers de configuration PPP locaux. Cependant, la méthode la plus courante pour établir la liaison est que l'utilisateur exécute la commande `pppd` sur la machine d'appel sortant.

Avant de passer à la tâche suivante, vous devez effectuer l'une des opérations suivantes ou les deux :

- Configuration de la machine d'appel sortant, comme décrit à la section “Configuration de la machine d'appel sortant” à la page 46
- Configuration du serveur d'appel entrant, comme décrit à la section “Configuration du serveur d'appel entrant” à la page 53

▼ Appel du serveur d'appel entrant

1. **Connectez-vous à la machine d'appel sortant à l'aide de votre compte utilisateur standard, pas `root`.**

2. **Appelez le serveur d'appel entrant en exécutant la commande `pppd`.**
   Par exemple, la commande suivante établit une liaison entre la machine d'appel sortant et le serveur d'appel entrant `myserver` :

   ```
   % pppd 57600 call myserver
   ```

`pppd`	Démarre l'appel en appelant le démon `pppd`
`57600`	Définit la vitesse de la ligne entre l'hôte et le modem
`call myserver`	Appelle l'option `call` de la commande `pppd`. Ensuite, `pppd` lit les options dans le fichier `/etc/ppp/peers/myserver`, créé à la section “Définition de la connexion à un pair donné” à la page 51

3. **Contactez un hôte sur le réseau du serveur, par exemple, l'hôte `lindyhop` illustré à la Figure 2-1, “Exemple de liaison commutée” :**

   ```
   ping lindyhop
   ```

   Si la liaison ne fonctionne pas correctement, reportez-vous au Chapitre 7, Dépannage de problèmes courants du Point-to-Point Protocol.

4. **Mettez fin à la session PPP :**

   ```
   % pkill -x pppd
   ```

Voir aussi Si vous avez suivi l'ensemble des procédures décrites dans ce chapitre, vous avez terminé la configuration de la liaison commutée. La liste ci-après fournit les références à des informations connexes.

- Pour que tous les utilisateurs commencent à travailler sur leur machine d'appel sortant, reportez-vous à la section “Appel du serveur d'appel entrant” à la page 58.
- Pour résoudre les problèmes de liaison, reportez-vousChapitre 7, Dépannage de problèmes courants du Point-to-Point Protocol.
- Pour en savoir plus sur les fichiers et les options utilisés dans ce chapitre, reportez-vous à la section “Utilisation des options PPP dans les fichiers et sur la ligne de commande ” à la page 111.

♦ ♦ ♦ CHAPITRE 4

Configuration d'une liaison Point-to-Point Protocol de ligne spécialisée

Ce chapitre explique comment configurer une liaison PPP entre pairs par le biais d'une ligne spécialisée. Les sections principales sont les suivantes :

Configuration d'une ligne spécialisée (liste des tâches)

Les liaisons de lignes spécialisées sont relativement faciles à configurer par rapport aux liaisons commutées. Dans la plupart des cas, il n'est pas nécessaire de configurer la CSU/DSU, les services ni l'authentification. Si vous devez configurer la CSU/DSU, reportez-vous à la documentation fournie par le fabricant pour obtenir de l'aide sur cette tâche complexe.

La liste des tâches répertoriées dans le tableau suivant décrit toutes les tâches que comporte la configuration d'une liaison de base par le biais d'une ligne spécialisée.

Remarque - Certains types de lignes spécialisées requièrent que la CSU/DSU "appelle" l'adresse du pair opposé. Par exemple, Frame Relay utilise le service SVC (Switched Virtual Circuits, circuits virtuels commutés) ou Switched 56.

TABLEAU 4-1 Liste des tâches de la configuration de la liaison de ligne spécialisée

Tâche	Description	Pour obtenir des instructions
1. Collecte d'informations de pré-configuration	Rassemblez les données qui sont nécessaires avant de procéder à la configuration de la liaison.	“Informations à rassembler pour la liaison de ligne spécialisée” à la page 34
2. Configuration du matériel de la ligne spécialisée	Assemblez la CSU/DSU et la carte d'interface synchrone.	“Configuration de périphériques synchrones ” à la page 62
3. Configuration de la carte d'interface, si nécessaire	Configurez le script d'interface à utiliser à l'initialisation de la ligne spécialisée.	“Configuration de périphériques synchrones ” à la page 62

Tâche	Description	Pour obtenir des instructions
4. Configuration des informations relatives au pair distant	Définissez le mode de fonctionnement des communications entre la machine locale et le pair distant.	“Configuration d'une machine sur une ligne spécialisée ” à la page 64
5. Initialisation de la ligne spécialisée	Configurez votre machine pour que la liaison PPP démarre sur la ligne spécialisée dans le cadre du processus d'initialisation.	“Configuration d'une machine sur une ligne spécialisée ” à la page 64

Configuration des périphériques synchrones sur la ligne spécialisée

La tâche décrite dans cette section consiste à configurer l'équipement requis par la topologie de ligne spécialisée présentée à la section “Exemple de configuration d'une liaison de ligne spécialisée” à la page 34. Les périphériques synchrones qui doivent se connecter à la ligne spécialisée incluent l'interface et le modem.

Prérequis à la configuration des périphériques synchrones

Avant d'effectuer la procédure suivante, vous devez disposer des éléments suivants :

- Ligne spécialisée en fonctionnement, installée sur votre site par le fournisseur
- Unité synchrone (CSU/DSU)
- Version de Oracle Solaris installée sur votre système
- Carte d'interface synchrone du type requis par votre système

▼ Configuration de périphériques synchrones

1. **Installez physiquement la carte d'interface dans la machine locale, si nécessaire.**
   Suivez les instructions décrites dans la documentation du fabricant.

2. **Connectez les câbles reliant la CSU/DSU à l'interface.**
   Au besoin, branchez les câbles de la CSU/DSU au connecteur de la ligne spécialisée ou à un connecteur similaire.

3. **Configurez la CSU/DSU, comme indiqué dans la documentation fournie par le fabricant ou fournisseur réseau.**

Remarque - Le fournisseur auquel vous avez loué la ligne spécialisée peut fournir et configurer la CSU/DSU pour votre liaison.

4. **Configurez la carte d'interface, si nécessaire, comme indiqué dans la documentation de l'interface.**

   La configuration de la carte d'interface implique la création d'un script de démarrage pour l'interface. Le routeur de LocalCorp dans la configuration de la ligne spécialisée, illustrée à la Figure 2-2, “Exemple d'une configuration de ligne spécialisée”, utilise une carte d'interface HSI/P.

   Le script suivant, `hsi conf-`, lance l'interface HSI/P.

```
#!/bin/ksh
/opt/SUNWconn/bin/hsip_init hihp1 speed=1536000 mode=fdx loopback=no \
nrzi=no txc=txc rxc=rxc txd=txd rxd=rxd signal=no 2>&1 > /dev/null
```

`hihp1`	Indique que HSI/P est le port synchrone utilisé
`speed=1536000`	Indique la vitesse de la CSU/DSU

Voir aussi Pour configurer la machine locale sur la ligne spécialisée, reportez-vous à la section “Configuration d'une machine sur une ligne spécialisée ” à la page 64.

Configuration d'une machine sur la ligne spécialisée

La procédure décrite dans cette section explique comment configurer un routeur en tant que pair local situé à votre extrémité de la ligne spécialisée. La tâche utilise la ligne spécialisée présentée à la section “Exemple de configuration d'une liaison de ligne spécialisée” à la page 34.

Prérequis à la configuration de la machine locale sur une ligne spécialisée

Avant d'effectuer la procédure ci-dessous, vous devez réaliser les opérations suivantes :

- Définition et configuration des périphériques synchrones de la liaison, comme décrit à la section “Configuration des périphériques synchrones sur la ligne spécialisée” à la page 62
- Obtention du mot de passe root de la machine locale sur la ligne spécialisée
- Configuration de la machine locale en tant que routeur sur le ou les réseaux afin d'utiliser les services du fournisseur de la ligne spécialisée

Configuration d'une machine sur une ligne spécialisée

1. **Connectez-vous en tant qu'administrateur à la machine locale (routeur).**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Ajoutez une entrée pour le pair distant dans le fichier `/etc/hosts` du routeur.**

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
192.168.130.10  local2-peer        loghost
192.168.130.11  local1-net
10.0.0.25        farISP
```

   L'exemple de fichier `/etc/hosts` est pour le routeur local de la société fictive LocalCorp. Notez l'adresse IP et le nom d'hôte pour le pair distant `farISP` du fournisseur de service.

3. **Créez le fichier `/etc/ppp/peers/`*peer-name* pour conserver des informations à propos du pair de l'opérateur.**

   Pour cet exemple de liaison de ligne spécialisée, créez le fichier `/etc/ppp/peers/farISP`.

```
# cat /etc/ppp/peers/farISP
init '/etc/ppp/conf_hsi'
local
/dev/hihp1
sync
noauth
192.168.130.10:10.0.0.25
passive
persist
noccp
nopcomp
novj
noaccomp
```

   Le tableau suivant décrit les options et les paramètres utilisés dans le fichier `/etc/ppp/peers/farISP`.

Option	Définition
`init '/etc/ppp/conf_hsi'`	Initialise la liaison. `init` configure ensuite les interfaces HSI à l'aide des paramètres du script `/etc/ppp/conf_hsi`.

Option	Définition
`local`	Indique au démon `pppd` de ne pas modifier l'état du signal DTR (Data Terminal Ready). Indique également à `pppd` d'ignorer le signal d'entrée DCD (Data Carrier Detect).
`/dev/hihp1`	Donne le nom de périphérique de l'interface synchrone.
`sync`	Etablit le codage synchrone de la liaison.
`noauth`	Etablit que le système local n'a pas besoin d'exiger du pair qu'il s'authentifie. Cependant, le pair peut toujours exiger l'authentification.
`192.168.130.10:10.0.0.25`	Définit les adresses IP du pair local et du pair distant, séparées par un signe deux-points.
`passive`	Indique au démon `pppd` résidant sur la machine locale de s'interrompre et d'attendre le démarrage du pair, après avoir établi le nombre maximal de demandes de configuration LCP.
`persist`	Indique au démon `pppd` d'essayer de redémarrer la liaison après l'arrêt d'une connexion.
`noccp, nopcomp, novj, noaccomp`	Désactive CCP (Compression Control Protocol), la compression du champ protocole, la compression Van Jacobson et la compression de champ adresse et contrôle, respectivement. Ces formes de compression accélèrent les transmissions sur une liaison commutée mais peuvent ralentir une ligne spécialisée.

4. Créez un script d'initialisation appelé `demand`, qui crée la liaison PPP dans le cadre du processus de démarrage.

```
# cat /etc/ppp/demand
#!/bin/sh
if [ -f /system/volatile/ppp-demand.pid ] &&
   /usr/bin/kill -s 0 `/bin/cat /system/volatile/ppp-demand.pid`
then
        :
else
        /usr/bin/pppd call farISP
fi
```

Le script `demand` contient la commande `pppd` permettant d'établir une liaison de ligne spécialisée. Le tableau suivant décrit le contenu de `$PPPDIR/demand`.

Exemple de code	Explication
`if [ -f /system/volatile/ppp-demand.pid ] && /usr/bin/kill -s 0 "/bin/cat /system/volatile/ppp-demand.pid"`	Ces lignes vérifient l'exécution de la commande `pppd`. Si `pppd` est en cours d'exécution, il n'est pas nécessaire de la démarrer.
`/usr/bin/pppd call farISP`	Cette ligne lance `pppd`. `pppd` lit les options de `/etc/ppp/options`. De plus, l'option `call farISP` sur la ligne de commande entraîne la lecture de `/etc/ppp/peers/farISP`.

Le script de démarrage Solaris PPP 4.0 `/etc/rc2.d/S47pppd` appelle le script `demand` dans le cadre du processus d'initialisation. Les lignes suivantes dans `/etc/rc2.dS47pppd` recherchent la présence d'un fichier appelé `$PPPDIR/demand`.

```
if [ -f $PPPDIR/demand ]; then
            . $PPPDIR/demand
    fi
```

S'il est trouvé, `$PPPDIR/demand` est exécuté. Au cours de l'exécution de `$PPPDIR/demand`, la liaison est établie.

Remarque - Pour atteindre les machines résidant en dehors du réseau local, demandez aux utilisateurs d'exécuter `telnet`, `ftp`, `rsh` ou des commandes similaires.

Voir aussi

Si vous avez suivi l'ensemble des procédures décrites dans ce chapitre, vous avez terminé la configuration de la liaison de ligne spécialisée. La liste ci-après fournit les références à des informations connexes.

- Pour obtenir des informations sur le dépannage, reportez-vous à la section “Correction des problèmes des lignes spécialisées” à la page 108.
- Pour en savoir plus sur les fichiers et les options utilisés dans ce chapitre, reportez-vous à la section “Utilisation des options PPP dans les fichiers et sur la ligne de commande ” à la page 111.

♦ ♦ ♦ CHAPITRE 5

Configuration de l'authentification Point-to-Point Protocol

Ce chapitre contient les tâches de la configuration de l'authentification PPP. Voici la liste des sujets abordés :

- “Configuration de l'authentification PAP” à la page 68
- “Configuration de l'authentification CHAP” à la page 76

Les procédures décrivent la mise en oeuvre de l'authentification sur une liaison commutée, car les liaisons commutées sont plus susceptibles d'être configurées pour l'authentification que les lignes spécialisées. Vous pouvez configurer l'authentification sur des lignes spécialisées, si la stratégie de sécurité de votre entreprise l'exige. Pour mettre en oeuvre l'authentification sur des lignes spécialisées, utilisez les tâches de ce chapitre comme directives.

Si vous souhaitez utiliser l'authentification PPP, mais que vous ne savez pas quel protocole utiliser, consultez la section “Raisons de l'utilisation de l'authentification PPP” à la page 24. Vous trouverez des informations plus détaillées sur l'authentification PPP dans la page de manuel `pppd`(1M) et à la section “Authentification des appelants sur une liaison” à la page 133.

Configuration de l'authentification PPP (liste des tâches)

Cette section contient la liste des tâches qui vous permettront d'accéder rapidement aux procédures de l'authentification PPP.

TABLEAU 5-1 Liste des tâches de l'authentification PPP générale

Tâche	Description	Pour obtenir des instructions
Configuration de l'authentification PAP	Utilisez ces procédures pour activer l'authentification PAP sur un serveur d'appel entrant et une machine d'appel sortant.	“Configuration de l'authentification PAP (liste des tâches) ” à la page 68
Configuration de l'authentification CHAP	Utilisez ces procédures pour activer l'authentification CHAP sur un serveur d'appel entrant et une machine d'appel sortant.	“Configuration de l'authentification CHAP (liste des tâches) ” à la page 76

Configuration de l'authentification PAP

Les tâches décrites dans cette section expliquent comment mettre en oeuvre l'authentification sur une liaison PPP à l'aide du protocole PAP (Password Authentication Protocol, protocole d'authentification par mot de passe). Les tâches utilisent l'exemple de la section “Exemples de configuration d'authentification PPP ” à la page 37 afin d'illustrer un scénario PAP qui fonctionne pour une liaison commutée. Utilisez les instructions comme base pour la mise en oeuvre de l'authentification PAP sur votre site.

Avant de réaliser les procédures suivantes, vous devez effectuer les opérations ci-dessous :

- Définissez et testez la liaison commutée entre le serveur d'appel entrant et les machines d'appel sortant appartenant à des appelants de confiance.
- Dans l'idéal, pour l'authentification du serveur d'appel entrant, obtenez l'autorisation de superutilisateur pour la machine gérant la base de données de mots de passe réseau, par exemple, dans les fichiers locaux, LDAP ou NIS.
- Obtenez les droits de superutilisateur pour la machine locale, qu'il s'agisse du serveur d'appel entrant ou de la machine d'appel sortant.

Configuration de l'authentification PAP (liste des tâches)

Utilisez la liste des tâches suivante pour accéder rapidement aux tâches relatives à PAP pour le serveur d'appel entrant et les appelants de confiance sur les machines d'appel sortant.

TABLEAU 5-2 Liste des tâches de l'authentification PAP (serveur d'appel entrant)

Tâche	Description	Pour obtenir des instructions
1. Collecte des informations de préconfiguration.	Rassemblez les noms d'utilisateur et autres données nécessaires à l'authentification.	“Planification de l'authentification sur une liaison” à la page 36
2. Mise à jour de la base de données de mots de passe, si nécessaire	Assurez-vous que tous les appelants figurent dans la base de données de mots de passe du serveur.	“Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant) ” à la page 69
3. Création de la base de données PAP	Créez des informations d'identification de sécurité pour tous les appelants potentiels dans `/etc/ppp/pap-secrets`.	“Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant) ” à la page 69
4. Modification des fichiers de configuration PPP	Ajoutez des options spécifiques à PAP dans les fichiers `/etc/ppp/options` et `/etc/ppp/peers/`*peer-name*.	“Ajout de la prise en charge PAP dans les fichiers de configuration PPP (serveur d'appel entrant)” à la page 71

TABLEAU 5-3 Liste des tâches pour l'authentification PAP (machine d'appel sortant)

Tâche	Description	Pour obtenir des instructions
1. Collecte des informations de préconfiguration.	Rassemblez les noms d'utilisateur et autres données nécessaires à l'authentification.	“Planification de l'authentification sur une liaison” à la page 36
2. Création de la base de données PAP pour la machine de l'appelant de confiance	Créez les informations d'identification de sécurité pour l'appelant de confiance et, si nécessaire, pour les autres utilisateurs qui appellent la machine d'appel sortant, dans `/etc/ppp/pap-secrets`.	“Configuration des informations d'authentification PAP pour les appelants de confiance ” à la page 73
3. Modification des fichiers de configuration PPP	Ajoutez des options spécifiques à PAP dans les fichiers `/etc/ppp/options` et `/etc/ppp/peers/`*peer-name*.	“Ajout de la prise en charge PAP dans les fichiers de configuration PPP (machine d'appel sortant)” à la page 74

Configuration de l'authentification PAP sur le serveur d'appel entrant

Pour configurer l'authentification PAP, vous devez effectuer les opérations suivantes :

- Création d'une base de données d'informations d'identification PAP
- Modification des fichiers de configuration PPP pour la prise en charge PAP

▼ Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant)

Cette procédure modifie le fichier `/etc/ppp/pap-secrets`, qui contient les informations d'identification de sécurité PAP permettant d'authentifier les appelants sur la liaison. Le fichier `/etc/ppp/pap-secrets` doit exister sur les deux machines sur une liaison PPP.

L'exemple de configuration PAP présenté à la Figure 2-3, “Exemple d'un scénario d'authentification PAP (travail à domicile) ” utilise l'option `login` de PAP. Si vous envisagez d'utiliser cette option, vous devrez peut-être mettre à jour la base de données de mots de passe de votre réseau. Pour plus d'informations sur l'option `login`, reportez-vous à la section “Utilisation de l'option `login` avec `/etc/ppp/pap-secrets`” à la page 136.

1. **Dressez la liste des éventuels appelants de confiance. Les appelants de confiance sont des utilisateurs auxquels vous accordez l'autorisation d'appeler le serveur d'appel entrant à partir de leur machine distante.**

2. **Vérifiez que chaque appelant de confiance possède déjà un nom d'utilisateur et un mot de passe UNIX dans la base de données des mots de passe du serveur d'appel entrant.**

Remarque - La vérification est particulièrement importante pour l'exemple de configuration PAP, qui utilise l'option `login` de PAP pour authentifier les appelants. Si vous choisissez de ne pas appliquer l'option `login` pour PAP, les noms d'utilisateur PAP des appelants ne doivent pas forcément correspondre à leurs noms d'utilisateur UNIX. Pour plus d'informations sur le fichier `/etc/ppp/pap-secrets` standard, reportez-vous à “Fichier `/etc/ppp/pap-secrets`” à la page 133.

Effectuez les opérations suivantes si un appelant de confiance potentiel ne possède pas un mot de passe et un nom d'utilisateur UNIX.

   a. **Confirmez avec leurs responsables que les appelants que vous ne connaissez pas personnellement sont autorisés à accéder au serveur d'appel entrant.**

   b. **Créez des noms d'utilisateur et mots de passe UNIX pour ces appelants, en conformité avec la stratégie de sécurité de votre entreprise.**

3. **Connectez-vous en tant qu'administrateur au serveur d'appel entrant.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

4. **Modifiez le fichier `/etc/ppp/pap-secrets`.**

   Cette version fournit un fichier `pap-secrets` dans `/etc/ppp` qui contient des commentaires relatifs à l'utilisation de l'authentification PAP mais pas d'options. Vous pouvez ajouter les options suivantes à la fin des commentaires.

```
user1      myserver       ""          *
user2      myserver       ""          *
myserver   user2          serverpass  *
```

   Pour utiliser l'option `login` de `/etc/ppp/pap-secrets`, vous devez taper le nom d'utilisateur UNIX de chaque appelant de confiance. Lorsqu'un jeu de guillemets doubles (““) s'affiche dans le troisième champ, le mot de passe pour l'appelant est recherché dans la base de données des mots de passe du serveur.

   L'entrée `myserver * serverpass *` contient le nom d'utilisateur et le mot de passe PAP pour le serveur d'appel entrant. Dans la Figure 2-3, “Exemple d'un scénario d'authentification PAP (travail à domicile) ”, l'appelant de confiance `user2` requiert l'authentification de pairs distants. Par conséquent, le fichier de `myserver`, `/etc/ppp/pap-secrets`, contient les informations d'identification PAP à utiliser lorsqu'une liaison est établie avec `user2`.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- “Modification des fichiers de configuration PPP pour PAP (serveur d'appel entrant)” à la page 71
- “Configuration de l'authentification PAP pour les appelants de confiance (machines d'appel sortant)” à la page 72

Modification des fichiers de configuration PPP pour PAP (serveur d'appel entrant)

Les tâches décrites dans cette section expliquent comment mettre à jour les fichiers de configuration PPP existants pour la prise en charge de l'authentification PAP sur le serveur d'appel entrant.

▼ Ajout de la prise en charge PAP dans les fichiers de configuration PPP (serveur d'appel entrant)

La procédure utilise comme exemples les fichiers de configuration PPP présentés à la section “Définition des communications sur la ligne série (serveur d'appel entrant) ” à la page 56.

1. **Connectez-vous en tant qu'administrateur au serveur d'appel entrant.**
   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Ajoutez des options d'authentification dans le fichier `/etc/ppp/options`.**
   Par exemple, ajoutez les options en gras dans un fichier `/etc/ppp/options` pour mettre en oeuvre l'authentification PAP :

```
lock
auth
login
nodefaultroute
proxyarp
ms-dns 10.0.0.1
idle 120
```

`auth`	Spécifie que le serveur doit authentifier les appelants avant d'établir la liaison.
`login`	Spécifie que l'appelant distant doit être authentifié à l'aide des services d'authentification d'utilisateur UNIX standard.

`nodefaultroute`	Indique qu'aucune session `pppd` sur le système local ne peut établir une route par défaut sans privilèges `root`.
`proxyarp`	Ajoute une entrée dans la table ARP (Address Resolution Protocol, protocole de résolution d'adresse) du système, qui indique l'adresse IP du pair et l'adresse Ethernet du système. Avec cette option, le pair semble se trouver sur le réseau Ethernet local aux autres systèmes.
`ms-dns 10.0.0.1`	Active `pppd` pour fournir l'adresse DNS (Domain Name Server) `10.0.0.1` au client
`idle 120`	Spécifie que les utilisateurs inactifs sont déconnectés après deux minutes.

3. **Dans le fichier `/etc/ppp/options.cua.a` , ajoutez l'adresse suivante pour l'utilisateur `cua/a`.**

```
:10.0.0.2
```

4. **Dans le fichier `/etc/ppp/options.cua.b` , ajoutez l'adresse suivante pour l'utilisateur `cua/b`.**

```
:10.0.0.3
```

5. **Dans le fichier `/etc/ppp/pap-secrets`, ajoutez l'entrée suivante.**

```
*     *       ""      *
```

Remarque - L'option `login`, comme décrit précédemment, fournit l'authentification utilisateur nécessaire. Cette entrée dans le fichier `/etc/ppp/pap-secrets` constitue la méthode normale d'activer PAP avec l'option `login`.

Voir aussi Pour configurer les informations d'authentification PAP des appelants de confiance du serveur d'appel entrant, reportez-vous à la section “Configuration de l'authentification PAP pour les appelants de confiance (machines d'appel sortant)” à la page 72.

Configuration de l'authentification PAP pour les appelants de confiance (machines d'appel sortant)

Cette section présente les tâches de configuration de l'authentification PAP sur les machines d'appel sortant des appelants de confiance. En tant qu'administrateur système, vous pouvez configurer l'authentification PAP sur les systèmes avant leur distribution aux appelants potentiels. Vous pouvez également affecter les tâches de cette section aux appelants distants, s'ils disposent déjà de leur machine.

La configuration PAP pour les appelants de confiance implique deux tâches :

- Configuration des informations d'identification de sécurité PAP des appelants
- Configuration des machines d'appel sortant des appelants pour prendre en charge l'authentification PAP

▼ Configuration des informations d'authentification PAP pour les appelants de confiance

Cette procédure indique comment configurer les informations d'identification PAP pour deux appelants de confiance, dont l'un requiert les informations d'authentification des pairs distants. Elle implique que vous, l'administrateur système, créez les informations d'identification PAP sur les machines d'appel sortant des appelants de confiance.

1. **Connectez-vous en tant qu'administrateur à la machine d'appel sortant.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

   Utilisez l'exemple de configuration PAP présenté à la Figure 2-3, "Exemple d'un scénario d'authentification PAP (travail à domicile) " et partez du principe que la machine d'appel sortant appartient à l'utilisateur `user1`.

2. **Modifiez la base de données des secrets PAP pour l'appelant.**

   cette version fournit un fichier `/etc/ppp/pap-secrets` qui contient des commentaires utiles mais aucune option. Vous pouvez ajouter les options suivantes à ce fichier `/etc/ppp/pap-secrets`.

   ```
   user1    myserver  pass1    *
   ```

   Notez que le mot de passe `pass1` de l'utilisateur `user1` est transmis au format ASCII lisible par la liaison. `myserver` est le nom de l'appelant `user1` pour le pair.

3. **Connectez-vous en tant qu'administrateur à la machine d'appel sortant.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

   Utilisez l'exemple d'authentification PAP et supposez que cette machine d'appel sortant appartient à l'appelant `user2`.

4. **Modifiez la base de données des secrets PAP pour l'appelant.**

Vous pouvez ajouter les options suivantes à la fin du fichier `/etc/ppp/pap-secrets`.

```
user2     myserver   pass2       *
myserver  user2      serverpass  *
```

Dans cet exemple, `/etc/ppp/pap-secrets` comporte deux entrées. La première entrée contient les informations d'identification de sécurité PAP que `user2` transmet au serveur d'appel entrant `myserver` pour l'authentification.

`user2` exige les informations d'identification PAP du serveur d'appel entrant dans le cadre de la négociation de la liaison. Par conséquent, le fichier `/etc/ppp/pap-secrets` contient également les informations d'identification PAP attendues de `myserver` sur la deuxième ligne.

Remarque - Dans la mesure où la plupart des FAI ne fournissent pas d'informations d'authentification, le scénario précédent peut manquer de réalisme en ce qui concerne les communications avec un FAI.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- “Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant) ” à la page 69
- “Configuration des informations d'authentification PAP pour les appelants de confiance ” à la page 73

Modification des fichiers de configuration PPP pour PAP (machine d'appel sortant)

Les tâches suivantes expliquent comment mettre à jour les fichiers de configuration PPP existants pour la prise en charge de l'authentification PAP sur les machines d'appel sortant des appelants de confiance.

La procédure utilise les paramètres suivants pour configurer l'authentification PAP sur la machine d'appel sortant qui appartient à `user2`, présenté à la Figure 2-3, “Exemple d'un scénario d'authentification PAP (travail à domicile) ”. L'utilisateur `user2` exige des appelants entrants de s'authentifier, appels de `myserver` compris.

▼ Ajout de la prise en charge PAP dans les fichiers de configuration PPP (machine d'appel sortant)

Cette procédure utilise comme exemples les fichiers de configuration PPP présentés à la section “Définition des communications sur la ligne série ” à la page 49. Elle permet de configurer la

machine d'appel sortant qui appartient à `user2`, comme indiqué à la Figure 2-3, “Exemple d'un scénario d'authentification PAP (travail à domicile) ”.

1. **Connectez-vous en tant que superutilisateur à la machine d'appel sortant.**

2. **Modifiez le fichier `/etc/ppp/options`.**

   Le fichier `/etc/ppp/options` suivant contient des options pour la prise en charge PAP, indiquées en gras.

```
# cat /etc/ppp/options
lock
name user2
auth
require-pap
```

   name user2 — Définit `user2` comme nom PAP de l'utilisateur sur la machine locale. Si l'option `login` est utilisée, le nom PAP doit être le même que celui de l'utilisateur UNIX dans la base de données de mots de passe.

   auth — Indique que la machine d'appel sortant doit authentifier les appelants avant d'établir la liaison.

   Remarque - Cette machine d'appel sortant exige l'authentification de ses pairs, bien que la plupart des machines d'appel sortant n'aient pas cette exigence. Les deux cas sont acceptables.

   require-pap — Exige les informations d'identification PAP du pair.

3. **Créez un fichier `/etc/ppp/peers/`*peer-name* pour la machine distante `myserver`.**

   L'exemple suivant indique comment ajouter la prise en charge PAP au fichier `/etc/ppp/peers/myserver` créé à la section “Définition de la connexion à un pair donné” à la page 51.

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user user2
remotename myserver
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

   Les nouvelles options en gras ajoutent les exigences PAP pour le pair `myserver`.

   user user2 — Définit `user2` comme le nom d'utilisateur de la machine locale.

   remotename myserver — Définit `myserver` comme un pair qui requiert les informations d'authentification de la machine locale.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- Pour tester la configuration de l'authentification PAP en appelant le serveur d'appel entrant, reportez-vous à la section “Appel du serveur d'appel entrant” à la page 58.
- Pour en savoir plus sur l'authentification PAP, reportez-vous à la section “Protocole d'authentification par mot de passe (PAP)” à la page 133.

Configuration de l'authentification CHAP

Les tâches décrites dans cette section expliquent comment mettre en oeuvre l'authentification sur une liaison PPP à l'aide du protocole CHAP (Challenge-Handshake Authentication Protocol, protocole d'authentification par défi-réponse). Les tâches utilisent l'exemple de la Figure 2-4, “Exemple d'un scénario d'authentification CHAP (appel d'un réseau privé) ” afin d'illustrer un scénario CHAP qui fonctionne pour une liaison commutée sur un réseau privé. Utilisez les instructions comme base pour la mise en oeuvre de l'authentification CHAP sur votre site.

Avant d'effectuer les procédures ci-dessous, vous devez réaliser les opérations suivantes :

- Définissez et testez la liaison commutée entre le serveur d'appel entrant et les machines d'appel sortant appartenant à des appelants de confiance.
- Obtenez les autorisations de superutilisateur pour la machine locale, qu'il s'agisse du serveur d'appel entrant ou de la machine d'appel sortant.

Configuration de l'authentification CHAP (liste des tâches)

TABLEAU 5-4 Liste des tâches de l'authentification CHAP (serveur d'appel entrant)

Tâche	Description	Pour obtenir des instructions
1. Affectation des secrets CHAP à tous les appelants de confiance	Créez les secrets CHAP des appelants ou demandez aux appelants qu'ils les créent.	“Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)” à la page 77
2. Création de la base de données chap-secrets	Ajoutez les informations d'identification de sécurité pour tous les appelants de confiance dans le fichier `/etc/ppp/chap-secrets`.	“Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)” à la page 77
3. Modification des fichiers de configuration PPP	Ajoutez des options spécifiques à CHAP dans les fichiers `/etc/ppp/options` et `/etc/ppp/peers/`*peer-name*.	“Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (serveur d'appel entrant)” à la page 79

TABLEAU 5-5 Liste des tâches pour l'authentification CHAP (machine d'appel sortant)

Tâche	Description	Pour obtenir des instructions
1. Création de la base de données CHAP pour la machine de l'appelant de confiance	Créez les informations d'identification de sécurité pour l'appelant de confiance et, si nécessaire, pour les autres utilisateurs qui appellent la machine d'appel sortant, dans `/etc/ppp/chap-secrets`.	“Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)” à la page 77
2. Modification des fichiers de configuration PPP	Ajoutez des options spécifiques à CHAP dans le fichier `/etc/ppp/options`.	“Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (machine d'appel sortant)” à la page 81

Configuration de l'authentification CHAP sur le serveur d'appel entrant

La première tâche de la configuration de l'authentification CHAP consiste à modifier le fichier `/etc/ppp/chap-secrets`. Ce fichier contient le informations d'identification de sécurité CHAP utilisées pour authentifier les appelants sur la liaison.

Remarque - Les mécanismes d'authentification PAM ou UNIX ne fonctionnent pas avec CHAP. Par exemple, vous ne pouvez pas utiliser l'option `login` PPP comme décrit dans la section “Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant) ” à la page 69. Si votre scénario d'authentification nécessite l'authentification de type UNIX ou PAM, choisissez plutôt PAP.

La procédure suivante met en oeuvre l'authentification CHAP pour un serveur d'appel entrant dans un réseau privé. La liaison PPP est la seule connexion au monde extérieur. Seuls les appelants autorisés par les gestionnaires du réseau (y compris l'administrateur système, éventuellement) peuvent accéder au réseau.

▼ Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)

1. **Dressez la liste des noms d'utilisateur de tous les appelants de confiance.**

   Les appelants de confiance incluent tous les utilisateurs auxquels l'autorisation d'appeler le réseau privé a été accordée.

2. **Affectez un secret CHAP à chaque utilisateur.**

Remarque - Assurez-vous de choisir un secret CHAP difficile à deviner. Aucune autre restriction n'est appliquée sur le contenu du secret CHAP.

La méthode d'attribution des secrets CHAP dépend de la stratégie de sécurité de votre site. Soit vous avez la responsabilité de créer les secrets, soit les appelants doivent créer leurs secrets eux-mêmes. Si vous n'êtes pas responsable de l'affectation des secrets CHAP, veillez à vous procurer les secrets CHAP qui ont été créés par, ou pour, chaque appelant de confiance.

3. **Connectez-vous en tant qu'administrateur au serveur d'appel entrant.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

4. **Modifiez le fichier `/etc/ppp/chap-secrets`.**

   Cette version inclut un fichier `/etc/ppp/chap-secrets` qui contient des commentaires utiles, mais aucune option. Vous pouvez ajouter les options suivantes pour le serveur `CallServe` à la fin du fichier `/etc/ppp/chap-secrets`.

   ```
   account1  CallServe   key123   *
   account2  CallServe   key456   *
   ```

   `key123` est le secret CHAP pour l'appelant de confiance `account1`.

   `key456` est le secret CHAP pour l'appelant de confiance `account2`.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- "Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)" à la page 77
- "Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (serveur d'appel entrant)" à la page 79
- "Configuration de l'authentification CHAP pour les appelants de confiance (machines d'appel sortant)" à la page 79

Modification des fichiers de configuration PPP pour CHAP (serveur d'appel entrant)

La tâche décrite dans cette section explique comment mettre à jour les fichiers de configuration PPP existants pour la prise en charge de l'authentification CHAP sur le serveur d'appel entrant.

▼ Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (serveur d'appel entrant)

1. **Connectez-vous en tant que superutilisateur au serveur d'appel entrant.**

2. **Modifiez le fichier `/etc/ppp/options`.**

   Ajoutez les options indiquées en caractères gras pour la prise en charge CHAP.

   ```
   # cat /etc/ppp/options
   lock
   nodefaultroute
   name CallServe
   auth
   ```

`name` *CallServe*	Définit *CallServe* comme le nom CHAP de l'utilisateur de la machine locale, dans ce cas le serveur d'appel entrant.
`auth`	Demande à la machine locale d'authentifier les appelants avant d'établir la liaison.

3. **Créez les fichiers de configuration PPP restants pour la prise en charge des appelants de confiance.**

   Reportez-vous aux sections “Configuration des utilisateurs du serveur d'appel entrant ” à la page 55 et “Définition des communications sur la ligne série (serveur d'appel entrant) ” à la page 56.

Voir aussi Pour configurer les informations d'authentification CHAP des appelants de confiance, reportez-vous à la section “Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)” à la page 77.

Configuration de l'authentification CHAP pour les appelants de confiance (machines d'appel sortant)

Cette section contient les tâches pour la configuration de l'authentification CHAP sur les machines d'appel sortant des appelants de confiance. En fonction de la stratégie de sécurité de votre site, vous ou les appelants de confiance pouvez être responsables de la configuration de l'authentification CHAP.

Pour que les appelants distants configurent l'authentification CHAP, assurez-vous que les secrets CHAP locaux des appelants correspondent aux secrets CHAP équivalents des appelants dans le fichier `/etc/ppp/chap-secrets` du serveur d'appel entrant. Ensuite, attribuez aux appelants les tâches de configuration CHAP décrites dans cette section.

La configuration CHAP pour les appelants de confiance implique deux tâches :

- Création des informations d'identification de sécurité CHAP des appelants
- Configuration des machines d'appel sortant des appelants pour prendre en charge l'authentification CHAP

▼ Configuration des informations d'authentification CHAP pour les appelants de confiance

Cette procédure indique comment configurer les informations d'identification CHAP de deux appelants de confiance. Elle implique que vous, l'administrateur système, créez les informations d'identification CHAP sur les machines d'appel sortant des appelants de confiance.

1. **Connectez-vous en tant qu'administrateur à la machine d'appel sortant.**
   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".
   Utilisez l'exemple de configuration CHAP présenté à la section "Exemple de configuration utilisant l'authentification CHAP" à la page 39 et partez du principe que la machine d'appel sortant appartient à l'appelant de confiance `account1`.

2. **Modifiez la base de données chap-secrets de l'appelant `account1`.**
   Cette version fournit un fichier `/etc/ppp/chap-secrets` qui contient des commentaires utiles mais aucune option. Vous pouvez ajouter les options suivantes au fichier `/etc/ppp/chap-secrets`.

   ```
   account1  CallServe   key123   *
   ```

   `CallServe` correspond au nom du pair que `account1` tente d'atteindre. `key123` est le secret CHAP à utiliser pour les liaisons entre `account1` et `CallServer`.

3. **Connectez-vous en tant qu'administrateur à la machine d'appel sortant.**
   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".
   Supposons que cette machine appartient à l'appelant `account2`.

4. **Modifiez la base de données `/etc/ppp/chap-secrets` pour l'appelant account2.**

   ```
   account2  CallServe   key456   *
   ```

   A présent, le secret `key456` correspond aux informations d'identification que l'appelant `account2` utilise pour communiquer avec le pair `CallServe` via la liaison.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- “Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)” à la page 77
- “Configuration des informations d'authentification CHAP pour les appelants de confiance ” à la page 80

Ajout de l'authentification CHAP dans les fichiers de configuration (machine d'appel sortant)

Pour en savoir plus sur l'authentification CHAP, reportez-vous à la section “Protocole CHAP (Challenge-Handshake Authentication Protocol)” à la page 136. La tâche suivante permet de configurer la machine d'appel sortant qui appartient à l'appelant `account1`, présenté à la section “Exemple de configuration utilisant l'authentification CHAP” à la page 39.

▼ Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (machine d'appel sortant)

1. **Connectez-vous en tant que superutilisateur à la machine d'appel sortant.**
2. **Assurez-vous que le fichier `/etc/ppp/options` possède les options suivantes.**

```
# cat /etc/ppp/options
lock
nodefaultroute
```

3. **Créez un fichier `/etc/ppp/peers/`*peer-name* pour la machine distante `CallServe`.**

```
# cat /etc/ppp/peers/CallServe
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user account1
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

L'option `user account1` définit `account1` comme le nom d'utilisateur CHAP à attribuer à `CallServe`. Pour obtenir une description des autres options du fichier précédent, reportez-vous au fichier similaire `/etc/ppp/peers/myserver` décrit à la section “Définition de la connexion à un pair donné” à la page 51.

Voir aussi Pour tester l'authentification CHAP en appelant le serveur d'appel entrant, reportez-vous à la section “Appel du serveur d'appel entrant” à la page 58.

♦ ♦ ♦ CHAPITRE 6

Configuration d'un tunnel PPP Over Ethernet

Ce chapitre décrit les tâches de la configuration des participants situés à chaque extrémité du tunnel PPPoE : le client PPPoE et le serveur d'accès PPPoE. Voici la liste des sujets abordés :

Le scénario présenté dans la section “Planification de la prise en charge DSL sur un tunnel PPPoE” à la page 41 sert d'exemple pour la description des tâches. Pour obtenir une présentation de PPPoE, reportez-vous à la section “Prise en charge des utilisateurs DSL via PPPoE ” à la page 25.

Tâches principales de la configuration d'un tunnel PPPoE (liste des tâches)

Les tableaux suivants répertorient les tâches principales de la configuration des clients PPPoE et du serveur d'accès PPPoE. Pour mettre en oeuvre PPPoE sur votre site, il vous suffit de configurer votre extrémité du tunnel PPPoE : le côté client ou le côté serveur d'accès.

TABLEAU 6-1 Liste des tâches de configuration d'un client PPPoE

Tâche	Description	Pour obtenir des instructions
1. Configuration d'une interface PPPoE	Définissez l'interface Ethernet à utiliser pour le tunnel PPPoE.	“Configuration d'une interface pour un client PPPoE ” à la page 84
2. Configuration des informations concernant le serveur d'accès PPPoE	Définissez les paramètres du serveur d'accès à l'extrémité du tunnel PPPoE où se trouve le fournisseur de services.	“Définition d'un pair de serveur d'accès PPPoE” à la page 85
3. Configuration des fichiers de configuration PPP	Définissez les fichiers de configuration PPP pour le client, si ce n'est déjà fait.	“Définition des communications sur la ligne série ” à la page 49
4. Création du tunnel	Appelez le serveur d'accès.	“Définition d'un pair de serveur d'accès PPPoE” à la page 85

TABLEAU 6-2 Liste des tâches de la configuration d'un serveur d'accès PPPoE

Tâche	Description	Pour obtenir des instructions
1. Configuration d'un serveur d'accès PPPoE	Définissez l'interface Ethernet à utiliser pour le tunnel PPPoE et les services offerts par le serveur d'accès.	“Configuration d'un serveur d'accès PPPoE” à la page 87
2. Configuration des fichiers de configuration PPP	Définissez les fichiers de configuration PPP pour le client, si ce n'est déjà fait.	“Configuration de la communication sur le serveur d'appel entrant ” à la page 56
3. (Facultatif) Restriction de l'utilisation d'une interface	Utilisez les options PPPoE et l'authentification PAP afin de limiter pour certains clients l'utilisation d'une interface Ethernet donnée.	“Limitation de l'utilisation d'une interface à des clients spécifiques ” à la page 89

Configuration du client PPPoE

Pour fournir PPP aux systèmes client via DSL, vous devez d'abord configurer PPPoE sur l'interface connectée au modem ou au hub. Vous devez ensuite modifier les fichiers de configuration PPP pour définir le serveur d'accès à l'extrémité opposée du protocole PPPoE.

Prérequis pour la configuration du client PPPoE

Avant de configurer le client PPPoE, vous devez effectuer les opérations suivantes :

- Installez la version Oracle Solaris sur les machines client qui doivent utiliser le tunnel PPPoE.
- Contactez le fournisseur de services pour plus d'informations sur son serveur d'accès PPPoE.
- Demandez à l'opérateur téléphonique ou au fournisseur de services de monter les périphériques utilisés par les machines client. Ces périphériques incluent, par exemple, le modem DSL et le séparateur, qu'il incombe à l'opérateur téléphonique de monter.

▼ Configuration d'une interface pour un client PPPoE

Suivez cette procédure pour définir l'interface Ethernet à utiliser pour le tunnel PPPoE.

1. **Connectez-vous en tant qu'administrateur au client PPPoE.**

Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Ajoutez le nom de l'interface Ethernet dotée de la connexion DSL au fichier `/etc/ppp/pppoe.if`.**

   Par exemple, vous pouvez ajouter l'entrée suivante à `/etc/ppp/pppoe.if` pour un client PPPoE qui utilise `hme0` comme l'interface réseau qui est connectée au modem DSL.

   ```
   hme0
   ```

   Pour plus d'informations sur `/etc/ppp/pppoe.if`, reportez-vous à la section "Fichier `/etc/ppp/pppoe.if`" à la page 142.

3. **Configurez l'interface pour une utilisation de PPPoE.**

   ```
   # /etc/init.d/pppd start
   ```

4. **(Facultatif) Vérifiez que l'interface est maintenant montée pour PPPoE.**

   ```
   # /usr/sbin/sppptun query
   hme0:pppoe
   hme0:pppoed
   ```

   Vous pouvez également monter manuellement les interfaces pour PPPoE à l'aide de la commande `/usr/sbin/sppptun` . Pour plus d'instructions, reportez-vous à la section "Commande `/usr/sbin/sppptun`" à la page 143.

▼ Définition d'un pair de serveur d'accès PPPoE

Vous définissez le serveur d'accès dans le fichier `/etc/ppp/peers/` *peer-name*. De nombreuses options utilisées pour le serveur d'accès permettent également de définir le serveur d'appel entrant dans le cadre d'un scénario de commutation. Pour obtenir une explication détaillée de `/etc/ppp/peers/`*peer-name*, reportez-vous à la section "Fichier `/etc/ppp/peers/`*peer-name*" à la page 120.

1. **Connectez-vous en tant qu'administrateur au client PPPoE.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Définissez le serveur d'accès PPPoE du fournisseur de services dans le fichier `/etc/ppp/peers/`*peer-name*.**

Par exemple, le fichier suivant, `/etc/ppp/peers/dslserve`, définit le serveur d'accès `dslserve` au niveau du FAI lointain, présenté à la section “Exemple de configuration d'un tunnel PPPoE ” à la page 43.

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

La section “Fichier `/etc/ppp/peers/`*peer-name* de définition d'un pair de serveur d'accès” à la page 150 définit les options contenues dans ce fichier.

3. **Modifiez les autres fichiers de configuration PPP sur le client PPPoE.**

   a. **Configurez `/etc/ppp/options` comme décrit dans les instructions de configuration d'une machine d'appel sortant à la section “Configuration de la machine d'appel sortant” à la page 46.**

   b. **Créez un fichier `/etc/ppp/options.sppptun`. `/etc/ppp/options.sppptun` définit les options PPP pour le port série auquel l'interface montée pour PPPoE est connectée.**

      Vous pouvez utiliser toutes les options disponibles pour le fichier `/etc/ppp/options.`*ttyname* décrit dans “Fichier de configuration `/etc/ppp/options.`*ttyname* ” à la page 117. Vous devez nommer le fichier `/etc/ppp/options.sppptun`, car `sppptun` est le nom de périphérique spécifié dans la configuration `pppd`.

4. **Assurez-vous que tous les utilisateurs peuvent démarrer PPP sur le client.**

   ```
   # touch /etc/ppp/options
   ```

5. **Vérifiez que PPP peut s'exécuter sur une ligne DSL.**

   ```
   % pppd debug updetach call dslserve
   ```

   `dslserve` est le nom attribué au serveur d'accès au niveau du FAI illustré à la section “Exemple de configuration d'un tunnel PPPoE ” à la page 43. L'option `debug updetach` entraîne l'affichage des informations de débogage dans la fenêtre de terminal.

   Si PPP fonctionne correctement, la sortie du terminal indique l'activation de la liaison. Si PPP n'est toujours pas exécuté, essayez d'utiliser la commande ci-dessous pour voir si les serveurs fonctionnent correctement :

```
# /usr/lib/inet/pppoec -i hme0
```

Remarque - Les utilisateurs de clients PPPoE configurés peuvent lancer l'exécution de PPP sur une ligne DSL à l'aide de la commande suivante :

```
% pppd call ISP-server-name
```

Les utilisateurs peuvent alors exécuter une application ou un service.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- Voir “Configuration du client PPPoE” à la page 84.
- Voir “Création de tunnels PPPoE pour la prise en charge DSL ” à la page 141.
- Reportez-vous au Chapitre 7, Dépannage de problèmes courants du Point-to-Point Protocol.
- Voir “Configuration d'un serveur d'accès PPPoE” à la page 87.

Configuration d'un serveur d'accès PPPoE

Si votre société est un fournisseur de services, vous pouvez offrir des services, notamment Internet, aux clients qui accèdent à votre site par le biais d'une connexion DSL. La procédure consiste à déterminer les interfaces du serveur à impliquer dans le tunnel PPPoE et à définir les services mis à la disposition des utilisateurs.

▼ Configuration d'un serveur d'accès PPPoE

Cette procédure permet de définir l'interface Ethernet à utiliser pour le tunnel PPPoE et de configurer les services offerts par le serveur d'accès.

1. **Connectez-vous en tant qu'administrateur au serveur d'accès.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Ajoutez le nom des interfaces Ethernet qui sont destinées aux tunnels PPPoE dans le fichier `/etc/ppp/pppoe.if`.**

   Par exemple, utilisez le fichier `/etc/ppp/pppoe.if` pour le serveur d'accès `dslserve` décrit à la section “Exemple de configuration d'un tunnel PPPoE ” à la page 43.

   ```
   # cat /etc/ppp/pppoe.if
   hme1
   hme2
   ```

3. **Définissez les services globaux fournis par le serveur d'accès dans le fichier /etc/ppp/pppoe.**
   Le fichier /etc/ppp/pppoe suivant répertorie les services fournis par le serveur d'accès dslserve illustré à la Figure 2-5, “Exemple de tunnel PPPoE ”.

   ```
   device hme1,hme2
   service internet
       pppd "proxyarp 192.168.1.1:"
   service debugging
       pppd "debug proxyarp 192.168.1.1:"
   ```

   Dans le fichier exemple, le service Internet est annoncé pour les interfaces Ethernet hme1 et hme2 de dslserve. Le débogage est activé pour les liaisons PPP sur les interfaces Ethernet.

4. **Configurez les fichiers de configuration PPP de la même façon que pour un serveur d'appel entrant.**
   Pour plus d'informations, reportez-vous à la section “Création d'un schéma d'adressage IP pour appelants ” à la page 139.

5. **Démarrez le démon pppoed.**

   ```
   # /etc/init.d/pppd start
   ```

   pppd monte également les interfaces qui sont répertoriées dans /etc/ppp/pppoe.if.

6. **(Facultatif) Vérifiez que les interfaces sur le serveur sont montées pour PPPoE.**

   ```
   # /usr/sbin/sppptun query
   hme1:pppoe
   hme1:pppoed
   hme2:pppoe
   hme2:pppoed
   ```

   L'exemple précédent indique que les interfaces hme1 et hme2 sont montées pour PPPoE. Vous pouvez également monter manuellement les interfaces pour PPPoE à l'aide de la commande /usr/sbin/sppptun . Pour plus d'instructions, reportez-vous à la section “Commande /usr/sbin/sppptun” à la page 143.

▼ Modification fichier /etc/ppp/pppoe

1. **Connectez-vous en tant qu'administrateur au serveur d'accès.**
   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Modifiez /etc/ppp/pppoe, selon vos besoins.**

3. **Faites en sorte que le démon `pppoed` reconnaisse les nouveaux services.**

```
# pkill -HUP pppoed
```

Limitation de l'utilisation d'une interface à des clients spécifiques

La procédure suivante indique comment limiter une interface à un groupe de clients PPPoE. Avant d'effectuer cette tâche, vous devez vous procurer les vraies adresses MAC Ethernet des clients que vous affectez à l'interface.

Remarque - Certains systèmes permettent de modifier l'adresse MAC sur l'interface Ethernet. Cette possibilité doit être pour vous une commodité, non une mesure de sécurité.

Si vous utilisez l'exemple illustré à la section “Exemple de configuration d'un tunnel PPPoE ” à la page 43, ces étapes indiquent comment réserver une interface de `dslserve`, `hme1`, aux clients ENT Centrale.

1. **Configurez les interfaces du serveur d'accès et définissez les services, comme indiqué à la section “Configuration d'un serveur d'accès PPPoE” à la page 87.**

2. **Créez des entrées pour les clients dans la base de données `/etc/ethers` du serveur.**
   Voici un exemple d'entrée pour les clients Red, Blue et Yellow.

```
8:0:20:1:40:30 redether
8:0:20:1:40:10 yellowether
8:0:20:1:40:25 blueether
```

   Dans cet exemple, les noms symboliques `redether`, `yellowether` et `blueether` sont affectés aux adresses Ethernet des clients Red, Yellow et Blue. L'affectation de noms symboliques aux adresses MAC est facultative.

3. **Pour limiter les services fournis sur une interface donnée, définissez les informations suivantes dans le fichier `/etc/ppp/pppoe.`*device*.**
   Dans ce fichier, *device* est le nom du périphérique à définir.

```
# cat /etc/ppp/pppoe.hme1
service internet
     pppd "name dslserve-hme1"
     clients redether,yellowether,blueether
```

   `dslserve-hme1` est le nom du serveur d'accès utilisé dans les entrées correspondantes dans le fichier `pap-secrets`. L'option `clients` limite l'utilisation de l'interface `hme1` aux clients portant les noms Ethernet symboliques `redether`, `yellowether` et `blueether`.

Si vous n'avez pas défini de noms symboliques pour les adresses MAC du client dans la base de données `/etc/ethers`, vous pouvez utiliser les adresses numériques sous forme d'arguments de l'option `clients`. Les caractères génériques sont autorisés.

Vous pouvez, par exemple, spécifier l'adresse numérique `clients 8:0:20:*:*:*`. Grâce aux caractères génériques, toutes les adresses correspondantes dans la base de données `/etc/ethers` sont acceptées.

4. **Créez le fichier `/etc/ppp/pap-secrets` pour le serveur d'accès :**

```
Red         dslserve-hme1   redpasswd     *
Blue        dslserve-hme1   bluepasswd    *
Yellow      dslserve-hme1   yellowpassd   *
```

Les entrées sont les noms et mots de passe PAP des clients autorisés à exécuter PPP sur l'interface `hme1` de `dslserve`.

Pour plus d'informations sur l'authentification PAP, reportez-vous à la section “Configuration de l'authentification PAP” à la page 68.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- Pour en savoir plus à propos de PPPoE, reportez-vous à la section “Création de tunnels PPPoE pour la prise en charge DSL ” à la page 141.
- Pour résoudre les problèmes liés à PPPoE et PPP, reportez-vous à la section “Résolution des problèmes liés à PPP et PPPoE” à la page 95.
- Pour configurer un client PPPoE, reportez-vous à la section “Configuration du client PPPoE” à la page 84.
- Pour configurer une authentification PAP pour un client, reportez-vous à la section “Configuration de l'authentification PAP pour les appelants de confiance (machines d'appel sortant)” à la page 72.
- Pour configurer une authentification PAP sur un serveur, reportez-vous à la section “Configuration de l'authentification PAP sur le serveur d'appel entrant ” à la page 69.

♦ ♦ ♦ CHAPITRE 7

Dépannage de problèmes courants du Point-to-Point Protocol

Ce chapitre contient des informations de dépannage des problèmes courants qui se produisent avec Solaris PPP 4.0. Il aborde les sujets suivants :

Le livre intitulé *PPP Design, Implementation, and Debugging* de James Carlson et le site Web de l'Australian National University proposent également des conseils détaillés pour la résolution des problèmes liés à PPP. Pour plus d'informations, reportez-vous à “Ouvrages de référence professionnelle à propos de PPP ” à la page 15.

Résolution des problèmes liés à PPP (liste des tâches)

Utilisez la liste des tâches suivante pour accéder facilement à des conseils et des solutions relatifs aux problèmes liés à PPP.

TABLEAU 7-1 Liste des tâches de résolution des problèmes liés à PPP

Tâche	Définition	Pour obtenir des instructions
Obtention d'informations de diagnostic sur la liaison PPP	Utilisez les outils de diagnostic PPP afin d'obtenir la sortie pour la résolution des problèmes.	“Obtention des informations de diagnostic à l'aide de `pppd`” à la page 93
Obtention des informations de débogage pour la liaison PPP	Utilisez la commande `pppd debug` afin de générer une sortie pour la résolution de problèmes.	“Activation du débogage de PPP” à la page 94
Résolution des problèmes généraux avec la couche réseau	Identifiez et corrigez les problèmes liés à PPP qui sont relatifs au réseau en	“Diagnostic des problèmes réseau ” à la page 96

Tâche	Définition	Pour obtenir des instructions
	effectuant une série de vérifications.	
Résolution de problèmes de communication généraux	Identifiez et corrigez les problèmes de communication qui affectent la liaison PPP.	“Diagnostic et résolution des problèmes de communication ” à la page 98
Résolution des problèmes de configuration	Identifiez et corrigez les problèmes dans les fichiers de configuration PPP.	“Diagnostic des problèmes liés à la configuration PPP” à la page 100
Résolution des problèmes liés au modem	Identifiez et corrigez les problèmes de modem.	“Diagnostic des problèmes de modem ” à la page 101
Résolution des problèmes liés aux scripts de discussion	Identifiez et corrigez les problèmes de script de discussion sur l'ordinateur des appels sortants.	“Obtention des informations de débogage pour les scripts de discussion” à la page 102
Résolution des problèmes de débit de la ligne série	Identifiez et corrigez les problèmes de débit de ligne sur le serveur des appels entrants.	“Diagnostic et résolution des problèmes de débit de ligne série” à la page 104
Résolution des problèmes courants pour les lignes spécialisées	Identifiez et corrigez les problèmes de performances sur une ligne spécialisée.	“Correction des problèmes des lignes spécialisées” à la page 108
Résolution des problèmes liés à l'authentification	Identifiez et corrigez les problèmes liés aux bases de données d'authentification.	“Diagnostic et résolution des problèmes d'authentification” à la page 109
Dépannage des zones à problème pour PPPoE	Utilisez les outils de diagnostic PPP afin d'obtenir la sortie pour l'identification et la résolution des problèmes liés à PPPoE.	“Obtention des informations de diagnostic pour PPPoE ” à la page 105

Outils de dépannage de PPP

Les liaisons PPP présentent généralement trois zones principales d'échec :

- échec de création du lien ;
- dégradation des performances du lien pendant l'utilisation normale ;
- problèmes pouvant être dus aux réseaux de l'un ou l'autre côté du lien.

La manière la plus simple de savoir si PPP fonctionne est d'exécuter une commande sur le lien. Exécutez une commande telle que `ping` ou `traceroute` sur un hôte du réseau du pair. Ensuite, observez les résultats. Cependant, vous devez utiliser les outils de débogage PPP et UNIX pour contrôler les performances d'un lien établi ou pour résoudre les problèmes posés par un lien.

Cette section explique comment obtenir les informations de diagnostic à l'aide de `pppd` et des fichiers journaux associés. Les autres sections de ce chapitre décrivent les problèmes

couramment posés par PPP que vous pouvez détecter et corriger à l'aide des outils de dépannage PPP.

▼ Obtention des informations de diagnostic à l'aide de pppd

La procédure suivante montre comment visualiser le fonctionnement en cours d'un lien sur la machine locale.

1. **Connectez-vous en tant qu'administrateur à la machine locale.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Exécutez `pppd` avec le périphérique série configuré pour PPP en tant qu'argument :**

   ```
   # pppd cua/b debug updetach
   ```

   Les exemples suivants présentent les sorties obtenues pour une liaison commutée et une liaison de ligne spécialisée lorsque `pppd` s'exécute en arrière-plan. Si vous exécutez `pppd debug` en arrière-plan, la sortie produite est envoyée dans le fichier `/etc/ppp/connect-errors`.

Exemple 7-1 Sortie d'une liaison commutée fonctionnant correctement

```
# pppd /dev/cua/b debug updetach
have route to 0.0.0.0/0.0.0.0 via 172.21.0.4
serial speed set to 230400 bps
Using interface sppp0
Connect: sppp0 <--> /dev/cua/b
sent [LCP ConfReq id=0x7b <asyncmap 0x0> <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP Ident id=0x79 magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6
 2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
 rcvd [LCP ConfRej id=0x7b <asyncmap 0x0>]
sent [LCP Ident id=0x7c magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Sep 15
 2004 09:38:33)"
sent [LCP ConfReq id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP Ident id=0x7e magic=0x73e981c8 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
 Sep 15 2004 09:38:33)"]
sent [IPCP ConfReq id=0x3d <addr 0.0.0.0> <compress VJ 0f 01>]
rcvd [LCP Ident id=0x7a magic=0xdd4ad820 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
 Oct  6 2004 09:36:22)"]
```

```
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
rcvd [IPCP ConfReq id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
sent [IPCP ConfAck id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
rcvd [IPCP ConfNak id=0x3d <addr 10.0.0.2>]]
sent [IPCP ConfReq id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
rcvd [IPCP ConfAck id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

Exemple 7-2 Sortie d'une liaison de ligne spécialisée fonctionnant correctement

```
# pppd /dev/se_hdlc1 default-asyncmap debug updetach
pppd 2.4.0b1 (Sun Microsystems, Inc., Oct 24 2004 07:13:18) started by root, uid 0
synchronous speed appears to be 0 bps
init option: '/etc/ppp/peers/syncinit.sh' started (pid 105122)
Serial port initialized.
synchronous speed appears to be 64000 bps
Using interface sppp0
Connect: sppp0 <--> /dev/se_hdlc1
sent [LCP ConfReq id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfAck id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP Ident id=0xea magic=0x474283c6 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
 22 2004 14:31:44)"]
sent [IPCP ConfReq id=0xf7 <addr 0.0.0.0> <compress VJ Of o1>]]
sent [CCP ConfReq id=0x3f <deflate 15> <deflate(old#) 15> <bsd v1 15>]
rcvd [LCP Ident id=0x23 magic=0x8e3a53ff "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
 22 2004 14:31:44)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct 22 2004 14:31:44)
rcvd [IPCP ConfReq id=0x25 <addr 10.0.0.1> <compress VJ Of 01>]
sent [IPCP ConfAck id=0x25 <addr 10.0.0.1> <compress VJ Of 01>]
rcvd [CCP ConfReq id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
sent [CCP ConfAck id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
rcvd [IPCP ConfNak id=0xf8 <addr 10.0.0.2>]
rcvd [IPCP ConfReq id=0xf7 <addr 10.0.0.2> <compress VJ Of 01>]
rcvd [CCP ConfAck id=0x3f <deflate 15> <deflate(old#) 15 <bsd v1 15>]
Deflate (15) compression enabled
rcvd [IPCP ConfAck id=0xf8 <addr 10.0.0.2> <compress VJ Of 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

▼ Activation du débogage de PPP

La tâche suivante présente l'utilisation de la commande `pppd` pour obtenir des informations de débogage.

Remarque - Vous n'avez besoin d'exécuter les étapes 1 à 3 qu'une fois pour chaque hôte. Par la suite, vous pouvez passer à l'étape 4 pour activer le débogage pour l'hôte.

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Créez un fichier journal pour enregistrer la sortie de `pppd`.**

   ```
   # touch /var/log/pppdebug
   ```

3. **Ajoutez les fonctions `syslog` suivantes pour `pppd` dans `/etc/syslog.conf`.**

   ```
   daemon.debug;local2.debug       /var/log/pppdebug
   ```

4. **Redémarrez `syslogd`.**

   ```
   # pkill -HUP -x syslogd
   ```

5. **Activez le débogage pour les appels à un pair particulier à l'aide de la syntaxe suivante de `pppd`.**

   ```
   # pppd debug call peer-name
   ```

   peer-name doit être le nom d'un fichier dans le répertoire `/etc/ppp/peers`.

6. **Affichez le contenu du fichier journal.**

   ```
   # tail -f /var/log/pppdebug
   ```

   Pour obtenir un exemple de fichier journal, reportez-vous à l'Étape 3.

Résolution des problèmes liés à PPP et PPPoE

Reportez-vous aux sections suivantes pour plus d'informations sur la façon de résoudre les problèmes liés à PPP et PPPoE.

Diagnostic des problèmes réseau

Si la liaison PPP devient active mais que peu d'hôtes du réseau distant sont accessibles, il peut s'agit d'un problème de réseau. La procédure suivante vous indique comment isoler et résoudre les problèmes réseau ayant une incidence sur une liaison PPP.

1. **Connectez-vous en tant qu'administrateur à la machine locale.**

   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Arrêtez le lien qui pose problème.**

3. **Désactivez les protocoles facultatifs dans les fichiers de configuration en ajoutant les options suivantes à votre configuration de PPP :**

   ```
   noccp novj nopcomp noaccomp default-asyncmap
   ```

   Ces options offrent le PPP non compressé le plus simple qui existe. Essayez d'appeler ces options en tant qu'arguments associés à `pppd` sur la ligne de commande. Si vous pouvez atteindre les hôtes précédemment inaccessibles, ajoutez les options dans l'un ou l'autre des emplacements ci-dessous.

   - `/etc/ppp/peers/`*peer-name*, après l'option `appel`
   - `/etc/ppp/options`, en vous assurant que les options s'appliquent de manière globale.

4. **Appelez le pair distant. Ensuite, activez les fonctions de débogage.**

   ```
   % pppd debug call peer-name
   ```

5. **Obtenez les journaux détaillés du programme de messagerie instantanée en utilisant l'option `-v` de `chat`.**

   Par exemple, utilisez le format suivant dans n'importe quel fichier de configuration PPP :

   ```
   connect 'chat -v -f /etc/ppp/chatfile'
   ```

   /etc/ppp/chatfile représente le nom de votre fichier de messagerie instantanée.

6. **Essayez de recréer le problème en utilisant Telnet ou d'autres applications pour atteindre les hôtes distants.**

   Etudiez les journaux de débogage. Si vous ne pouvez toujours pas atteindre les hôtes distants, le problème PPP peut être lié au réseau.

7. **Vérifiez que les adresses IP des hôtes distants sont des adresses Internet enregistrées.**

   Certaines organisations assignent des adresses IP internes qui sont connues au sein du réseau local mais ne sont pas routables sur Internet. Si les hôtes distants se trouvent au sein de votre entreprise, vous devez définir un serveur de conversion de nom en adresse ou un serveur proxy pour accéder à Internet. Si les hôtes distants ne sont pas au sein de votre entreprise, vous devez signaler le problème à l'organisation distante.

8. **Examinez les tables de routage.**

   a. **Vérifiez les tables de routage sur la machine locale et le pair.**

   b. **Vérifiez les tables de routage pour les routeurs qui sont dans le chemin d'accès du pair vers le système distant. Vérifiez également les tables de routage pour les routeurs du chemin d'accès de retour au pair.**

      Assurez-vous que les routeurs intermédiaires n'ont pas été configurés de manière incorrecte. Souvent, le problème peut être trouvé dans le chemin de retour au pair.

9. **(Facultatif) Si la machine est un routeur, vérifiez les fonctionnalités facultatives.**

   ```
   # ndd -set /dev/ip ip_forwarding 1
   ```

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

   Dans Solaris 10, vous pouvez utiliser `routeadm`(1M), au lieu de `ndd`(1M).

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

   Remarque - La commande `ndd` n'est pas persistante. Les valeurs définies à l'aide de cette commande sont perdues lors de la réinitialisation du système. La commande `routeadm` est persistante. Les valeurs définies avec cette commande sont conservées après la réinitialisation du système.

10. **Vérifiez les statistiques qui sont obtenues à l'aide de `netstat -s` et des outils similaires.**

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

    a. **Exécutez les statistiques sur la machine locale.**

    b. **Appelez le pair.**

    c. **Observez les nouvelles statistiques générées par `netstat -s`.**

       Pour plus d'informations, reportez-vous à la section “Problèmes réseau courants affectant PPP ” à la page 98.

11. **Vérifiez la configuration DNS.**

    Une configuration de service de noms incorrecte entraîne l'échec des applications car les adresses IP ne peuvent pas être résolues.

Problèmes réseau courants affectant PPP

Vous pouvez utiliser les messages qui sont générés par `netstat- s` pour corriger les problèmes de réseau présentés dans le tableau suivant. Pour des informations sur les procédures associées, reportez-vous à la section “Diagnostic des problèmes réseau ” à la page 96.

TABLEAU 7-2 Problèmes réseau courants affectant PPP

Message	Problème	Solution
`IP packets not forwardable` (Paquets IP non transmissibles)	Une route est manquante pour l'hôte local.	Ajoutez la route manquante aux tables de routage de l'hôte local.
`ICMP input destination unreachable` (Destination d'entrée ICMP inaccessible)	Une route est manquante pour l'hôte local.	Ajoutez la route manquante aux tables de routage de l'hôte local.
`ICMP time exceeded` (Temps ICMP dépassé)	Deux routeurs se transfèrent la même adresse de destination, ce qui entraîne le rebondissement du paquet jusqu'à ce que la valeur de durée de vie soit dépassée.	Utilisez `traceroute` pour trouver l'origine de la boucle de routage, puis contactez l'administrateur du routeur concerné. Pour plus d'informations sur `traceroute`, reportez-vous à la page de manuel `traceroute`(1M).
`IP packets not forwardable` (Paquets IP non transmissibles)	Une route est manquante pour l'hôte local.	Ajoutez la route manquante à la table de routage de l'hôte local.
`ICMP input destination unreachable` (Destination d'entrée ICMP inaccessible)	Une route est manquante pour l'hôte local.	Ajoutez la route manquante aux tables de routage de l'hôte local.

▼ Diagnostic et résolution des problèmes de communication

Les problèmes de communication surviennent lorsque les deux pairs ne parviennent pas à un établir une liaison. Il arrive parfois que ces problèmes soient en fait des problèmes de négociation causés par une configuration incorrecte des scripts de discussion. La procédure suivante vous indique comment supprimer les problèmes de communication. Pour supprimer les problèmes de négociation dus à des scripts de discussion erronés, reportez-vous au Tableau 7-5, “Problèmes de scripts de discussion courants”.

1. **Connectez-vous en tant qu'administrateur à la machine locale.**

Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Appelez le pair.**

3. **Appelez le pair distant. Ensuite, activez les fonctions de débogage.**

```
% pppd debug call peer-name
```

Vous devrez peut-être obtenir des informations de débogage du pair afin de résoudre certains problèmes de communication.

4. **Vérifiez les journaux obtenus pour connaître les problèmes de communication. Pour plus d'informations, reportez-vous à la section "Problèmes de communication généraux affectant PPP " à la page 99.**

Problèmes de communication généraux affectant PPP

Le tableau suivant présente les symptômes associés à la sortie de journal de la procédure, "Diagnostic et résolution des problèmes de communication " à la page 98.

TABLEAU 7-3 Problèmes de communication généraux affectant PPP

Symptôme	Problème	Solution
`too many Configure-Requests` (Demandes de configuration trop nombreuses)	Un pair ne peut pas entendre l'autre pair.	Vérifiez les problèmes suivants : ■ Le câblage de l'ordinateur ou du modem est peut-être défectueux. ■ Les paramètres binaires de la configuration du modem sont peut-être incorrects. Il se peut également que le contrôle de flux de la configuration soit interrompu. ■ Le script de discussion a peut-être subi un échec. Dans cette situation, reportez-vous au Tableau 7-5, "Problèmes de scripts de discussion courants".
La sortie `pppd debug` montre que LCP démarre, mais que les protocoles de niveau supérieur échouent ou affichent des erreurs CRC.	La table des caractères de contrôle asynchrone (ACCM) n'est pas correctement définie.	Utilisez l'option `default-async` afin de définir l'ACCM sur la valeur par défaut de FFFFFFFF. Tout d'abord, essayez d'utiliser `default-async` en tant qu'option de `pppd` sur la ligne de commande. Si le problème disparaît, ajoutez ensuite `default-async` à `/etc/ppp/options` ou `/etc/ppp/peers/`*peer-name* après l'appel.
La sortie de `pppd debug` montre qu'IPCP démarre mais s'arrête immédiatement.	Les adresses IP sont peut-être configurées de façon incorrecte.	1. Vérifiez le script de discussion afin de vérifier si le script contient des adresses IP incorrectes. 2. Si le script de discussion est correct, demandez les journaux de débogage du pair, et vérifiez-y les adresses IP.

Symptôme	Problème	Solution
Les performances du lien sont médiocres.	Le modem est peut-être mal configuré (erreurs de configuration du contrôle de flux, erreurs de configuration du modem et débits DTE configurés de façon incorrecte).	Vérifiez la configuration du modem. Modifiez la configuration, le cas échéant.

▼ Diagnostic des problèmes liés à la configuration PPP

Certains problèmes liés à PPP sont dus aux problèmes contenus dans les fichiers de configuration PPP. La procédure suivante vous indique comment identifier et résoudre les problèmes de configuration généraux.

1. **Connectez-vous en tant qu'administrateur à la machine locale.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Appelez le pair distant. Ensuite, activez les fonctions de débogage.**

   ```
   % pppd debug call peer-name
   ```

3. **Vérifiez le journal qui en résulte à la recherche de problèmes de configuration. Pour plus d'informations, reportez-vous à la section "Problèmes courants de configuration de PPP " à la page 100.**

Problèmes courants de configuration de PPP

Le tableau suivant présente les symptômes associés à la sortie de journal de la procédure, "Diagnostic des problèmes liés à la configuration PPP" à la page 100.

TABLEAU 7-4 Problèmes courants de configuration de PPP

Symptôme	Problème	Solution
La sortie de `pppd debug` contient le message d'erreur `Could not determine remote IP address` (Impossible de déterminer l'adresse IP distante).	Le fichier `/etc/ppp/peers/`*peer-name* ne contient pas d'adresse IP pour le pair. Le pair ne fournit pas d'adresse IP pendant la négociation de lien.	Fournissez une adresse IP pour le pair sur la ligne de commande pppd ou dans `/etc/ppp/peers/`*peer-name* en utilisant le format suivant : :10.0.0.10

Symptôme	Problème	Solution
La sortie de `pppd debug` indique que la compression de données CCP a échoué. La sortie indique également que le lien a été supprimé.	Les configurations de compression PPP du pair sont peut-être en conflit.	Désactivez la compression CCP en ajoutant l'option `noccp` à `/etc/ppp/options` sur l'un des pairs.

▼ Diagnostic des problèmes de modem

Les modems peuvent être des sources de problèmes majeures pour les liaisons commutées. L'indicateur le plus commun des problèmes liés à la configuration du modem est l'absence de réponse du pair. Cependant, il se peut que vous ayez des difficultés à déterminer si un problème de lien est effectivement le résultat des problèmes de configuration du modem.

La documentation et les sites Web des fabricants de modems contiennent des solutions aux problèmes rencontrés avec leurs équipements. La procédure ci-après permet de déterminer si une configuration de modem incorrecte entraîne des problèmes de liens.

1. **Une fois le débogage activé, appelez le pair, comme expliqué dans la section “Activation du débogage de PPP” à la page 94.**

2. **Affichez le journal `/var/log/pppdebug` obtenu pour vérifier si la configuration du modem est incorrecte.**

3. **Utilisez `ping` pour envoyer des paquets de tailles diverses sur le lien.**

   Pour des informations complètes sur la commande `ping`, reportez-vous à la page de manuel `ping`(1M).

   Si les petits paquets sont reçus mais que les paquets plus volumineux sont supprimés, il existe des problèmes au niveau du modem.

4. **Vérifiez la présence d'erreurs sur l'interface `sppp0` :**

```
% netstat -ni
Name  Mtu  Net/Dest   Address      Ipkts    Ierrs Opkts    Oerrs Collis Queue
lo0   8232 127.0.0.0  127.0.0.1    826808   0     826808   0     0      0
hme0  1500 172.21.0.0 172.21.3.228 13800032 0     1648464  0     0      0
sppp0 1500 10.0.0.2   10.0.0.1     210      0     128      0     0      0
```

   Si les erreurs d'interface augmentent au fil du temps, il existe peut-être des problèmes au niveau de la configuration du modem.

Erreurs fréquentes

Lorsque vous affichez le journal `/var/log/pppdebug` obtenu, les symptômes suivants dans la sortie peuvent indiquer une configuration de modem incorrecte. La machine locale peut entendre le pair, mais ce dernier ne peut entendre la machine locale.

- Aucun message `recvd` n'a été émis par le pair.
- La sortie contient les messages LCP du pair, mais le lien échoue avec les messages `too many LCP Configure Requests` (Demandes de configuration LCP trop nombreuses) envoyés par la machine locale.
- Le lien se termine avec un signal SIGHUP.

Obtention des informations de débogage pour les scripts de discussion

La procédure suivante permet d'obtenir des informations de débogage à l'aide de `chat`, ainsi que des suggestions pour la résolution des problèmes courants. Pour plus d'informations, reportez-vous à la section “Problèmes de scripts de discussion courants” à la page 102.

1. **Connectez-vous en tant qu'administrateur à la machine d'appel sortant.**
   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Modifiez le fichier `/etc/ppp/peers/`*peer-name* pour le pair à appeler.**

3. **Ajoutez `-v` en tant qu'argument à la commande `chat` qui est spécifiée dans l'option `connect`.**

   ```
   connect "/usr/bin/chat -v -f /etc/ppp/chat-script-name"
   ```

4. **Prenez connaissance des erreurs de script de discussion dans le fichier `/etc/ppp/connect-errors`.**
   L'erreur suivante est la principale erreur qui se produit avec `chat`.

   ```
   Oct 31 08:57:13 deino chat[107294]: [ID 702911 local2.info] expect (CONNECT)
   Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] alarm
   Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] Failed
   ```

   L'exemple montre le délai d'attente lors de l'attente d'une chaîne `(CONNECT)`. En cas d'échec de `chat`, vous obtenez le message suivant de `pppd` :

   ```
   Connect script failed
   ```

Problèmes de scripts de discussion courants

Les scripts de discussion sont des sources de problèmes pour les liaisons commutées. Le tableau suivant énumère les erreurs courantes de script de discussion et donne des

suggestions pour résoudre les erreurs. Pour des informations sur les procédures à suivre, reportez-vous à la section “Obtention des informations de débogage pour les scripts de discussion” à la page 102.

TABLEAU 7-5 Problèmes de scripts de discussion courants

Symptôme	Problème	Solution
La sortie de `pppd debug` contient `Connect script failed` (Echec du script de connexion)	Votre script de discussion fournit un nom d'utilisateur et un mot de passe. `ogin:` *user-name* `ssword:` *password* Cependant, le pair auquel vous aviez l'intention de vous connecter n'invite pas fournir ces informations.	1. Supprimez l'identification et le mot de passe du script de discussion. 2. Essayez d'appeler le pair une nouvelle fois. 3. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez-lui la séquence de connexion correcte.

Le journal `/usr/bin/chat -v` contient `"expect (login:)" alarm read timed out`	Votre script de discussion fournit un nom d'utilisateur et un mot de passe.
	
	`ogin: pppuser`
	`ssword: \q\U`
	
	Cependant, le pair auquel vous essayez de vous connecter n'invite pas à fournir ces informations.
		1. Supprimez l'identification et le mot de passe du script de discussion.
		2. Essayez d'appeler le pair une nouvelle fois.
		3. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez-lui la séquence de connexion correcte.

La sortie de `pppd debug` contient `possibly looped-back`	La machine locale ou son pair se bloque au niveau de la ligne de commande et n'exécute pas PPP. Le script de discussion contient un nom de connexion et un mot de passe configurés de manière incorrecte.	1. Supprimez l'identification et le mot de passe du script de discussion. 2. Essayez d'appeler le pair une nouvelle fois. 3. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez la séquence de connexion correcte.
La sortie de `pppd debug` indique que le protocole LCP s'active, mais que la liaison s'arrête rapidement après.	Le mot de passe contenu dans le script de discussion est peut-être incorrect.	1. Assurez-vous que vous avez le mot de passe correct pour la machine locale. 2. Vérifiez le mot de passe dans le script de discussion. Corrigez le mot de passe, le cas échéant. 3. Essayez d'appeler le pair une nouvelle fois. 4. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez-lui la séquence de connexion correcte.
Le texte du pair commence par un tilde (~).	Votre script de discussion fournit un nom d'utilisateur et un mot de passe. `ogin: pppuser`	1. Supprimez l'identification et le mot de passe du script de discussion.

Symptôme	Problème	Solution
	`ssword: \q\U` Cependant, le pair auquel vous essayez de vous connecter n'invite pas à fournir ces informations.	2. Essayez d'appeler le pair une nouvelle fois. 3. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez la séquence de connexion correcte.
Le modem se bloque.	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.
La sortie de `pppd debug` contient `LCP: timeout sending Config-Requests`	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.
La sortie de `pppd debug` contient `Serial link is not 8-bit clean`	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.
La sortie de `pppd debug` contient `Loopback detected` (Loopback détecté)	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.
La sortie de `pppd debug` contient `SIGHUP`	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.

▼ Diagnostic et résolution des problèmes de débit de ligne série

Les serveurs des appels entrants peuvent rencontrer des problèmes en raison de conflits au niveau des paramètres de débit. La procédure suivante vous permet d'identifier la cause du problème de lien liée aux conflits de débits de ligne série.

Les comportements suivants causent des problèmes de débit :

- Vous avez appelé PPP par l'intermédiaire d'un programme tel que `/bin/login` et indiqué le débit de la ligne.
- Vous avez démarré PPP à partir de `mgetty` et fourni accidentellement le débit binaire.

pppd modifie le débit qui a été défini à l'origine pour la ligne au profit du débit défini par `/bin/login` ou `mgetty`. En conséquence, la ligne échoue.

1. **Connectez-vous au serveur d'appel entrant. Le débogage étant activé, appelez le pair.**
   Si vous avez besoin d'instructions, reportez-vous à la section “Activation du débogage de PPP” à la page 94.

2. **Afficher le journal `/var/log/pppdebug` obtenu.**
   Vérifiez la sortie pour le message suivant :

   ```
   LCP too many configure requests
   ```

   Ce message indique que le débit des lignes série qui ont été configurées pour PPP peut potentiellement être en conflit.

3. **Vérifiez si PPP est appelé par le biais d'un programme tel que `/bin/login` et le débit de ligne qui a été défini.**
   Dans une telle situation, `pppd` modifie le débit de ligne initialement configuré au profit du débit spécifié dans `/bin/login`.

4. **Vérifiez si un utilisateur a démarré PPP à l'aide de la commande `mgetty` et accidentellement spécifié un débit binaire.**
   Cette action entraîne également des conflits entre les débits de ligne série.

5. **Résolvez ce problème de conflit comme suit :**

   a. **Verrouillez le débit ETTD sur le modem.**

   b. **N'utilisez pas autobaud.**

   c. **Ne modifiez pas le débit de ligne après la configuration.**

▼ Obtention des informations de diagnostic pour PPPoE

Vous pouvez utiliser PPP et les utilitaires UNIX standard pour identifier les problèmes liés à PPPoE. Lorsque vous avez des raisons de croire que PPPoE est la cause des problèmes se

produisant sur un lien, utilisez les outils de diagnostic suivants pour obtenir des informations sur le dépannage.

1. **Connectez-vous en tant que superutilisateur sur l'ordinateur qui exécute le tunnel PPPoE, le client PPPoE ou le serveur d'accès PPPoE.**

2. **Activez le débogage en suivant la procédure présentée dans la section “Activation du débogage de PPP” à la page 94.**

3. **Affichez le contenu du fichier journal `/var/log/pppdebug`.**

   L'exemple ci-dessous montre une partie d'un fichier journal qui a été généré pour une liaison avec un tunnel PPPoE.

```
Sep  6 16:28:45 enyo pppd[100563]: [ID 702911 daemon.info] Plugin
  pppoe.so loaded.
Sep  6 16:28:45 enyo pppd[100563]: [ID 860527 daemon.notice] pppd
  2.4.0b1 (Sun Microsystems, Inc.,
Sep  5 2001 10:42:05) started by troot, uid 0
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] connect option:
   '/usr/lib/inet/pppoec
-v hme0' started (pid 100564)
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Serial connection established.
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Using interface sppp0
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.notice] Connect: sppp0
   <--> /dev/sppptun
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/pap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/chap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] sent
  [LCP ConfReq id=0xef <mru 1492>
asyncmap 0x0 <magic 0x77d3e953><pcomp><acomp>
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] rcvd
  [LCP ConfReq id=0x2a <mru 1402>
asyncmap 0x0 <magic 0x9985f048><pcomp><acomp
```

   Si la sortie de débogage ne vous permet pas d'identifier le problème, passez à la procédure suivante.

4. **Obtenez les messages de diagnostic pour PPPoE.**

```
# pppd connect "/usr/lib/inet/pppoec -v interface-name"
```

   `pppoec` envoie les informations de diagnostic dans le fichier `stderr`. Si vous exécutez `pppd` au premier plan, la sortie s'affiche à l'écran. Si `pppd` s'exécute en arrière-plan, la sortie est envoyé dans `/etc/ppp/connect-errors`.

   L'exemple suivant présente les messages qui sont générés lors de la négociation du tunnel PPPoE.

```
Connect option: '/usr/lib/inet/pppoec -v hme0' started (pid 100564)
```

```
/usr/lib/inet/pppoec: PPPoE Event Open (1) in state Dead (0): action SendPADI (2)
/usr/lib/inet/pppoec: Sending PADI to ff:ff:ff:ff:ff:ff: 18 bytes
/usr/lib/inet/pppoec: PPPoE State change Dead (0) -> InitSent (1)
/usr/lib/inet/pppoec: Received Active Discovery Offer from 8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADO+ (5) in state InitSent (1): action SendPADR+ (5)
/usr/lib/inet/pppoec: Sending PADR to 8:0:20:cd:c1:2: 22 bytes
/usr/lib/inet/pppoec: PPPoE State change InitSent (1) -> ReqSent (3)
/usr/lib/inet/pppoec: Received Active Discovery Session-confirmation from
   8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADS (7) in state ReqSent (3): action Open (7)
/usr/lib/inet/pppoec: Connection open; session 0002 on hme0:pppoe
/usr/lib/inet/pppoec: PPPoE State change ReqSent (3) -> Convers (4)
/usr/lib/inet/pppoec: connected
```

Si les messages de diagnostic ne vous permettent pas d'identifier le problème, passez à la procédure suivante.

5. Exécutez `snoop`. Enregistrez ensuite le suivi dans un fichier.

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

```
# snoop -o pppoe-trace-file
```

6. Affichez le fichier de suivi `snoop`.

```
# snoop -i pppoe-trace-file -v pppoe

ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 1 arrived at 6:35:2.77
ETHER: Packet size = 32 bytes
ETHER: Destination = ff:ff:ff:ff:ff:ff, (broadcast)
ETHER: Source      = 8:0:20:78:f3:7c, Sun
ETHER: Ethertype = 8863 (PPPoE Discovery)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 9 (Active Discovery Initiation)
PPPoE: Session Id = 0
PPPoE: Length = 12 bytes
PPPoE:
PPPoE: ----- Service-Name -----
PPPoE: Tag Type = 257
PPPoE: Tag Length = 0 bytes
PPPoE:
PPPoE: ----- Host-Uniq -----
PPPoE: Tag Type = 259
PPPoE: Tag Length = 4 bytes
PPPoE: Data = Ox00000002
PPPoE:
.
.
```

```
.
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 5 arrived at 6:35:2.87
ETHER: Packet size = 60 bytes
ETHER: Destination = 8:0:20:78:f3:7c, Sun)
ETHER: Source      = 0:2:fd:39:7f:7,
ETHER: Ethertype = 8864 (PPPoE Session)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 0 (PPPoE Session)
PPPoE: Session Id = 24383
PPPoE: Length = 20 bytes
PPPoE:
PPP: ----- Point-to-Point Protocol -----
PPP:
PPP-LCP: ----- Link Control Protocol -----
PPP-LCP:
PPP-LCP: Code = 1 (Configure Request)
PPP-LCP: Identifier = 80
PPP-LCP: Length = 18
```

Correction des problèmes des lignes spécialisées

Les problèmes les plus couramment rencontrés avec les lignes spécialisées sont des performances médiocres. Dans la plupart des cas, vous pouvez résoudre le problème en collaboration avec l'opérateur téléphonique.

TABLEAU 7-6 Problèmes courants liés aux lignes spécialisées

Symptôme	Problème	Solution
Le lien ne démarre pas.	Cela peut être dû à des violations de bipolarité CSU. Une extrémité du lien est configurée pour les lignes AMI. L'autre extrémité est configurée pour le remplacement de huit zéros par un bit ESF (B8ZS).	Si vous êtes aux Etats-Unis ou au Canada, vous pouvez corriger ce problème directement à partir du menu du CSU/DSU. Vérifiez la documentation du fabricant du CSU/DSU pour plus de détails. Dans d'autres pays, le fournisseur peut être responsable de la correction des violations de bipolarité CSU.
Le lien présente des performances médiocres.	La sortie `pppd debug` indique des erreurs CRC lorsque le trafic est soutenu sur le lien. Votre ligne présente peut-être un problème de synchronisation, dû à des	Contactez l'opérateur téléphonique pour vous assurer que l'option de synchronisation en boucle (loop clocking) est activée.

Symptôme	Problème	Solution
	erreurs de configuration entre la compagnie de téléphone et votre réseau.	Sur certaines lignes spécialisées non structurées, vous pouvez être amené à mettre en place la synchronisation. Les utilisateurs nord-américains doivent utiliser la synchronisation en boucle.

Diagnostic et résolution des problèmes d'authentification

Le tableau suivant décrit les solutions aux problèmes d'authentification généraux.

TABLEAU 7-7 Problèmes d'authentification généraux

Symptôme	Problème	Solution
La sortie de `pppd debug` indique le message `Peer is not authorized to use remote address` (Pair non autorisé à utiliser l'adresse à distance) *address*.	Vous utilisez l'authentification PAP, et l'adresse IP du pair distant ne se trouve pas dans le fichier `/etc/ppp/pap-secrets`.	Ajoutez un astérisque (*) après l'entrée pour le pair dans le fichier `/etc/ppp/pap-secrets`.
La sortie de `pppd debug` montre que LCP démarre mais s'arrête peu après.	Le mot de passe est peut-être incorrect dans la base de données pour le protocole de sécurité utilisé.	Vérifiez le mot de passe pour le pair dans le fichier `/etc/ppp/pap-secrets` ou `/etc/ppp/chap-secrets`.

♦ ♦ ♦ CHAPITRE 8

Solaris PPP 4.0 (reference)

Ce chapitre fournit des informations détaillées sur les concepts de Solaris PPP 4.0. Les sujets abordés sont les suivants :

Utilisation des options PPP dans les fichiers et sur la ligne de commande

Solaris PPP 4.0 contient un grand nombre d'options permettant de définir votre configuration PPP. Vous pouvez utiliser ces options dans les fichiers de configuration PPP ou sur la ligne de commande, ou à l'aide à la fois des fichiers et des options de ligne de commande. Cette section contient des informations détaillées sur l'utilisation des options PPP dans les fichiers de configuration et sous forme d'arguments de commandes PPP.

Où définir les options PPP

La configuration de Solaris PPP 4.0 est très souple. Vous pouvez définir les options PPP aux endroits suivants :

- Fichiers de configuration PPP
- à l'aide des commandes PPP exécutées sur la ligne de commande ;

- à la fois dans ces fichiers et à l'aide de ces commandes.

Le tableau suivant répertorie les fichiers de configuration et les commandes PPP.

TABLEAU 8-1 Récapitulatif des fichiers de configuration et des commandes PPP

Fichier ou commande	Description	Voir
`/etc/ppp/options`	Fichier contenant les caractéristiques appliquées par défaut à toutes les liaisons PPP du système (si la machine exige des pairs qu'ils s'authentifient, par exemple). En cas d'absence de ce fichier, un utilisateur sans rôle root n'est pas autorisé à utiliser PPP.	"Fichier de configuration `/etc/ppp/options`" à la page 115
`/etc/ppp/options.`*ttyname*	Fichier qui décrit les caractéristiques de toutes les communications transitant par le port série *ttyname*.	"Fichier de configuration`/etc/ppp/options.`*ttyname*" à la page 117
`/etc/ppp/peers`	Répertoire contenant généralement des informations sur les pairs auxquels une machine d'appel sortant se connecte. Les fichiers de ce répertoire sont utilisés avec l'option `call` de la commande `pppd`.	"Spécification des informations relatives à la communication avec le serveur d'appel entrant " à la page 120
`/etc/ppp/peers/`*peer-name*	Fichier contenant les caractéristiques du pair distant *peer-name*. Les caractéristiques habituelles comprennent le numéro de téléphone et le script de discussion du pair distant pour la négociation de la liaison avec le pair.	"Fichier `/etc/ppp/peers/`*peer-name*" à la page 120
`/etc/ppp/pap-secrets`	Fichier contenant les informations d'identification de sécurité nécessaires à l'authentification PAP (Password Authentication Protocol, protocole d'authentification par mot de passe).	"Fichier `/etc/ppp/pap-secrets`" à la page 133
`/etc/ppp/chap-secrets`	Fichier contenant les informations d'identification de sécurité nécessaires à l'authentification CHAP (Challenge-Handshake Authentication Protocol, protocole d'authentification par stimulation-réponse).	"Fichier `/etc/ppp/chap-secrets`" à la page 137
`~/.ppprc`	Fichier résidant dans le répertoire personnel de l'utilisateur PPP, plus souvent utilisé avec les serveurs d'appel entrant. Ce fichier contient des informations spécifiques sur la configuration de chaque utilisateur.	"Configuration de `$HOME/.ppprc` sur un serveur d'appel entrant" à la page 119
`pppd` *options*	Commande et options d'amorce d'une liaison PPP et de description de ses caractéristiques.	"Traitement des options PPP" à la page 113

Pour plus d'informations sur les fichiers PPP, reportez-vous à la page de manuel `pppd`(1M). `pppd` (1M) comprend également les descriptions complètes de toutes les options disponibles pour la commande `pppd`. Vous trouverez des exemples de modèles pour tous les fichiers de configuration PPP dans `/etc/ppp`.

Traitement des options PPP

1. Le démon `pppd` réalise l'analyse suivante :

   Toutes les opérations Solaris PPP 4.0 sont traitées par le démon `pppd`, qui démarre lorsqu'un utilisateur exécute la commande `pppd`. Lorsqu'un utilisateur appelle un pair distant, les événements suivants se produisent :

   - `/etc/ppp/options`
   - `$HOME/.ppprc`
   - Tous les fichiers ouverts par l'option `file` ou `call` dans `/etc/ppp/options` et `$HOME/.ppprc`
2. `pppd` examine la ligne de commande afin de déterminer le périphérique en cours d'utilisation. Le démon n'interprète pas encore les options rencontrées.
3. `pppd` tente de détecter le périphérique série à utiliser en fonction des critères suivants :
   - Si un périphérique série est indiqué sur la ligne de commande, ou dans un fichier de configuration déjà traité, `pppd` utilise le nom de ce périphérique.
   - Si aucun périphérique série n'est nommé, `pppd` recherche l'option `notty`, `pty` ou `socket` sur la ligne de commande. Si l'une de ces options est spécifiée, `pppd` suppose qu'aucun nom de périphérique n'existe.
   - Dans le cas contraire, si `pppd` découvre que l'entrée standard est connectée à un tty, le nom du tty est utilisé.
   - Si `pppd` ne trouve toujours pas de périphérique série, `pppd` met fin à la connexion et émet un message d'erreur.
4. `pppd` vérifie alors l'existence du fichier `/etc/ppp/options.`*ttyname*. Si le fichier est trouvé, `pppd` l'analyse.
5. `pppd` traite toutes les options sur la ligne de commande.
6. `pppd` négocie le protocole LCP (Link Control Protocol) pour configurer la liaison.
7. (Facultatif) Si l'authentification est requise, `pppd` lit `/etc/ppp/pap-secrets` ou `/etc/ppp/chap-secrets` afin d'authentifier le pair opposé.

Le fichier `/etc/ppp/peers/`*peer-name* est lu lorsque le démon `pppd` rencontre l'option `call` *peer-name* sur la ligne de commande ou dans les autres fichiers de configuration.

Fonctionnement des privilèges du fichier de configuration PPP

La configuration d'Solaris PPP 4.0 configuration inclut concept de *privilèges*. Les privilèges déterminent l'ordre de priorité des options de configuration, en particulier lorsque la même option est appelée à plusieurs emplacements. Toute option appelée d'une source privilégiée est prioritaire sur la même option appelée d'une source non privilégiée.

Privilèges utilisateur

Le seul utilisateur privilégié est le superutilisateur (`root`), dont l'ID utilisateur est zéro. Tous les autres utilisateurs ne sont pas privilégiés.

Privilèges de fichier

Les fichiers de configuration suivants sont privilégiés, peu importe qui est leur propriétaire :

- `/etc/ppp/options`
- `/etc/ppp/options.`*ttyname*
- `/etc/ppp/peers/`*peer-name*

Le fichier `$HOME/.ppprc` appartient à l'utilisateur. Les options lues à partir de `$HOME/.ppprc` et de la ligne de commande sont privilégiées si l'utilisateur à l'origine de l'appel de `pppd` est `root` et uniquement à cette condition.

Les arguments qui suivent l'option `file` sont privilégiés.

Effets des privilèges d'option

Certaines options ne fonctionnent que si l'utilisateur ou la source à l'origine de l'appel est privilégié. Les options appelées sur la ligne de commande se voient affecter les privilèges de l'utilisateur qui exécute la commande `pppd`. Ces options ne sont pas privilégiées à moins que l'utilisateur qui appelle la commande `pppd` soit `root`.

Option	orphelin ?	Explication
`domain`	Privilégiée	Privilèges requis pour l'utiliser
`linkname`	Privilégiée	Privilèges requis pour l'utiliser
`noauth`	Privilégiée	Privilèges requis pour l'utiliser
`nopam`	Privilégiée	Privilèges requis pour l'utiliser
`pam`	Privilégiée	Privilèges requis pour l'utiliser
`plugin`	Privilégiée	Privilèges requis pour l'utiliser
`privgroup`	Privilégiée	Privilèges requis pour l'utiliser
`allow-ip` *addresses*	Privilégiée	Privilèges requis pour l'utiliser
`name` *hostname*	Privilégiée	Privilèges requis pour l'utiliser
`plink`	Privilégiée	Privilèges requis pour l'utiliser
`noplink`	Privilégiée	Privilèges requis pour l'utiliser

Option	orphelin ?	Explication
`plumbed`	Privilégiée	Privilèges requis pour l'utiliser
`proxyarp`	Devient privilégiée si `noproxyarp` a été spécifiée	Ne peut pas être ignorée par un utilisateur sans privilège
`defaultroute`	Privilégiée si `nodefaultroute` est définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`disconnect`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`bsdcomp`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	L'utilisateur sans privilège ne peut pas spécifier une taille de code plus grande que celle spécifiée par l'utilisateur privilégié
`deflate`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	L'utilisateur sans privilège ne peut pas spécifier une taille de code plus grande que celle spécifiée par l'utilisateur privilégié
`connect`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`init`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`pty`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`welcome`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
ttyname	Privilégiée si définie dans un fichier privilégié	Ouverte avec des permissions root quel que soit l'utilisateur qui appelle `pppd`.
	Non privilégiée si définie dans un fichier sans privilège	Ouverte avec les privilèges de l'utilisateur qui appelle `pppd`

Fichier de configuration `/etc/ppp/options`

Le fichier `/etc/ppp/options` permet de définir des options s'appliquant à l'ensemble des communications PPP sur la machine locale. Le fichier `/etc/ppp/options` est privilégié. `/etc/ppp/options` doit appartenir à l'utilisateur root, bien que `pppd` n'impose pas cette règle. Les options que vous définissez dans `/etc/ppp/options` sont prioritaires sur les définitions des mêmes options dans tous les autres fichiers et sur la ligne de commande.

Les options classiques que vous pouvez être amené à utiliser dans `/etc/ppp/options` incluent les suivantes :

- **`lock`** : permet le verrouillage de fichier de type UUCP.
- **`noauth`** : indique que la machine n'authentifie pas les appelants.

Remarque - Le logiciel Solaris PPP 4.0 ne comprend aucun fichier `/etc/ppp/options` par défaut. La commande `pppd` peut fonctionner sans le fichier `/etc/ppp/options`. Si une machine ne dispose pas d'un fichier `/etc/ppp/options` , seul l'utilisateur `root` peut exécuter la commande `pppd` sur cette machine.

Vous devez créer le fichier `/etc/ppp/options` à l'aide d'un éditeur de texte, comme illustré dans la section “Définition des communications sur la ligne série ” à la page 49. Si une machine ne nécessite pas d'options globales, créez un fichier `/etc/ppp/options` vide. Ensuite, l'utilisateur `root` et les utilisateurs standard peuvent exécuter `pppd` sur la machine locale.

Modèle `/etc/ppp/options.tmpl`

`/etc/ppp/options.tmpl` contient des commentaires utiles à propos du fichier `/etc/ppp/options` ainsi que de trois options courantes du fichier `/etc/ppp/options` général.

```
lock
nodefaultroute
noproxyarp
```

Option	Définition
`lock`	Active le verrouillage de fichier de type UUCP
`nodefaultroute`	Spécifie qu'aucune route par défaut n'est définie
`noproxyarp`	Rejette `proxyarp`

Pour utiliser `/etc/ppp/options.tmpl` en tant que fichier d'options globales, renommez `/etc/ppp/options.tmpl` en `/etc/ppp/options`. Ensuite, modifiez le contenu du fichier en fonction des besoins de votre site.

Où trouver des exemples des fichiers `/etc/ppp/options`

Les sections suivantes contiennent des exemples du fichier `/etc/ppp/options` :

- Pour une machine d'appel sortant, reportez-vous à la section “Définition des communications sur la ligne série ” à la page 49
- Pour un serveur d'appel entrant, reportez-vous à la section “Définition des communications sur la ligne série (serveur d'appel entrant) ” à la page 56
- Pour la prise en charge PAP sur un serveur d'appel entrant, reportez-vous à la section “Ajout de la prise en charge PAP dans les fichiers de configuration PPP (serveur d'appel entrant)” à la page 71

- Pour la prise en charge PAP sur une machine d'appel sortant, reportez-vous à la section “Ajout de la prise en charge PAP dans les fichiers de configuration PPP (machine d'appel sortant)” à la page 74
- Pour la prise en charge CHAP sur un serveur d'appel entrant, reportez-vous à la section “Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (serveur d'appel entrant)” à la page 79.

Fichier de configuration `/etc/ppp/options.`*ttyname*

Vous pouvez configurer les caractéristiques des communications sur la ligne série dans le fichier `/etc/ppp/options.`*ttyname*. `/etc/ppp/options.`*ttyname* est un fichier privilégié, lu par la commande `pppd` après l'analyse des fichiers `/etc/ppp/options` et `$HOME/.pppрc` existants. Autrement, `pppd` lit `/etc/ppp/options.`*ttyname* après l'analise de `/etc/ppp/options`.

ttyname est utilisé dans le cadre des liaisons de ligne spécialisées et commutées. *ttyname* représente un port série particulier sur une machine, comme `cua/a` ou `cua/b`, à laquelle un modem ou un adaptateur de terminal RNIS peut être connecté.

Au moment d'attribuer un nom au fichier `/etc/ppp/options.`*ttyname*, remplacez la barre oblique (/) dans le nom de périphérique par un point (.). Par exemple, le fichier `options` du périphérique `cua/b` doit être nommé `/etc/ppp/options.cua.b.`.

Remarque - Solaris PPP 4.0 peut fonctionner sans le fichier `/etc/ppp/options.` *ttyname*. Votre serveur peut avoir une seule ligne série dédiée à PPP. En outre, le serveur nécessite peu d'options. Dans ce cas, vous pouvez spécifier les options requises dans un autre fichier de configuration ou sur la ligne de commande.

Utilisation de `/etc/ppp/options.`*ttyname* sur un serveur d'appel entrant

Pour une liaison commutée, vous pouvez choisir de créer des fichiers `/etc/ppp/options.`*ttyname* pour chaque port série sur un serveur d'appel entrant avec modem. Des options standard sont répertoriées ci-dessous :

- Adresse IP requise par le serveur d'appel entrant

  Définissez cette option si vous demandez aux appelants sur le port série *ttyname* d'utiliser une adresse IP particulière. Il est possible que votre espace d'adresse ait un nombre limité d'adresses IP disponibles pour PPP, par rapport au nombre d'appelants éventuels. Dans ce cas, envisagez d'assigner une adresse IP à chaque interface série utilisée pour PPP sur le serveur d'appel entrant. Cette affectation applique l'adressage dynamique pour PPP.
- `asyncmap` *map-value*

L'option `asyncmap` configure les caractères de contrôle que le modem ou adaptateur de terminal RNIS spécifique ne peut pas recevoir par le biais de la ligne série. Lorsque l'option `xonxoff` est utilisée, `pppd` définit automatiquement l'option asyncmap sur 0xa0000.

map-value indique, au format hexadécimal, les caractères de contrôle problématiques.

- `init "chat -U -f /etc/ppp/mychat"`

  L'option `init` indique au modem d'initialiser les communications sur la ligne série à l'aide des informations contenues dans la commande `chat -U`. Le modem utilise la chaîne de discussion dans le fichier `/etc/ppp/mychat`.

- Les paramètres de sécurité répertoriés dans la page de manuel `pppd`(1m)

Utilisation `/etc/ppp/options.`*ttyname* sur une machine d'appel sortant

Dans le cadre d'un système d'appel sortant, vous pouvez soit créer un fichier `/etc/ppp/options.` *ttyname* pour le port série connecté au modem, soit décider de ne pas utiliser `/etc/ppp/options.`*ttyname*.

Remarque - Solaris PPP 4.0 peut fonctionner sans le fichier `/etc/ppp/options.` *ttyname*. Une machine d'appel sortant peut avoir une seule ligne série pour PPP. En outre, la machine d'appel sortant peut nécessiter peu d'options. Vous pouvez spécifier les options requises dans un autre fichier de configuration ou sur la ligne de commande.

Fichier modèle `options.ttya.tmpl`

Le fichier `/etc/ppp/options.ttya.tmpl` contient des commentaires utiles concernant le fichier `/etc/ppp/options.`*tty-name*. Le modèle contient trois options courantes pour le fichier `/etc/ppp/options.`*tty-name*.

```
38400
asyncmap 0xa0000
:192.168.1.1
```

Option	Définition
`38400`	Utilisez ce débit en bauds pour le port ttya.
`asyncmap 0xa0000`	Affectez à asyncmap la valeur 0xa0000 de telle sorte que la machine locale puisse communiquer avec les pairs interrompus.
`:192.168.1.1`	Affectez l'adresse IP 192.168.1.1 à tous les pairs qui lancent un appel sur la liaison.

Pour utiliser `/etc/ppp/options.ttya.tmpl` sur votre site, renommez `/etc/ppp/options.tmpl` en `/etc/ppp/options.`*ttya-name*. Remplacez *ttya-name* par le nom du port série connecté au modem. Puis, modifiez le contenu du fichier en fonction des besoins de votre site.

Où trouver des exemples des fichiers `/etc/ppp/options.`*ttyname*

Les sections suivantes contiennent des exemples du fichier `/etc/ppp/options.`*ttyname* :

- Pour une machine d'appel sortant, reportez-vous à la section “Définition des communications sur la ligne série ” à la page 49
- Pour un serveur d'appel entrant, reportez-vous à la section “Définition des communications sur la ligne série (serveur d'appel entrant) ” à la page 56

Configuration des options spécifiques à l'utilisateur

Cette section contient des informations détaillées à propos de la configuration des utilisateurs sur le serveur d'appel entrant.

Configuration de `$HOME/.ppprc` sur un serveur d'appel entrant

Le fichier `$HOME/.ppprc` est destiné aux utilisateurs qui configurent des options PPP préférées. En tant qu'administrateur, vous pouvez également configurer `$HOME/.ppprc` pour les utilisateurs.

Les options de `$HOME/.ppprc` sont privilégiées lorsque l'utilisateur qui appelle le fichier est lui-même privilégié, et à cette seule condition.

Lorsqu'un appelant utilise la commande `pppd` pour lancer un appel, `.ppprc` est le deuxième fichier que le démon `pppd` vérifie.

La section “Configuration des utilisateurs du serveur d'appel entrant ” à la page 55 contient des instructions sur la configuration de `$HOME/.ppprc` sur le serveur d'appel entrant.

Configuration de `$HOME/.ppprc` sur une machine d'appel sortant

Le fichier `$HOME/.ppprc` n'est pas nécessaire sur la machine d'appel sortant pour que Solaris PPP 4.0 fonctionne correctement. En outre, une machine d'appel sortant ne nécessite pas

un fichier `$HOME/.ppprc`, sauf dans des cas particuliers. Créez un ou plusieurs fichiers `.ppprc` si vous effectuez les opérations suivantes :

- Vous autorisez plusieurs utilisateurs ayant des besoins différents en matière de communication à appeler des pairs distants à partir de la même machine. Dans ce cas, créez des fichiers `.ppprc` distincts dans les répertoires personnels de chaque utilisateur devant effectuer un appel sortant.
- Vous devez spécifier des options qui gèrent les problèmes spécifiques à votre liaison, comme la désactivation de la compression Van Jacobson. L'ouvrage *PPP Design, Implementation, and Debugging* de James Carlson et la page de manuel pppd(1M) vous aideront à résoudre les problèmes de liaison.

Dans la mesure où le fichier `.ppprc` est plus souvent utilisé dans le cadre de la configuration d'un serveur d'appel entrant, reportez-vous à la section “Configuration des utilisateurs du serveur d'appel entrant ” à la page 55 pour obtenir les instructions de configuration de `.ppprc`.

Spécification des informations relatives à la communication avec le serveur d'appel entrant

Pour communiquer avec un serveur d'appel entrant, vous devez rassembler des informations le concernant. Modifiez ensuite un petit nombre de fichiers. Plus concrètement, vous devez configurer les exigences en matière de communication de tous les serveurs d'appel entrant que la machine d'appel sortant doit appeler. Vous pouvez spécifier des options sur un serveur d'appel entrant, tel que le numéro de téléphone du FAI, dans le fichier `/etc/ppp/options.`*ttyname*. Cependant, le meilleur emplacement pour configurer les informations de pair est le fichier `/etc/ppp/peers/`*peer-name*.

Fichier `/etc/ppp/peers/`*peer-name*

Remarque - Le fichier `/etc/ppp/peers/`*peer-name* n'est pas nécessaire sur la machine d'appel sortant pour que Solaris PPP 4.0 fonctionne correctement.

Utilisez le fichier `/etc/ppp/peers/`*peer-name* pour fournir des informations relatives à la communication avec un pair particulier. Le fichier `/etc/ppp/peers/` *peer-name* autorise les utilisateurs ordinaires à appeler des options privilégiées présélectionnées qu'ils ne sont pas autorisés à définir.

Par exemple, un utilisateur sans privilège ne peut pas ignorer l'option `noauth` si `noauth` est spécifiée dans le fichier `/etc/ppp/peers/`*peer-name*. Supposons que l'utilisateur souhaite configurer une liaison à `peerB`, qui ne fournit pas d'informations d'authentification. En tant que

superutilisateur, vous pouvez créer un fichier `/etc/ppp/peers/peerB` qui comprend l'option `noauth`. L'option `noauth` indique que la machine locale n'authentifie pas les appels de `peerB`.

Le démon `pppd` lit `/etc/ppp/peers/`*peer-name* quand `pppd` rencontre l'option suivante :

`call` *peer-name*

Vous pouvez créer un fichier `/etc/ppp/peers/`*peer-name* pour chaque pair cible avec lequel la machine d'appel sortant doit communiquer. Cette pratique est particulièrement utile pour autoriser les utilisateurs ordinaires à appeler les liaisons d'appel sortant spécifiques sans avoir besoin des privilèges root.

Les options suivantes sont fréquemment spécifiées dans `/etc/ppp/peers/`*peer-name* :

- `user` *user-name*

  Fournissez *user-name* au serveur d'appel entrant comme nom de connexion à la machine d'appel sortant, lors de l'authentification avec PAP ou CHAP.

- `remotename` *peer-name*

  Utilisez *peer-name* comme nom de la machine d'appel entrant. L'option `remotename` est utilisée avec l'authentification PAP ou CHAP lors de l'analyse des fichiers `/etc/ppp/pap-secrets` ou `/etc/ppp/chap-secrets`.

- `connect "chat` *chat_script*`..."`

  Ouvrez la communication vers le serveur d'appel entrant à l'aide des instructions fournies dans le script de discussion.

- `noauth`

  N'authentifiez pas le pair *peer-name* lors de l'initialisation des communications.

- `noipdefault`

  Définissez la première adresse IP utilisée dans la négociation avec le pair sur 0.0.0.0. Utilisez `noipdefault` lors de la configuration d'une liaison vers la plupart des fournisseurs d'accès Internet pour faciliter la négociation IPCP entre les pairs.

- `defaultroute`

  Installez une route IPv4 par défaut lorsque l'adresse IP est établie sur la liaison.

La page de manuel `pppd`(1M) contient plus d'options qui peuvent s'appliquer à un pair cible spécifique.

Fichier modèle `/etc/ppp/peers/myisp.tmpl`

Le fichier `/etc/ppp/peers/myisp.tmpl` contient des commentaires utiles à propos du fichier `/etc/ppp/peers/`*peer-name*. Le modèle se termine par des options courantes que vous pouvez utiliser pour un fichier `/etc/ppp/peers/`*peer-name* :

```
connect "/usr/bin/chat -f /etc/ppp/myisp-chat"
```

```
user myname
remotename myisp
noauth
noipdefault
defaultroute
updetach
noccp
```

Option	Définition
`connect "/usr/bin/chat -f /etc/ppp/myisp-chat"`	Appelez le pair à l'aide du script de discussion `/etc/ppp/myisp-chat`.
`user myname`	Utilisez ce nom de compte pour la machine locale. `myname` est le nom de cette machine dans le fichier `/etc/ppp/pap-secrets` du pair.
`remotename myisp`	Reconnaissez `myisp` comme le nom du pair dans le fichier `/etc/ppp/pap-secrets` de la machine locale.
`noauth`	N'exigez pas des pairs qui effectuent des appels qu'ils fournissent des informations d'authentification.
`noipdefault`	N'utilisez pas une adresse IP par défaut pour la machine locale.
`defaultroute`	Utilisez la route par défaut qui est affectée à la machine locale.
`updetach`	Consignez les erreurs dans les fichiers journaux PPP, plutôt que sur la sortie standard.
`noccp`	N'utilisez pas la compression CCP.

Pour utiliser `/etc/ppp/peers/myisp.tmpl` sur votre site, renommez `/etc/ppp/peers/myisp.tmpl` en `/etc/ppp/peers/`*peer-name*. Remplacez *peer-name* par le nom du pair à appeler. Puis, modifiez le contenu du fichier en fonction des besoins de votre site.

Où trouver des exemples des fichiers `/etc/ppp/peers/`*peer-name*

Les sections suivantes contiennent des exemples de fichiers `/etc/ppp/peers/`*peer-name* :

- Pour une machine d'appel sortant, reportez-vous à la section “Définition de la connexion à un pair donné” à la page 51.
- Pour une machine locale sur une ligne spécialisée, reportez-vous à la section “Configuration d'une machine sur une ligne spécialisée ” à la page 64.
- Pour la prise en charge de l'authentification PAP sur une machine d'appel sortant, reportez-vous à la section “Ajout de la prise en charge PAP dans les fichiers de configuration PPP (machine d'appel sortant)” à la page 74

- Pour la prise en charge de l'authentification CHAP sur une machine d'appel sortant, reportez-vous à la section “Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (machine d'appel sortant)” à la page 81
- Pour la prise en charge du protocole PPPoE sur un système client, reportez-vous à la section “Configuration du client PPPoE” à la page 84.

Configuration de la vitesse du modem pour une liaison commutée

Le problème principal posé par la configuration du modem est de désigner la vitesse à laquelle le modem doit fonctionner. Les recommandations suivantes s'appliquent aux modems utilisés avec les ordinateurs Sun Microsystems :

- Anciens systèmes SPARC : vérifiez la documentation du matériel qui accompagne le système. De nombreuses machines SPARCstation™ exigent que la vitesse du modem soit inférieure à 38 400 bps.
- Machines UltraSPARC® : définissez la vitesse du modem sur 115 200 bps, ce qui s'avère utile avec les modems modernes et suffisamment rapide pour une liaison commutée. Si vous prévoyez d'utiliser un adaptateur de terminal RNIS à double canal avec compression, il vous faudra augmenter la vitesse du modem. La limite sur les machines UltraSPARC est de 460 800 bps pour une liaison asynchrone.

Pour une *machine d'appel sortant*, définissez la vitesse du modem dans les fichiers de configuration PPP, tels que `/etc/ppp/peers/`*peer-name* ou spécifiez la vitesse en tant qu'option de la commande `pppd`.

Pour un *serveur d'appel entrant*, vous devez définir la vitesse à l'aide de l'utilitaire `ttymon` comme décrit dans la section “Configuration des périphériques sur le serveur d'appel entrant ” à la page 53.

Définition de la conversation sur la liaison commutée

La machine d'appel sortant et son pair distant communiquent via la liaison PPP, par négociation et échange de diverses instructions. Lors de la configuration d'une machine d'appel sortant, vous devez déterminer les instructions requises par les modems locaux et distants. Ensuite, vous créez un fichier appelé un script de discussion, qui contient ces instructions. Cette section contient des informations relatives à la configuration des modems et à la création des scripts de discussion.

Contenu du script de discussion

Chaque pair distant auquel la machine d'appel sortant doit se connecter a probablement besoin de son propre script de discussion.

Remarque - Les scripts de discussion sont habituellement utilisés sur les liaisons commutées uniquement. Les liaisons de ligne spécialisées n'utilisent pas les scripts de discussion à moins qu'elles ne comportent une interface asynchrone qui nécessite une configuration de démarrage.

Le contenu du script de discussion est déterminé par les exigences de votre modem ou adaptateur de terminal RNIS et le pair distant. Ce contenu s'affiche sous la forme d'un jeu de chaînes expect-send. La machine d'appel sortant et ses pairs distants échangent ces chaînes dans le cadre du processus d'initialisation des communications.

Une chaîne *expect* contient des caractères que la machine hôte d'appel sortant attend de recevoir du pair distant pour amorcer le dialogue. Une chaîne *send* contient des caractères que la machine d'appel sortant envoie au pair distant après la réception de la chaîne expect.

Le script de discussion contient habituellement les informations suivantes :

- Des commandes de modem, souvent appelées *commandes AT*, qui permettent au modem de transmettre des données par téléphone
- Le numéro de téléphone du pair cible

  Ce numéro de téléphone peut être le numéro requis par votre fournisseur d'accès à Internet, un serveur d'appel entrant sur un site d'entreprise ou une machine spécifique.
- Le délai d'expiration, si nécessaire
- La séquence de connexion attendue du pair distant
- La séquence de connexion envoyée par la machine d'appel sortant

Exemples de scripts de discussion

Cette section contient des scripts de discussion que vous pouvez utiliser comme référence pour créer vos propres scripts de discussion. Le manuel du fabricant de votre modem et les informations fournies par votre fournisseur d'accès Internet et d'autres hôtes cible contiennent les exigences du modem et de vos pairs cible en matière de discussion. En outre, de nombreux sites Web PPP proposent des exemples de scripts de discussion.

Script de discussion de modem de base

Le script de discussion de base ci-après peut vous servir de modèle lorsque vous créerez vos propres scripts de discussion.

```
ABORT    BUSY
```

```
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
"" AT&F1M0&M5S2=255
SAY     "Calling myserver\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
ogin: pppuser
ssword: \q\U
% pppd
```

Le tableau suivant décrit le contenu du script de discussion.

Contenu du script	Explication
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER'`	Abandon de la transmission si le modem signale `ABORT 'NO CARRIER'` lors de la numérotation. L'échec de la numérotation ou de la négociation du modem génère généralement ce message.
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes. La réponse du modem doit être immédiate.
`"" AT&F1M0&M5S2=255`	`M0` : désactivation du haut-parleur pendant la connexion. `&M5` : le modem requiert le contrôle d'erreur. `S2=255` : désactivation de la séquence d'interruption TIES "+++"
`SAY "Calling myserver\n"`	Affichage du message `Calling myserver` sur la machine locale.
`TIMEOUT 60`	Réinitialisation du délai d'attente de 60 secondes pour laisser plus de temps à la négociation de liaison.
`OK "ATDT1-123-555-1212"`	Appel du pair distant à l'aide du numéro de téléphone 123-555-1212.
`ogin: pppuser`	Connexion au pair à l'aide d'une connexion de type UNIX Indiquer le nom d'utilisateur `pppuser`.
`ssword: \q\U`	`\q` : ne pas se connecter si le débogage est effectué avec l'option `-v`. `\U` : insérer à cet emplacement le contenu de la chaîne qui suit `-U`, spécifié sur la ligne de commande. Généralement, la chaîne contient le mot de passe.
`% pppd`	Attendre l'invite shell % et exécuter la commande `pppd`.

Modèle de script de discussion `/etc/ppp/myisp-chat.tmpl`

Cette version inclut le modèle `/etc/ppp/myisp-chat.tmpl`, que vous pouvez modifier pour l'utiliser sur votre site. Le modèle `/etc/ppp/myisp-chat.tmpl` ressemble au script de discussion de modem de base, à ceci près qu'il n'inclut pas une séquence de connexion.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
""      "AT&F1"
OK      "AT&C1&D2"
SAY     "Calling myisp\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
```

Contenu du script	Explication
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER`	Abandon de la transmission si le modem signale `ABORT 'NO CARRIER'` lors de la numérotation. L'échec de la numérotation ou de la négociation du modem génère généralement ce message.
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes. La réponse du modem doit être immédiate.
`"" "AT&F1"`	Rétablissement des valeurs par défaut du modem.
`OK "AT&C1&D2"`	Réinitialisation du modem afin que, pour &C1, le DCD du modem suive la porteuse. Si le côté distant raccroche le téléphone pour une raison quelconque, le DCD diminue. Pour &D2, la transition DTR décroissante fait raccrocher le modem.
`SAY "Calling myisp\n"`	Affichage du message "Calling myisp" sur la machine locale.
`TIMEOUT 60`	Réinitialisation du délai d'attente de 60 secondes pour laisser plus de temps à la négociation de liaison.
`OK "ATDT1-123-555-1212"`	Appel du pair distant à l'aide du numéro de téléphone 123-555-1212.
`CONNECT \c`	Attendre que le modem du pair opposé envoie le message `CONNECT`.

Script de discussion du modem pour appeler le fournisseur d'accès Internet

Utilisez le script de discussion suivant comme modèle pour appeler un fournisseur d'accès à Internet (FAI) à partir d'une machine d'appel sortant équipée d'un modem U.S. Robotics Courier.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
"" AT&F1M0&M5S2=255
SAY     "Calling myisp\n"
```

```
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

Le tableau ci-dessous décrit le contenu du script de discussion.

Contenu du script	Explication
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER'`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes. La réponse du modem doit être immédiate.
`"" AT&F1M0M0M0M0&M5S2=255`	`M0` : désactivation du haut-parleur pendant la connexion. `&M5` : le modem requiert le contrôle d'erreur. `S2=255` : désactivation de la séquence d'interruption TIES "+++"
`SAY "Calling myisp\n"`	Affichage du message `Calling myisp` sur la machine locale.
`TIMEOUT 60`	Réinitialisation du délai d'attente de 60 secondes pour laisser plus de temps à la négociation de liaison.
`OK "ATDT1-123-555-1212"`	Appel du pair distant à l'aide du numéro de téléphone 123-555-1212.
`CONNECT \c`	Attendre que le modem du pair opposé envoie le message `CONNECT`.
`\r \d\c`	Patienter jusqu'à la fin du message `CONNECT`.
SAY "Connected; running PPP\n"	Affichage du message d'informations `Connected; running PPP` sur la machine locale.

Script de discussion de base amélioré pour une connexion de type UNIX

Le script de discussion suivant est un script de base amélioré pour appeler un pair Oracle Solaris distant ou un autre pair de type UNIX. Ce script de discussion est utilisé à la section “Création des instructions pour l'appel d'un pair” à la page 50.

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&F1&M5S2=255
TIMEOUT 60
```

```
OK ATDT1-123-555-1234
CONNECT \c
SAY "Connected; logging in.\n"
TIMEOUT 5
ogin:--ogin: pppuser
TIMEOUT 20
ABORT 'ogin incorrect'
ssword: \qmypassword
"% " \c
SAY "Logged in.  Starting PPP on peer system.\n"
ABORT 'not found'
"" "exec pppd"
~ \c
```

Le tableau ci-dessous décrit les paramètres du script de discussion.

Contenu du script	Explication
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes. La réponse du modem doit être immédiate.
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER'`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT ERROR`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`"" AT&F1&M5S2=255`	`&M5` : le modem requiert le contrôle d'erreur. `S2=255` : désactivation de la séquence d'interruption TIES "+++"
`TIMEOUT 60`	Réinitialisation du délai d'attente de 60 secondes pour laisser plus de temps à la négociation de liaison.
`OK ATDT1-123-555-1234`	Appel du pair distant à l'aide du numéro de téléphone 123-555-1212.
`CONNECT \c`	Attendre que le modem du pair opposé envoie le message `CONNECT`.
`SAY "Connected; logging in.\n"`	Affichage du message d'informations `Connected; logging in` sur l'état de l'utilisateur.
`TIMEOUT 5`	Modification du délai d'expiration pour activer l'affichage rapide de l'invite de connexion.
`ogin:--ogin: pppuser`	Attendre l'invite de connexion. Si l'invite n'est pas reçue, envoyer un RETURN et attendre. Envoyer ensuite le nom d'utilisateur `pppuser` au pair. La séquence qui suit est désignée par la plupart des FAI en tant que connexion PAP. Cependant, la connexion PAP n'est pas liée de quelque façon que ce soit à l'authentification PAP.
`TIMEOUT 20`	Remplacer la valeur du délai d'expiration par 20 secondes pour permettre une vérification lente du mot de passe.

Contenu du script	Explication
`ssword: \qmysecrethere`	Attendre l'invite de mot de passe du pair. A la réception de l'invite, envoyer le mot de passe `\qmysecrethere`. L'option `\q` empêche l'écriture du mot de passe sur les fichiers journaux du système.
`"% " \c`	Attendre l'invite shell du pair. Le script de discussion utilise le shell C. Modifier cette valeur si l'utilisateur préfère se connecter avec un shell différent.
`SAY "Logged in. Starting PPP on peer system. \n"`	Affichage du message d'information `Logged in. Starting PPP on peer system` sur l'état de l'utilisateur.
`ABORT 'not found'`	Abandon de la transmission si le shell rencontre des erreurs.
`"" "exec pppd"`	Démarrage de `pppd` sur le pair.
`~ \c`	Attendre que PPP démarre sur le pair.

Le démarrage PPP juste après `CONNECT \c` est souvent appelé *connexion PAP* par les fournisseurs d'accès Internet (FAI) bien que la connexion PAP ne fasse pas partie de l'authentification PAP.

L'expression `ogin:--ogin: pppuser` indique au modem d'envoyer le nom d'utilisateur `pppuser` en réponse à l'invite de connexion du serveur d'appel entrant. `pppuser` est un nom de compte utilisateur PPP créé spécialement pour l'utilisateur distant `user1` sur le serveur d'appel entrant. Pour obtenir des instructions sur la création de comptes utilisateur PPP sur les serveurs d'appel entrant, reportez-vous à la section “Configuration des utilisateurs du serveur d'appel entrant ” à la page 55.

Script de discussion pour adaptateur de terminal RNIS externe

Le script de discussion suivant sert à appeler à partir d'une machine d'appel sortant équipée d'un terminal ISDN `ZyXEL omni.net`..

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255
OK ATDI18882638234
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

Le tableau ci-dessous décrit les paramètres du script de discussion.

Contenu du script	Explication
`SAY "Calling the peer"`	Affichage de ce message sur l'écran de la machine d'appel sortant.
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes.
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER'`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT ERROR`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255`	Les lettres dans cette ligne ont la signification suivante : ■ `&F` : utiliser les valeurs d'usine ■ `B40` : effectuer une conversion PPP asynchrone ■ `S83.7=1` : utiliser les données sur support vocal ■ `&K44` : activer la compression CCP ■ `&J3` : activer MP ■ `X7` : signaler les vitesses côté DCE ■ `S61.3=1` : utiliser la fragmentation des paquets ■ `S0=0` : aucune réponse automatique ■ `S2=255` : désactiver l'échappement TIES
`OK ATDI18882638234`	Réalisation d'un appel RNIS. Pour les liaisons multiples, le deuxième appel est passé au même numéro de téléphone, ce que la plupart des FAI requièrent habituellement. Si le pair distant requiert un deuxième numéro de téléphone différent, ajoutez "+ *nnnn*.". *nnnn* représente le deuxième numéro de téléphone.
`CONNECT \c`	Patientez jusqu'à ce que le message `CONNECT` du modem du pair opposé s'affiche.
`\r \d\c`	Patienter jusqu'à la fin du message `CONNECT`.
`SAY "Connected; running PPP\n"`	Affichage de ce message sur l'écran de la machine d'appel sortant.

Pour obtenir la description des options et d'autres informations détaillées sur le script de discussion, reportez-vous à la page de manuel `chat`(1M). Pour obtenir une explication sur les chaînes expect-send, reportez-vous à la section “Champ Phone du fichier `/etc/uucp/Systems`” à la page 183.

Pour d'autres exemples de scripts de discussion

Certains sites web offrent des exemples et leur assistance pour vous permettre de créer vos scripts de discussion. Visitez, par exemple, http://ppp.samba.org/ppp/index.html.

Appel du script de discussion

Pour appeler un script de discussion, utilisez l'option `connect`. Vous pouvez utiliser `connect "chat ..."` dans tous les fichiers de configuration PPP ou sur la ligne de commande.

Les scripts de discussion ne sont pas exécutables, mais le programme appelé par `connect` doit l'être. L'utilitaire de discussion peut servir de programme devant être appelé par `connect`. Dans cet exemple, si vous stockez le script de discussion dans un fichier externe à l'aide de l'option `-f`, votre fichier de script de discussion n'est pas exécutable.

Le programme `chat` décrit dans `chat`(1m) exécute le script de discussion réel. Le démon `pppd` appelle le programme `chat` chaque fois que `pppd` rencontre l'option `connect "chat ..."`.

Remarque - Vous pouvez utiliser n'importe quel programme externe, tel que `Perl` ou `Tcl`, afin de créer des scripts de discussion perfectionnés. L'utilitaire `chat` est fourni pour votre convenance.

▼ Appel d'un script de discussion (tâche)

1. **Créez le script de discussion sous forme de fichier ASCII.**

2. **Appelez le script de discussion dans un fichier de configuration PPP à l'aide de la syntaxe suivante :**

   ```
   connect 'chat  -f /etc/ppp/chatfile'
   ```

   L'indicateur `-f` indique qu'un nom de fichier doit suivre. */etc/ppp/chatfile* représente le nom du fichier de discussion.

3. **Accordez l'autorisation de lecture du fichier de discussion externe à l'utilisateur qui exécute la commande `pppd`.**

Attention - Le programme de discussion est toujours exécuté avec les privilèges de l'utilisateur, même si l'option `connect 'chat ...'` est appelée à partir d'une source privilégiée. Par conséquent, un autre fichier de discussion lu avec l'option `-f` doit être lisible par l'utilisateur à l'origine de l'appel. Ce privilège risque de poser un problème de sécurité si le script de discussion contient des mots de passe ou d'autres informations confidentielles.

Exemple 8-1 Script de discussion en ligne

Vous pouvez placer l'intégralité de la conversation du script de discussion sur une seule ligne, comme dans l'exemple suivant :

```
connect 'chat "" "AT&F1" OK ATDT5551212 CONNECT "\c"'
```

Le script de discussion complet suit le mot-clé `chat`. Le script se termine par `"\c"'`. Vous utilisez cette forme dans tous les fichiers de configuration PPP ou sur la ligne de commande en tant qu'argument de `pppd` .

Script de discussion dans un fichier externe

Si le script de discussion nécessaire à un pair donné est long ou complexe, vous pouvez envisager de le créer sous forme de fichier séparé. Les fichiers de discussion externes sont faciles à gérer et à documenter. Vous pouvez ajouter des commentaires au fichier de discussion en les faisant précéder du signe dièse (#).

La section “Création des instructions pour l'appel d'un pair” à la page 50 présente la procédure d'utilisation d'un script de discussion contenu dans un fichier externe.

Création d'un fichier de discussion exécutable

Vous pouvez créer un fichier de discussion à exécuter automatiquement à l'initialisation de la liaison commutée. Ainsi, vous pouvez exécuter des commandes supplémentaires au cours de l'initialisation de la liaison, comme `stty` pour les paramètres de parité, outre les commandes contenues dans un script de discussion classique.

Ce script de discussion exécutable se connecte à un système UNIX de type ancien qui nécessite 7 bits de même parité. Le système passe alors à 8 bits sans parité lors de l'exécution de PPP.

```
#!/bin/sh
chat "" "AT&F1" OK "ATDT555-1212" CONNECT "\c"
stty evenp
chat ogin: pppuser ssword: "\q\U" % "exec pppd"
stty -evenp
```

▼ Création d'un programme de discussion exécutable

1. **Utilisez votre éditeur de texte pour créer un programme de discussion exécutable, comme dans l'exemple précédent.**
2. **Rendez le programme de discussion exécutable.**

   ```
   # chmod +x /etc/ppp/chatprogram
   ```

3. **Appelez le programme de discussion.**

   ```
   connect /etc/ppp/chatprogram
   ```

   Il n'est pas nécessaire que les programmes de discussion résident dans le système de fichiers `/etc/ppp`. Vous pouvez stocker les programmes de discussion dans n'importe quel emplacement.

Authentification des appelants sur une liaison

Cette section explique le fonctionnement des protocoles d'authentification PPP et décrit les bases de données qui leur sont associées.

Protocole d'authentification par mot de passe (PAP)

L'authentification PAP est similaire dans son fonctionnement au programme `login` d'UNIX, à ceci près que PAP n'accorde pas l'accès shell à l'utilisateur. PAP utilise les fichiers de configuration PPP et la base de données PAP sous forme de fichier `/etc/ppp/pap-secrets` pour configurer l'authentification. PAP utilise également `/etc/ppp/pap-secrets` pour définir les informations d'identification de sécurité PAP. Les informations d'identification se composent d'un nom de pair, "nom d'utilisateur" dans le jargon PAP, et d'un mot de passe. Les informations d'identification PAP contiennent également les informations associées à chaque appelant autorisé à se connecter à la machine locale. Les noms d'utilisateur et mots de passe PAP peuvent être identiques aux noms d'utilisateur et mots de passe UNIX de la base de données de mots de passe, ou bien différents.

Fichier `/etc/ppp/pap-secrets`

La base de données PAP est mise en oeuvre dans le fichier `/etc/ppp/pap-secrets`. Pour que l'authentification réussisse, les informations d'identification PAP des machines situées des deux

côtés de la liaison PPP doivent être correctement configurées dans les fichiers `/etc/ppp/pap-secrets`. L'appelant (l'authentifié) fournit les informations d'identification dans les colonnes `user` et `password` du fichier `/etc/ppp/pap-secrets` ou dans le fichier `+ua` obsolète. Le serveur (l'authentificateur) valide les informations d'identification par rapport aux informations contenues dans le fichier `/etc/ppp/pap-secrets`, par l'intermédiaire de la base de données UNIX `passwd` ou de l'utilitaire PAM.

La syntaxe du fichier `/etc/ppp/pap-secrets` est la suivante.

```
myclient ISP-server mypassword *
```

Signification des paramètres .

`myclient`	Nom d'utilisateur PAP de l'appelant. Ce nom est souvent identique au nom d'utilisateur UNIX de l'appelant, en particulier si le serveur d'appel entrant utilise l'option `login` de PAP.
`ISP-server`	Nom de la machine distante, souvent un serveur d'appel entrant.
`mypassword`	Mot de passe PAP de l'appelant.
`*`	Adresse IP associée à l'appelant. L'astérisque (*) représente n'importe quelle adresse IP.

Création de mots de passe PAP

Les mots de passe PAP sont envoyés via la liaison *en clair*, c'est-à-dire dans un format ASCII lisible. Pour l'appelant (l'authentifié), le mot de passe PAP doit être stocké en clair dans l'un des emplacements suivants :

- dans `/etc/ppp/pap-secrets` ;
- dans un autre fichier externe ;
- dans un tube nommé par le biais de la fonction `pap-secrets @` ;
- en tant qu'option de `pppd`, sur la ligne de commande ou dans un fichier de configuration PPP ;
- par l'intermédiaire du fichier `+ua`.

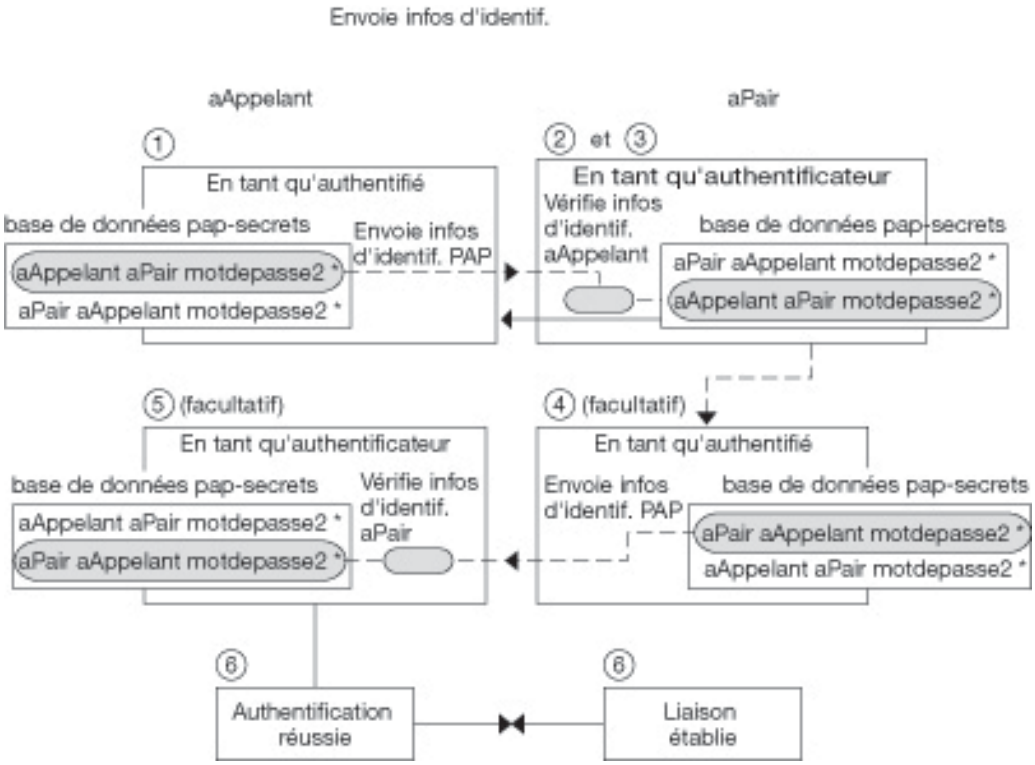
Sur le serveur (l'authentificateur), vous pouvez masquer le mot de passe PAP en effectuant l'une des opérations suivantes :

- Spécifiez `papcrypt` et utilisez des mots de passe hachés par la commande `encrypt` dans le fichier `pap-secrets`.
- Spécifiez l'option `login` sur `pppd` et omettez le mot de passe dans le fichier `pap-secrets` en plaçant des guillemets doubles (`""`) dans la colonne de mot de passe. Dans ce cas, l'authentification est effectuée par l'intermédiaire de la base de données passwd UNIX ou du mécanisme PAM.

Description de l'authentification PAP

L'authentification PAP se déroule dans l'ordre indiqué ci-dessous.

FIGURE 8-1 Processus d'authentification PAP



1. L'appelant (l'authentifié) appelle le pair distant (authentificateur) et fournit ses nom d'utilisateur et mot de passe PAP dans le cadre de la négociation de liaison.
2. Le pair vérifie l'identité de l'appelant dans son fichier `/etc/ppp/pap-secrets`. S'il utilise l'option `login` de PAP, le pair vérifie le nom d'utilisateur et le mot de passe de l'appelant dans sa base de données de mots de passe.
3. Si l'authentification réussit, le pair continue la négociation de liaison avec l'appelant. Si l'authentification échoue, la liaison est interrompue.
4. (Facultatif) Si l'appelant authentifie les réponses de pairs distants, ceux-ci doivent lui envoyer leurs informations d'identification PAP. Ainsi, le pair distant devient l'authentifié et l'appelant l'authentificateur.
5. (Facultatif) L'appelant d'origine lit son fichier `/etc/ppp/pap-secrets` pour vérifier l'identité du pair distant.

Remarque - Si l'appelant d'origine ne nécessite pas les informations d'identification du pair distant, l'étape 1 et l'étape 4 se déroulent en parallèle.

Si le pair est authentifié, la négociation se poursuit. Dans le cas contraire, la liaison est interrompue.

6. La négociation entre l'appelant et le pair se poursuit jusqu'à ce que la liaison soit finalement établie.

Utilisation de l'option `login` avec `/etc/ppp/pap-secrets`

Vous pouvez ajouter l'option `login` pour authentifier les informations d'identification PAP dans les fichiers de configuration PPP. Lorsque vous spécifiez l'option `login` dans `/etc/ppp/options` par exemple, `pppd` vérifie que les informations d'identification PAP de l'appelant existent dans la base de données de mots de passe. L'exemple suivant représente le format d'un fichier `/etc/ppp/pap-secrets` avec l'option `login`.

```
joe    *  ""  *
sally  *  ""  *
sue    *  ""  *
```

Signification des paramètres .

Appelant	`joe`, `sally` et `sue` sont les noms des appelants autorisés.
Serveur	L'astérisque (*) indique que tous les noms de serveur sont valides. L'option `name` n'est pas obligatoire dans les fichiers de configuration PPP.
Mot de passe	Les guillemets doubles indiquent les mots de passe valides. Si un mot de passe figure dans cette colonne, le mot de passe du pair doit correspondre à la fois au mot de passe PAP et au mot de passe dans la base de données `passwd` UNIX.
Adresses IP	L'astérisque (*) indique que toutes les adresses IP sont valides.

Protocole CHAP (Challenge-Handshake Authentication Protocol)

L'authentification CHAP utilise la notion de *défi* et de *réponse*, ce qui signifie que le pair (l'authentificateur) défie l'appelant (l'authentifié) de prouver son identité. Le défi comprend un

nombre aléatoire et un ID unique généré par l'authentificateur. L'appelant doit utiliser l'ID, le nombre aléatoire et ses informations d'identification de sécurité CHAP pour générer la réponse adéquate (protocole de transfert) à envoyer au pair.

Les informations d'identification et de connexion de sécurité CHAP CHAP nom d'utilisateur et inclure CHAP un "secret" CHAP. Le secret CHAP est une chaîne arbitraire, connue à la fois de l'appelant et le PPP pair avant qu'ils ne négocient une liaison. Vous pouvez configurer les informations d'identification de sécurité CHAP dans la base de données CHAP, `/etc/ppp/chap-secrets`.

Fichier `/etc/ppp/chap-secrets`

La base de données CHAP est mise en oeuvre dans le fichier `/etc/ppp/chap-secrets`. Les machines de chaque côté de la liaison PPP doivent disposer de leurs informations d'identification CHAP mutuelles dans leurs fichiers `/etc/ppp/chap-secrets` pour que l'authentification réussisse.

Remarque - Contrairement à PAP, le secret partagé doit être en clair sur les deux pairs. Vous ne pouvez pas utiliser crypt, PAM ni l'option login PPP avec le protocole CHAP.

La syntaxe du fichier `/etc/ppp/chap-secrets` est la suivante.

```
myclient myserver secret5748 *
```

Signification des paramètres :

`myclient` Nom d'utilisateur CHAP de l'appelant. Ce nom peut être identique au nom d'utilisateur UNIX de l'appelant, ou bien différent.

`myserver` Nom de la machine distante, souvent un serveur d'appel entrant.

`secret5748` Secret CHAP de l'appelant.

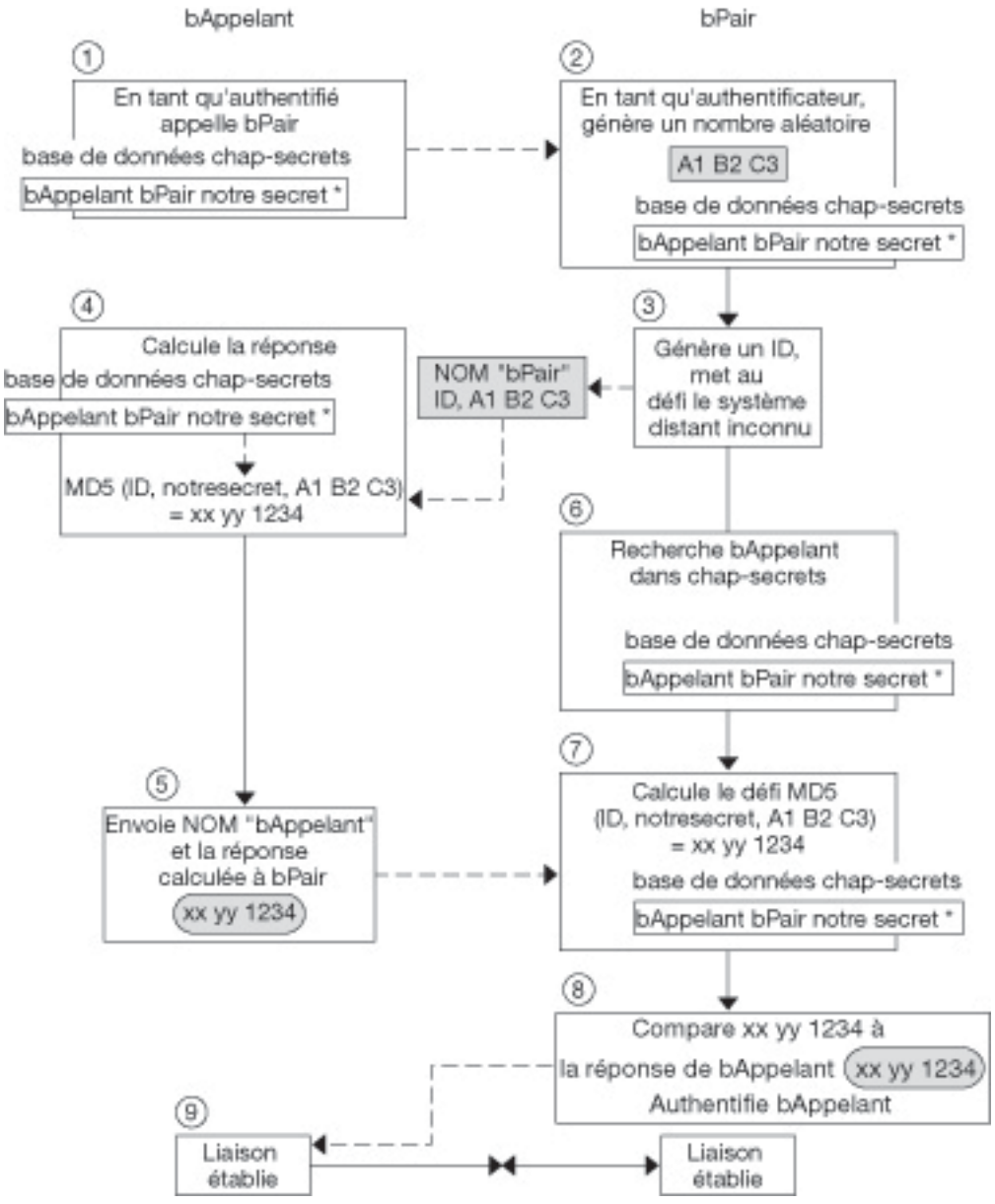
Remarque - Contrairement aux mots de passe PAP, les secrets CHAP ne sont jamais envoyés via la liaison. Ils sont plutôt utilisés lorsque les machines locales calculent la réponse.

`*` Adresse IP associée à l'appelant. L'astérisque (*) représente n'importe quelle adresse IP.

Description de l'authentification CHAP

L'authentification CHAP se déroule dans l'ordre indiqué ci-après.

FIGURE 8-2 Ordre de l'authentification CHAP



1. Deux pairs sur le point d'initialiser la communication conviennent d'un secret à utiliser pour l'authentification lors de la négociation d'une liaison PPP.

2. Les administrateurs des deux machines ajoutent le secret, les noms d'utilisateur CHAP et d'autres informations d'identification CHAP dans la base de données `/etc/ppp/chap-secrets` de leur machine respective.
3. L'appelant (l'authentifié) appelle le pair distant (l'authentificateur).
4. L'authentificateur génère un numéro aléatoire et un ID, et envoie ces données à l'authentifié sous forme de défi.
5. L'authentifié recherche le nom et le secret du pair dans sa base de données `/etc/ppp/chap-secrets`.
6. L'authentifié calcule une réponse en appliquant l'algorithme de calcul MD5 au secret et au défi de numéro aléatoire du pair. Ensuite, l'authentifié envoie pour réponse les résultats à l'authentificateur.
7. L'authentificateur recherche le nom et le secret de l'authentifié dans sa base de données `/etc/ppp/chap-secrets`,
8. L'authentificateur calcule son propre chiffre en appliquant MD5 au numéro généré en tant que défi et secret pour l'authentifié dans la base de données `/etc/ppp/chap-secrets`.
9. L'authentificateur compare les résultats avec la réponse de l'appelant. Si les deux valeurs sont identiques, le pair a authentifié l'appelant et la négociation de liaison se poursuit. Dans le cas contraire, la liaison est interrompue.

Création d'un schéma d'adressage IP pour appelants

Envisagez de créer une ou plusieurs adresses IP pour tous les appels entrants au lieu d'affecter une adresse IP unique à chaque utilisateur distant. Les adresses IP dédiées sont particulièrement importantes si le nombre d'appelants dépasse le nombre de ports série et de modems sur le serveur d'appel entrant. Vous pouvez mettre en place des scénarios différents, en fonction des besoins de votre site. En outre, les scénarios ne s'excluent pas mutuellement.

Affectation des adresses IP dynamiques aux appelants

L'adressage dynamique implique l'affectation de l'adresse IP définie dans le fichier `/etc/ppp/options.`*ttyname*. L'adressage dynamique s'effectue sur chaque port série. A l'arrivée d'un appel sur une ligne série, l'appelant reçoit l'adresse IP dans le fichier `/etc/ppp/options.`*ttyname* de l'interface série de l'appel.

Par exemple, supposons qu'un serveur d'appel entrant dispose de quatre interfaces série fournissant un service d'accès commuté aux appels entrants :

- Pour le port série `term/a`, créez le fichier `/etc/ppp/options.term.a` avec l'entrée suivante :

```
:10.1.1.1
```

- Pour le port série `term/b`, créez le fichier `/etc/ppp/options.term.b` avec l'entrée suivante :

```
:10.1.1.2
```

- Pour le port série `term/c`, créez le fichier `/etc/ppp/options.term.c` avec l'entrée suivante :

```
:10.1.1.3
```

- Pour le port série `term/d`, créez le fichier `/etc/ppp/options.term.d` avec l'entrée suivante :

```
:10.1.1.4
```

Selon le schéma d'adressage précédent, un appel entrant sur l'interface série `/dev/term/c` reçoit l'adresse IP 10.1.1.3 pour la durée de l'appel. Une fois que le premier appelant raccroche, un appel ultérieur entrant par l'interface série `/dev/term/c` se voit également attribuer l'adresse IP 10.1.1.3.

Les avantages de l'adressage dynamique sont les suivants :

- Vous pouvez suivre l'utilisation du réseau PPP jusqu'au niveau du port série.
- Vous pouvez affecter un nombre minimal d'adresses IP à l'utilisation de PPP.
- Vous pouvez simplifier la gestion du filtrage IP.

Affectation des adresses IP statiques aux appelants

Si votre site met en oeuvre l'authentification PPP, vous pouvez assigner des adresses IP spécifiques, *static*, à des appelants donnés. Dans ce cas, chaque fois qu'une machine d'appel sortant appelle le serveur d'appel entrant, l'appelant reçoit la même adresse IP.

Vous mettez en oeuvre les adresses statiques dans la base de données de secrets pap-secrets ou chap-secrets. Voici un exemple de fichier `/etc/ppp/chap-secrets` définissant des adresses IP statiques.

```
joe    myserver  joepasswd   10.10.111.240
sally  myserver  sallypasswd 10.10.111.241
sue    myserver  suepasswd   10.10.111.242
```

Appelant	`joe`, `sally` et `sue` sont les noms des appelants autorisés.
Serveur	`myserver` indique le nom du serveur.
Mot de passe	`joepasswd`, `sallypasswd` et `suepasswd` indiquent les mots de passe de chaque appelant.

Adresses IP	`10.10.111.240`, `10.10.111.241` et `10.10.111.242` sont les adresses IP affectées à chaque appelant.

Voici un exemple de fichier `/etc/ppp/chap-secrets` définissant des adresses IP statiques.

```
account1 myserver secret5748  10.10.111.244
account2 myserver secret91011 10.10.111.245
```

Appelant	`account1` et `account2` indiquent les noms des appelants.
Serveur	`myserver` indique le nom du serveur pour chaque appelant.
Mot de passe	`secret5748` et `secret91011` indiquent le secret CHAP de chaque appelant.
Adresses IP	`10.10.111.244` et `10.10.111.245` sont les adresses IP de chaque appelant.

Affectation d'adresses IP par numéro d'unité sppp

Si vous utilisez l'authentification PAP ou CHAP, vous pouvez affecter des adresses IP aux appelants par le numéro d'unité `sppp`. L'exemple suivant illustre ce type d'utilisation.

```
myclient ISP-server mypassword 10.10.111.240/28+
```

Le signe plus (+) indique que le numéro d'unité est ajouté à l'adresse IP. Remarques :

- Les adresses comprises entre `10.10.111.240` et `10.10.111.255` sont affectées à des utilisateurs distants.
- `sppp0` obtient l'adresse IP `10.10.111.240`.
- `sppp1` obtient l'adresse IP `10.10.111.241` et ainsi de suite.

Création de tunnels PPPoE pour la prise en charge DSL

L'utilisation de PPPoE permet de fournir des services numériques haut débit PPP à plusieurs clients équipés d'un ou de plusieurs modems. Pour mettre en oeuvre ces services, PPPoE crée un tunnel Ethernet par le biais de trois participants : l'entreprise, l'opérateur téléphonique et le fournisseur d'accès.

- Pour une présentation générale de PPPoE et une description de son fonctionnement, reportez-vous à la section “Présentation PPPoE” à la page 26.
- Pour une description des tâches de configuration des tunnels PPPoE, reportez-vous au Chapitre 6, Configuration d'un tunnel PPP Over Ethernet.

Cette section contient des informations détaillées relatives aux commandes et fichiers PPPoE, qui sont résumées dans le tableau suivant.

TABLEAU 8-2 Commandes et fichiers de configuration PPPoE

Fichier ou commande	Description	Pour obtenir des instructions
`/etc/ppp/pppoe`	Fichier qui contient les caractéristiques appliquées par défaut à tous les tunnels configurés par PPPoE sur le système	"Fichier `/etc/ppp/pppoe`" à la page 144
`/etc/ppp/pppoe.`*device*	Fichier qui contient les caractéristiques d'une interface spécifique utilisée par PPPoE pour un tunnel	"`/etc/ppp/pppoe.`*device*" à la page 146
`/etc/ppp/pppoe.if`	Fichier qui indique l'interface Ethernet sur laquelle s'exécute le tunnel configuré par PPPoE	"Fichier `/etc/ppp/pppoe.if`" à la page 142
`/usr/sbin/sppptun`	Commande de configuration des interfaces Ethernet impliquées dans un tunnel PPPoE	"Commande `/usr/sbin/sppptun`" à la page 143
`/usr/lib/inet/pppoed`	Commande et options d'utilisation de PPPoE pour configurer un tunnel	"Démon `/usr/lib/inet/pppoed`" à la page 144

Fichiers de configuration d'interfaces PPPoE

Les interfaces utilisées à chaque extrémité du tunnel PPPoE doivent être configurées avant que le tunnel puisse prendre en charge les communications PPP. Utilisez les fichiers `/usr/sbin/sppptun` et `/etc/ppp/pppoe.if` à cette fin. Vous devez utiliser ces outils pour configurer les interfaces Ethernet sur tous les clients PPPoE Oracle Solaris et serveurs d'accès PPPoE.

Fichier `/etc/ppp/pppoe.if`

Le fichier `/etc/ppp/pppoe.if` répertorie les noms de toutes les interfaces Ethernet sur un hôte à utiliser pour les tunnels PPPoE. Ce fichier est traité lors de l'initialisation du système, au moment du montage des interfaces répertoriées pour une utilisation dans des tunnels PPPoE.

Vous devez créer explicitement `/etc/ppp/pppoe.if`. Tapez le nom d'une interface à configurer pour PPPoE sur chaque ligne.

L'exemple ci-dessous illustre un fichier `/etc/ppp/pppoe.if` pour un serveur offrant trois interfaces pour des tunnels PPPoE.

```
# cat /etc/ppp/pppoe.if
hme1
hme2
hme3
```

Généralement, les clients PPPoE ont une seule interface répertoriée dans le fichier `/etc/ppp/pppoe.if` .

Commande `/usr/sbin/sppptun`

Vous pouvez utiliser la commande `/usr/sbin/sppptun` pour monter et démonter manuellement les interfaces Ethernet à utiliser pour les tunnels PPPoE. Par contraste, `/etc/ppp/pppoe.if` n'est lu qu'au démarrage du système. Ces interfaces doivent correspondre à celles qui sont répertoriées dans `/etc/ppp/pppoe.if`.

`sppptun` monte les interfaces Ethernet utilisées dans les tunnels PPPoE de manière similaire à la commande `ipadm`. Contrairement à `ipadm`, vous devez monter les interfaces deux fois pour prendre en charge PPPoE, car deux numéros de protocole Ethernet sont impliqués.

La syntaxe de base de `sppptun` est la suivante :

```
# /usr/sbin/sppptun plumb pppoed device-name
      device-name:pppoed
# /usr/sbin/sppptun plumb pppoe device-name
      device-name:pppoe
```

Dans cette syntaxe, *device-name* correspond au nom du périphérique à monter pour PPPoE.

La première fois que vous exécutez la commande `sppptun`, le protocole de découverte `pppoed` est monté sur l'interface. A la seconde exécution de `sppptun`, le protocole de session `pppoe` est monté. `sppptun` imprime le nom de l'interface qui vient d'être montée. Vous utilisez ce nom pour démonter l'interface, le cas échéant.

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

Exemples de commandes `sppptun` pour l'administration des interfaces

L'exemple suivant montre comment monter manuellement une interface pour PPPoE à l'aide de la commande `/usr/sbin/sppptun`.

```
# /usr/sbin/sppptun plumb pppoed hme0
hme0:pppoed
# /dev/sppptun plumb pppoe hme0
 hme0:pppoe
```

Cet exemple illustre comment répertorier les interfaces sur un serveur d'accès monté pour PPPoE.

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
hme1:pppoe
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

Cet exemple montre comment démonter une interface.

```
# sppptun unplumb hme0:pppoed
# sppptun unplumb hme0:pppoe
```

Fichiers et commandes du serveur d'accès PPPoE

Un prestataire de services qui offre des services ou une assistance DSL peut utiliser un serveur d'accès équipé de PPPoE. La relation entre le serveur et le client d'accès PPPoE est une relation client-serveur classique. Elle s'apparente à celle que la machine d'appel sortant et le serveur d'appel entrant entretiennent sur une liaison commutée. Un système PPPoE initialise la communication et un système PPPoE répond. Par contraste, le protocole PPP n'a aucune notion de la relation client-serveur. PPP place les deux systèmes sur un plan d'égalité.

Les commandes et fichiers qui permettent de configurer un serveur d'accès PPPoE sont les suivants :

- "Commande `/usr/sbin/sppptun`" à la page 143
- "Démon `/usr/lib/inet/pppoed`" à la page 144
- "Fichier `/etc/ppp/pppoe`" à la page 144
- "`/etc/ppp/pppoe.`*device*" à la page 146
- "Objet partagé `pppoe.so`" à la page 150

Démon `/usr/lib/inet/pppoed`

Le démon `pppoed` accepte des diffusions de services de clients PPPoE potentiels. En outre, `pppoed` négocie le côté serveur du tunnel PPPoE tunnel et exécute `pppd`, le démon PPP, sur ce tunnel.

Vous configurez les services `pppoed` dans les fichiers `/etc/ppp/pppoe` et `/etc/ppp/pppoe.`*device*. Si `/etc/ppp/pppoe` existe au démarrage du système, `pppoed` s'exécute automatiquement. Vous pouvez également exécuter explicitement le démon `pppoed` en tapant `/usr/lib/inet/pppoed` sur la ligne de commande.

Fichier `/etc/ppp/pppoe`

Le fichier `/etc/ppp/pppoe` décrit les services offerts par un serveur d'accès et les options définissant l'exécution de PPP sur le tunnel PPPoE. Vous pouvez définir des services pour chacune des interfaces ou de manière globale, c'est-à-dire pour toutes les interfaces du serveur d'accès. Le serveur d'accès envoie les informations dans le fichier `/etc/ppp/pppoe` en réponse à une diffusion d'un client potentiel PPPoE.

Voici la syntaxs de base de `/etc/ppp/pppoe` :

global-options
service service-name
    service-specific-options
    device interface-name

Signification des paramètres .

global-options — Définit les options par défaut du fichier `/etc/ppp/pppoe`. Il s'agit d'options disponibles via `pppoed` ou `pppd`. Pour obtenir la liste complète de ces options, reportez-vous aux pages de manuel `pppoed`(1M) et `pppd`(1M).

Par exemple, vous devez répertorier les interfaces Ethernet disponibles pour le tunnel PPPoE en tant qu'*options globales*. Si vous ne définissez pas de périphériques dans le fichier `/etc/ppp/pppoe`, les services ne sont proposés sur aucune interface.

Pour définir `devices` en tant qu'option globale, utilisez le format suivant :

device interface <,interface>

interface spécifie l'interface où le service est à l'écoute des clients PPPoE potentiels. Si plusieurs interfaces sont associées au service, séparez leur nom par une virgule.

service service-name — Démarre la définition du service *service-name*. *service-name* est une chaîne qui peut être une expression appropriée aux services fournis.

service-specific-options — Répertorie les options PPP et PPPoE spécifiques à ce service.

`device` *interface-name* — Spécifie l'interface où le service énoncé précédemment est disponible.

Pour obtenir d'autres options de `/etc/ppp/pppoe`, reportez-vous aux pages de manuel `pppoed`(1M) et `pppd`(1M).

Un fichier `/etc/ppp/pppoe` typique peut se présenter comme suit.

EXEMPLE 8-2 Fichier `/etc/ppp/pppoe` de base

```
device hme1,hme2,hme3
service internet
   pppd "name internet-server"
service intranet
   pppd "192.168.1.1:"
```

```
service debug
   device hme1
   pppd "debug name internet-server"
```

Dans ce fichier, les valeurs suivantes s'appliquent.

`hme1,hme2,hme3`	Trois interfaces sur le serveur d'accès à utiliser pour les tunnels PPPoE.
`service internet`	Signale un service appelé `internet` aux clients potentiels. Le fournisseur qui propose le service détermine également comment `internet` est défini. Par exemple, un fournisseur peut interpréter `internet` au sens de services IP variés, ainsi qu'accès à Internet.
`pppd`	Définit les options de ligne de commande utilisées lorsque l'appelant appelle `pppd`. L'option `"name internet-server"` donne le nom `internet-server` à la machine locale, serveur d'accès.
`service intranet`	Signale un autre service appelé `intranet` aux clients potentiels.
`pppd "192.168.1.1:"`	Définit les options de ligne de commande utilisées lorsque l'appelant appelle `pppd`. Lorsque l'appelant appelle `pppd`, 192.168.1.1 est défini comme l'adresse IP de la machine locale, serveur d'accès.
`service debug`	Signale un troisième service (débogage) sur les interfaces définies pour PPPoE.
`device hme1`	Restreint le débogage des tunnels PPPoE à `hme1`.
`pppd "debug name internet-server"`	Définit les options de ligne de commande utilisées lorsque l'appelant appelle `pppd`, dans ce cas, PPP déboguant la machine locale `internet-server` .

`/etc/ppp/pppoe.`*device*

Le fichier `/etc/ppp/pppoe.`*device* décrit les services qui sont offerts sur une interface d'un serveur d'accès aux PPPoE. `/etc/ppp/pppoe.`*device* comporte également des options qui définissent l'exécution de PPP sur le tunnel PPPoE. `/etc/ppp/pppoe.`*device* est un fichier facultatif, qui fonctionne exactement comme le fichier `/etc/ppp/pppoe` global. Cependant, lorsque `/etc/ppp/pppoe.`*device* est défini pour une interface, ses paramètres sont prioritaires pour cette interface par rapport aux paramètres globaux définis dans `/etc/ppp/pppoe`.

La syntaxe de base de `/etc/ppp/pppoe.`*device* est la suivante :

`service` *service-name*
    service-specific-options

service *another-service-name*
service-specific-options

La seule différence avec la syntaxe de `/etc/ppp/pppoe` est l'impossibilité d'utiliser l'option `device` illustrée dans “Fichier `/etc/ppp/pppoe`” à la page 144.

Plugin `pppoe.so`

`pppoe.so` est le fichier d'objet partagé PPPoE qui doit être appelé par les clients et serveurs d'accès PPPoE. Ce fichier limite MTU et MRU à 1492, filtre les paquets à partir du pilote et négocie le tunnel PPPoE, avec `pppoed`. Côté serveur d'accès, `pppoe.so` est automatiquement appelé par le démon `pppd`.

Configuration du serveur d'accès à l'aide des fichiers PPPoE et PPP

Cette section contient des exemples de tous les fichiers permettant de configurer un serveur d'accès. Le serveur d'accès est multiréseau. Le serveur est connecté à trois sous-réseaux : `green`, `orange` et `purple`. Par défaut, `pppoed` s'exécute en tant que `root` sur le serveur.

Les clients PPPoE peuvent accéder aux réseaux `orange` et `purple` par le biais des interfaces `hme0` et `hme1`. Les clients se connectent au serveur à l'aide de la connexion UNIX standard. Le serveur authentifie les clients à l'aide de PAP.

Le réseau `green` n'est pas signalé aux clients. Le seul moyen pour les clients d'accéder au réseau `green` est de spécifier directement "`green-net`" et de fournir les informations d'identification CHAP. En outre, seuls les clients `joe` et `mary` sont autorisés à accéder au réseau `green` à l'aide d'adresses IP statiques.

EXEMPLE 8-3 Fichier `/etc/ppp/pppoe` pour un serveur d'accès

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
service purple-net
     device hme0,hme1
     pppd "require-pap login name purple-server purple-server:"
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

Cet exemple décrit les services disponibles à partir du serveur d'accès. La première section décrit les services du réseau `orange`.

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
```

Les clients accèdent au réseau `orange` via les interfaces `hme0` et `hme1`. Les options données à la commande `pppd` force le serveur à demander aux clients potentiels leurs informations d'identification PAP. Les options `pppd` définissent également le nom du serveur sur `orange-server`, tel qu'il est utilisé dans le fichier `pap-secrets`.

La section des services du réseau `purple` est identique à celle du réseau `orange`, à l'exception des noms du réseau et du serveur.

La section suivante décrit les services du réseau `green` :

```
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

Cette section restreint l'accès client à l'interface `hme1`. Les options données à la commande `pppd` forcent le serveur à demander aux clients potentiels leurs informations d'identification CHAP. Les options `pppd` définissent également le nom du serveur sur `green-server`, à utiliser dans le fichier `chap-secrets`. L'option `nowildcard` spécifie que l'existence du réseau green n'est pas signalée aux clients.

Pour le scénario décrit ci-dessus, vous pouvez configurer le fichier `/etc/ppp/options`.

EXEMPLE 8-4 Fichier `/etc/ppp/options` pour un serveur d'accès

```
auth
proxyarp
nodefaultroute
name no-service # don't authenticate otherwise
```

L'option `name no-service` remplace le nom du serveur qui est normalement recherché au cours de l'authentification PAP ou CHAP. Le nom par défaut du serveur est celui trouvé par la commande `/usr/bin/hostname`. L'option `name` dans l'exemple précédent remplace le nom du serveur par `no-service`. Il est peu probable que le nom `no-service` soit trouvé dans un fichier `pap` ou `chap-secrets`. Cette action empêche un utilisateur aléatoire d'exécuter `pppd` et de remplacer les options `auth` et `name` définies dans le fichier `/etc/ppp/options`. `pppd` échoue, car aucun secret ne peut être trouvé pour le client avec le nom de serveur `no-service`.

Le scénario de serveur d'accès utilise le fichier `/etc/hosts` suivant.

EXEMPLE 8-5 Fichier `/etc/hosts` pour un serveur d'accès

```
     172.16.0.1 orange-server
     172.17.0.1 purple-server
```

```
172.18.0.1 green-server
172.18.0.2 joes-pc
172.18.0.3 marys-pc
```

Voici le fichier `/etc/ppp/pap-secrets`, utilisé pour l'authentification PAP des clients qui tentent d'accéder aux réseaux `orange` et `purple`.

EXEMPLE 8-6 Fichier `/etc/ppp/pap-secrets` pour un serveur d'accès

```
* orange-server "" 172.16.0.2/16+
* purple-server "" 172.17.0.2/16+
```

Voici le fichier `/etc/ppp/chap-secrets`, utilisé pour l'authentification CHAP. Notez que seuls les clients `joe` et `mary` figurent dans la liste du fichier.

EXEMPLE 8-7 Fichier `/etc/ppp/chap-secrets` pour un serveur d'accès

```
 joe green-server "joe's secret" joes-pc
mary green-server "mary's secret" marys-pc
```

Commandes et fichiers du client PPPoE

Pour exécuter PPP sur un modem DSL, une machine doit devenir client PPPoE. Vous devez monter une interface pour exécuter PPPoE, puis détecter l'existence d'un serveur d'accès à l'aide de l'utilitaire `pppoec`. Le client peut alors créer le tunnel PPPoE via le modem DSL et exécuter PPP.

Le client PPPoE communique avec le serveur d'accès sur le modèle client-serveur classique. Le tunnel PPPoE n'est pas une liaison commutée, mais il est configuré et fonctionne de façon similaire.

Les commandes et fichiers qui configurent un client PPPoE sont les suivants :

- “Commande `/usr/sbin/sppptun`” à la page 143
- “Utilitaire `/usr/lib/inet/pppoec`” à la page 149
- “Objet partagé `pppoe.so`” à la page 150
- “Fichier `/etc/ppp/peers/`*peer-name*” à la page 120
- “Fichier de configuration `/etc/ppp/options`” à la page 115

Utilitaire `/usr/lib/inet/pppoec`

L'utilitaire `/usr/lib/inet/pppoec` est responsable de la négociation du côté client d'un tunnel PPPoE. `pppoec` est similaire à l'utilitaire `chat`. Vous n'appelez pas `pppoec` directement.

Vous démarrez plutôt `/usr/lib/inet/pppoec` comme argument de l'option `connect` de la commande `pppd`.

Objet partagé `pppoe.so`

`pppoe.so` est l'objet partagé PPPoE que PPPoE doit charger pour fournir aux clients et serveurs d'accès la capacité PPPoE. L'objet partagé `pppoe.so` limite MTU et MRU à 1492, filtre les paquets en provenance du pilote et gère les messages PPPoE d'exécution.

Côté client, `pppd` charge `pppoe.so` lorsque l'utilisateur spécifie l'option `plugin pppoe.so`.

Fichier `/etc/ppp/peers/`*peer-name* de définition d'un pair de serveur d'accès

Lorsque vous définissez un serveur d'accès pour qu'il soit détecté par `pppoec`, utilisez les options qui s'appliquent à la fois à `pppoec` et au démon `pppd`. Le fichier `/etc/ppp/peers/`*peer-name* du serveur d'accès requiert les paramètres suivants :

- `sppptun` : nom du périphérique série utilisé par le tunnel PPPoE.
- `plugin pppoe.so` : indique à `pppd` de charger l'objet partagé `pppoe.so`.
- `connect "/usr/lib/inet/pppoec`*device*`"` : démarre une connexion. `connect` appelle ensuite l'utilitaire `pppoec` sur *device*, l'interface montée pour PPPoE.

Les paramètres restants dans le fichier `/etc/ppp/peers/`*peer-name* doivent s'appliquer à la liaison PPP sur le serveur. Utilisez les options que vous utiliseriez pour `/etc/ppp/peers/`*peer-name* sur une machine d'appel sortant. Essayez de limiter le nombre d'options à celles dont vous avez vraiment besoin pour la liaison PPP.

L'exemple suivant est présenté dans la section “Définition d'un pair de serveur d'accès PPPoE” à la page 85.

EXEMPLE 8-8 Fichier `/etc/ppp/peers/`*peer-name* de définition d'un serveur d'accès à distance

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

Ce fichier définit les paramètres à utiliser lors de la configuration d'un tunnel PPPoE et d'une liaison PPP pour accéder au serveur `dslserve`. Les options incluses sont les suivantes :

Option	Description
`sppptun`	Définit `sppptun` comme nom du périphérique série.
`plugin pppoe.so`	Demande à `pppd` de charger l'objet partagé `pppoe.so`.
`connect "/usr/lib/inet/pppoec hme0"`	Exécute `pppoec` et désigne `hme0` en tant qu'interface pour le tunnel PPPoE et la liaison PPP.
`noccp`	Désactive la compression CCP sur la liaison. **Remarque -** De nombreux FAI utilisent uniquement les algorithmes de compression propriétaires. La désactivation de l'algorithme CCP mis à la disposition du public permet de réduire la durée de la négociation et d'éviter des problèmes d'interopérabilité peu fréquents.
`noauth`	Empêche `pppd` d'exiger les informations d'identification du serveur d'accès. La plupart des FAI ne fournissent pas d'informations d'identification aux clients.
`user Red`	Définit `Red` en tant que nom d'utilisateur du client, qui est requis pour l'authentification PAP par le serveur d'accès.
`password redsecret`	Définit `redsecret` comme le mot de passe à fournir au serveur d'accès pour l'authentification PAP.
`noipdefault`	Affecte 0.0.0.0 en tant qu'adresse IP initiale.
`defaultroute`	Indique à `pppd` d'installer une route IPv4 par défaut après la négociation IPCP. Vous devez inclure `defaultroute` dans le fichier `/etc/ppp/peers/`*peer-name* lorsque la liaison est la liaison du système à Internet, ce qui est le cas pour un client PPPoE.

♦ ♦ ♦ CHAPITRE 9

Migration de Solaris PPP vers Solaris PPP 4.0 (tâches)

Les versions antérieures du système d'exploitation Oracle Solaris incluaient une implémentation PPP différente, asynchrone (`asppp`). Si vous souhaitez convertir des pairs qui exécutent `asppp` à la nouvelle implémentation PPP 4.0, vous devez exécuter un script de conversion. Ce chapitre aborde les points suivants de la conversion PPP :

Dans ce chapitre, un exemple de configuration `asppp` permet d'expliquer comment effectuer la conversion PPP. Vous trouverez une description des différences entre Solaris PPP 4.0 et `asppp` à la section "Quelle version de Solaris PPP utiliser" à la page 14.

Avant la conversion des fichiers `asppp`

Vous pouvez utiliser le script de conversion `/usr/sbin/asppp2pppd` pour convertir les fichiers qui composent une configuration `asppp` standard :

- `/etc/asppp.cf` : fichier de configuration PPP asynchrone
- `/etc/uucp/Systems` : fichier UUCP qui décrit les caractéristiques du pair distant
- `/etc/uucp/Devices` : fichier UUCP qui décrit le modem sur la machine locale
- `/etc/uucp/Dialers` fichier UUCP qui contient la séquence de connexion à utiliser par le modem décrit dans le fichier `/etc/uucp/Devices`

Pour plus d'informations sur `asppp`, reportez-vous au document *Solaris 8 System Administration collection, Volume 3*, disponible sur le site Web http://docs.oracle.com/cd/E19455-01/index.html.

Exemple du fichier de configuration /etc/asppp.cf

La procédure illustrée à la section “Conversion de asppp à Solaris PPP 4.0” à la page 157 utilise le fichier /etc/asppp.cf suivant.

```
#
ipadm create-if ipdptp0
ipadm create-addr -T static -a local=mojave,remote=gobi ipdptp0/ppaddr

path
 inactivity_timeout 120     # Approx. 2 minutes
 interface ipdptp0
 peer_system_name Pgobi    # The name we log in with (also in
                          # /etc/uucp/Systems
```

Le fichier contient les paramètres suivants.

ifpadm create-if ipdptp0	Exécute la commande ipadm pour créer une interface appelée ipdptp0
ipadm create-addr -T static -a local=mojave,remote=gobi ipdptp0/ppadd	Exécute la commande ipadm pour configurer un lien de l'interface PPP ipdptp0 sur la machine locale mojave vers le pair distant gobi
inactivity_timeout 120	Met fin à la ligne après deux minutes d'inactivité
interface ipdptp0	Configure l'interface ipdptp0 sur la machine d'appel sortant pour une liaison PPP asynchrone
peer_system_name Pgobi	Attribue le nom du pair distant, Pgobi

Exemple du fichier /etc/uucp/Systems

La procédure illustrée à la section “Conversion de asppp à Solaris PPP 4.0” à la page 157 utilise le fichier /etc/uucp/Systems suivant.

```
#ident  "@(#)Systems 1.5  92/07/14 SMI"  /* from SVR4 bnu:Systems 2.4 */
#

# .
# .
Pgobi Any ACU 38400 15551212 in:--in: mojave word: sand
```

Le fichier contient les paramètres suivants :

`Pgobi`	Utilise `Pgobi` comme nom d'hôte du pair distant
`Any ACU`	Indique au modem sur la machine d'appel sortant `mojave` d'établir une liaison avec un modem sur `Pgobi` à tout moment de la journée. ACU signifie "rechercher ACU dans le fichier `/etc/uucp/Devices`".
`38400`	Définit la vitesse maximale de la liaison sur 38400.
`15551212`	Indique le numéro de téléphone de `Pgobi`.
`in:–in: mojave word: sand`	Définit le script de connexion requis par `Pgobi` pour authentifier la machine d'appel sortant `mojave`.

Exemple du fichier `/etc/uucp/Devices`

La procédure illustrée à la section “Conversion de asppp à Solaris PPP 4.0” à la page 157 utilise le fichier `/etc/uucp/Devices` suivant.

```
#ident  "@(#)Devices  1.6  92/07/14 SMI"  /* from SVR4 bnu:Devices 2.7 */

.
.
#

TCP,et - - Any TCP -
.
.
#
ACU cua/b - Any hayes
# 0-7 are on a Magma 8 port card
Direct cua/0 - Any direct
Direct cua/1 - Any direct
Direct cua/2 - Any direct
Direct cua/3 - Any direct
Direct cua/4 - Any direct
Direct cua/5 - Any direct
Direct cua/6 - Any direct
Direct cua/7 - Any direct
# a is the console port (aka "tip" line)
Direct cua/a - Any direct
# b is the aux port on the motherboard
Direct cua/b - Any direct
# c and d are high speed sync/async ports
Direct cua/c - Any direct
Direct cua/d - Any direct
```

Le fichier prend en charge tous les modems Hayes connectés au port série `cua/b`.

Exemple du fichier /etc/uucp/Dialers

La procédure illustrée à la section “Conversion de asppp à Solaris PPP 4.0” à la page 157 utilise le fichier /etc/uucp/Dialers suivant.

```
#
#       <Much information about modems supported by Oracle Solaris UUCP>


penril =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
ventel =&-% "" \r\p\r\c $ k\c ONLINE!
vadic =K-K "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE
develcon "" "" \pr\ps\c est:\007 \E\D\e \n\007
micom "" "" \s\c NAME? \D\r\c GO
direct
#
#
#
#   Hayes Smartmodem -- modem should be set with the configuration
#   switches as follows:
#
#       S1 - UP  S2 - UP  S3 - DOWN S4 - UP
#       S5 - UP  S6 - DOWN S7 - ?  S8 - DOWN
#
hayes =,-, "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT

      <much more information about modems supported by Oraccle Solaris UUCP>
```

Ce fichier contient les scripts de discussion pour tous les types de modems, y compris les modems Hayes qui sont pris en charge dans le fichier /etc/uucp/Dialers.

Exécution du script de conversion asppp2pppd (tâches)

Le script /usr/sbin/asppp2pppd copie les informations PPP contenues dans les fichiers /etc/asppp.cf et UUCP PPP aux emplacements appropriés dans les fichiers Solaris PPP 4.0.

Tâches préliminaires

Avant de réaliser la tâche suivante, vous devez effectuer les opérations suivantes :

- Installation de Oracle Solaris sur la machine où résident également les fichiers de configuration asppp et UUCP
- Connexion en tant que superutilisateur sur la machine où résident les fichiers PPP, par exemple, mojave

Conversion de asppp à Solaris PPP 4.0

1. **Lancez le script de conversion.**

   ```
   # /usr/sbin/asppp2pppd
   ```

   Le processus de conversion démarre et la sortie suivante s'affiche à l'écran.

   ```
   This script provides only a suggested translation for your existing aspppd
   configuration.  You will need to evaluate for yourself whether the translation
   is appropriate for your operating environment.
   Continue [Yn]?
   ```

2. **Tapez "Y" pour continuer.**

   La sortie suivante s'affiche :

   ```
   Chat cannot do echo checking; requests for this removed.
   Adding 'noauth' to /etc/ppp/options

   Preparing to write out translated configuration:
       1 chat file:
           1.  /etc/ppp/chat.Pgobi.hayes
       2 option files:
           2.  /etc/ppp/peers/Pgobi
           3.  /etc/ppp/options
       1 script file:
           4.  /etc/ppp/demand
   ```

   Les nouveaux fichiers Solaris PPP 4.0 ont été générés.

Affichage des résultats de la conversion

Vous pouvez afficher les fichiers Solaris PPP 4.0 créés par le script de conversion `/usr/sbin/asppp2pppd` à la fin du processus de conversion. Le script affiche la liste d'options suivante.

```
Enter option number:
        1 - view contents of file on standard output
        2 - view contents of file using /usr/bin/less
        3 - edit contents of file using /usr/bin/vi
        4 - delete/undelete file from list
        5 - rename file in list
        6 - show file list again
        7 - escape to shell (or "!")
        8 - abort without saving anything
        9 - save all files and exit (default)
Option:
```

1. **Entrez `1` pour afficher le contenu des fichiers à l'écran.**

Le script vous demande le numéro du fichier que vous souhaitez visualiser.

```
File number (1 .. 4):
```

Les numéros renvoient aux fichiers convertis qui sont répertoriés pendant le processus de conversion, comme indiqué à l'étape 2 précédente.

2. **Entrez `1` pour visualiser le fichier de discussion `/etc/ppp/chat.Pgobi.hayes`.**

```
File number (1 .. 4):  1
"" \d\dA\p\pTE1V1X1Q0S2=255S12=255\r\c
OK\r ATDT\T\r\c
CONNECT \c
in:--in: mojave
word: sand
```

Le script de discussion contient les informations de discussion du modem qui s'affichent sur la ligne hayes dans le fichier d'exemple `/etc/uucp/Dialers`. `/etc/ppp/chat.Pgobi.hayes` contient également la séquence de connexion pour `Pgobi` qui s'affiche dans le fichier d'exemple `/etc/uucp/Systems`. Le script de discussion se trouve à présent dans le fichier `/etc/ppp/chat.Pgobi.hayes`.

3. **Entrez `2` pour visualiser le fichier de pairs `/etc/ppp/peers/Pgobi`.**

```
File number (1 .. 4):  2
/dev/cua/b
38400
demand
idle 120
connect "/usr/bin/chat -f /etc/ppp/chat.Pgobi.hayes -T '15551212'"
user NeverAuthenticate
mojave:gobi
```

Les informations sur le port série (`/dev/cua/b`) proviennent du fichier `/etc/uucp/Devices`. La vitesse de la liaison, le temps d'inactivité, les informations d'authentification et les noms des pairs proviennent du fichier `/etc/asppp.cf`. "demand" fait référence au script de demande, à appeler lorsque la machine d'appel sortant tente de se connecter au pair `Pgobi`.

4. **Entrez `3` pour visualiser le fichier `/etc/ppp/options` créé pour la machine d'appel sortant `mojave`.**

```
File number (1 .. 4):  3
#lock
noauth
```

Les informations dans `/etc/ppp/options` proviennent du fichier `/etc/asppp.cf` .

5. **Entrez `4` pour visualiser le contenu du script `demand`.**

```
File number (1 .. 4):  4
/usr/bin/pppd file /etc/ppp/peers/Pgobi
```

Ce script, lorsqu'il est appelé, exécute la commande `pppd`, qui lit ensuite le fichier `/etc/ppp/peers/Pgobi` pour initialiser la liaison entre `mojave` et `Pgobi`.

6. **Entrez `9` pour enregistrer les fichiers créés. Quittez ensuite le script de conversion.**

♦ ♦ ♦ CHAPITRE 10

A propos d'UNIX-to-UNIX Copy Program

Ce chapitre présente le programme UUCP (UNIX-to-UNIX Copy Program) et ses démons. Il aborde les sujets suivants :

UUCP permet aux ordinateurs de transférer des fichiers et d'échanger des messages électroniques entre eux. Le programme permet également aux ordinateurs d'être intégrés dans de grands réseaux tels que Usenet.

Le système d'exploitation Oracle Solaris fournit la version BNU (Basic Network Utilities) d'UUCP, également appelée HoneyDanBer UUCP. Le terme *UUCP* indique la plage complète de fichiers et d'utilitaires qui composent le système, dont le programme `uucp` n'est qu'une partie. Les utilitaires UUCP vont des utilitaires utilisés pour copier des fichiers entre ordinateurs (`uucp` et `uuto`) aux utilitaires utilisés pour la connexion à distance et l'exécution de commandes (`cu` et `uux a`).

Configurations matérielles UUCP

UUCP prend en charge les configurations matérielles suivantes

Liens directs	Vous pouvez créer un lien direct vers un autre ordinateur en plaçant des câbles RS-232 entre les ports série des deux ordinateurs. Les liens directs sont utiles lorsque deux ordinateurs communiquent régulièrement et sont physiquement proches (dans un rayon de 15 mètres). Vous pouvez utiliser un modem courte distance pour augmenter quelque peu cette distance.
Lignes téléphoniques	En utilisant une unité d'appel automatique (ACU), telle qu'un modem haut débit, votre ordinateur peut communiquer avec d'autres ordinateurs via des lignes téléphoniques classiques. Le modem compose le numéro de téléphone demandé par UUCP. L'ordinateur de destination doit disposer d'un modem capable de répondre aux appels entrants.

Network (Réseau) — UUCP peut également communiquer sur un réseau qui exécute le protocole TCP/IP ou une autre famille de protocole. Une fois que votre ordinateur a été défini en tant qu'hôte sur un réseau, il peut contacter n'importe quel hôte connecté au réseau.

Ce chapitre suppose que votre matériel UUCP a déjà été assemblé et configuré. Si vous devez configurer un modem, reportez-vous aux manuels accompagnant le modem pour obtenir de l'aide.

Logiciel UUCP

Le logiciel UUCP est automatiquement inclus lorsque vous exécutez le programme d'installation Oracle Solaris et sélectionnez la distribution entière. Vous pouvez également ajouter le logiciel UUCP à l'aide de la commande `pkgadd`. Les programmes UUCP peuvent être divisés en trois catégories : démons, programmes d'administration et programmes utilisateur.

Démons UUCP

Le système UUCP possède quatre démons : `uucico`, `uuxqt`, `uusched` et `in.uucpd`. Ces démons gèrent les transferts de fichiers UUCP et l'exécution des commandes. Vous pouvez également les lancer manuellement à partir du shell, si nécessaire.

`uucico` — Permet de sélectionner le périphérique utilisé pour le lien, d'établir le lien vers l'ordinateur distant et d'exécuter la séquence de connexion et les vérifications d'autorisations requises. En outre, `uucico` transfère les fichiers de données, exécute les fichiers, résulte de journaux et notifie l'utilisateur par e-mail lorsque les transferts sont terminés. `uucico` agit comme shell de connexion pour les comptes de connexion UUCP. Lorsque le démon `uucico` local appelle une machine distante, il communique directement avec le démon `uucico` distant au cours de la session.

Quand tous les fichiers requis ont été créés, les programmes `uucp`, `uuto` et `uux` exécutent le démon `uucico` pour contacter l'ordinateur éloignée. `uusched` et`Uutry` exécutent `uucico`. Reportez-vous à la page de manuel `uucico`(1M) pour plus d'informations.

`uuxqt` — Exécute requêtes d'exécution distantes. Ce démon effectue des recherches dans le répertoire spool pour exécuter des fichiers (toujours nommés `X.`*file*) envoyés à partir d'un ordinateur distant. Quand un fichier `X.` *file* est trouvé, `uuxqt` l'ouvre pour obtenir la liste des fichiers de données

nécessaires à l'exécution. `uuxqt` vérifie ensuite si les fichiers de données requis sont disponibles et accessibles. Si les fichiers sont disponibles, `uuxqt` vérifie le fichier `Permissions` afin de vérifier qu'il possède l'autorisation d'exécuter la commande demandée. Le démon `uuxqt` est exécuté par le script de shell `uudemon.hour`, qui est démarré par `cron`. Reportez-vous à la page de manuel `uuxqt`(1M) pour plus d'informations.

`uusched` — Permet de planifier les travaux en attente dans le répertoire spool. `uusched` est initialement exécuté au démarrage par le script de shell `uudemon.hour`, qui est démarré par `cron`. Pour plus d'informations, reportez-vous à la page de manuel `uusched`(1M). Avant de démarrer le démon `uucico`, `uusched` rend aléatoire l'ordre dans lequel les ordinateurs distants sont appelés.

`in.uucpd` — Prend en charge les connexions UUCP via réseau. Le fichier `inetd` sur l'hôte distant appelle `in.uucpd` chaque fois qu'une connexion UUCP est établie. `uucpd` vous invite alors à saisir un nom de connexion. `uucico` sur l'hôte appelant doit répondre par un nom de connexion. `in.uucpd` vous invite ensuite à saisir un mot de passe, à moins qu'aucun mot de passe ne soit nécessaire. Reportez-vous à la page de manuel `in.uucpd`(1M) pour plus d'informations.

Programmes d'administration UUCP

La plupart des programmes administratifs UUCP se trouvent dans `/usr/lib/uucp`. Les fichiers de base de données les plus basiques se trouvent dans `/etc/uucp`. La seule exception est `uulog` qui se trouve sous `/usr/bin`. Le répertoire personnel de l'ID de connexion `uucp` est `/usr/lib/uucp`. Lorsque vous exécutez les programmes d'administration via `su` ou `login`, utilisez l'ID utilisateur `uucp`. L'ID utilisateur possède les programmes et fichiers de données de spool.

`uulog` — Affiche le contenu de fichiers de journal d'un ordinateur spécifique. Les fichiers journaux sont créés pour chaque ordinateur distant avec lequel votre machine communique. Les fichiers journaux enregistrent chaque utilisation de `uucp`, `uuto` et `uux -a`. Reportez-vous à la page de manuel `uucp`(1C) pour plus d'informations.

`uucleanup` — Vide le répertoire spool. `uucleanup` est normalement exécuté à partir du script shell `uudemon.cleanup`, démarré par `cron`. Reportez-vous à la page de manuel `uucleanup`(1M) pour plus d'informations.

`Uutry` — Teste les capacités de traitement d'appels et ne gère pas le débogage. La commande `Uutry` appelle le démon `uucico` pour établir un lien de

communication entre votre ordinateur et l'ordinateur distant spécifié. Reportez-vous à la page de manuel `Uutry`(1M) pour plus d'informations.

`uucheck` Vérifie la présence de répertoires UUCP, programmes et fichiers de support. `uucheck` peut également contrôler certaines parties du fichier `/etc/uucp/Permissions` afin de détecter des erreurs syntactiques manifestes. Reportez-vous à la page de manuel `uucheck`(1M) pour plus d'informations.

Programmes utilisateur UUCP

Les programmes utilisateur UUCP se trouvent sous `/usr/bin`. Vous n'avez pas besoin d'autorisation spéciale pour utiliser ces programmes.

`cu` Permet de connecter votre ordinateur à un ordinateur distant afin que vous puissiez vous connecter aux deux machines en même temps. La commande `cu` vous permet de transférer des fichiers ou d'exécuter des commandes sur l'un ou l'autre des ordinateurs sans supprimer le lien initial. Reportez-vous à la page de manuel `cu`(1C) pour plus d'informations.

`uucp` Permet de copier un fichier d'un ordinateur à un autre. La commande `uucp` crée des fichiers de travail et des fichiers de données, met le travail en attente de transfert et appelle le démon `uucico`, qui à son tour tente de contacter l'ordinateur distant. Reportez-vous à la page de manuel `uucp`(1C) pour plus d'informations.

`uuto` Permet de copier les fichiers à partir de la machine locale sur le spool répertoire public `/var/spool/uucppublic/receive` sur l'ordinateur distant. Contrairement à la commande `uucp`, qui vous permet de copier un fichier sur n'importe quel répertoire accessible sur l'ordinateur distant, `uuto` place le fichier dans un répertoire spool approprié et indique à l'utilisateur distant de récupérer le fichier avec `uupick`. Reportez-vous à la page de manuel `uuto`(1C) pour plus d'informations.

`uupick` Permet de récupérer les fichiers dans `/var/spool/uucppublic/receive` lorsque les fichiers sont transférés vers un ordinateur à l'aide de la commande `uuto`. Reportez-vous à la page de manuel `uuto`(1C).

`uux` Permet de créer le travail, les données et d'exécuter des fichiers nécessaires à l'exécution des commandes sur une machine distante. Reportez-vous à la page de manuel `uux`(1C) pour plus d'informations.

`uustat`	Affiche l'état des transferts demandés (`uucp`, `uuto` ou `uux`). `uustat` fournit également une méthode de contrôle de transferts mise en queue d'attente. Reportez-vous à la page de manuel `uustat`(1C) pour plus d'informations.

Fichiers de base de données UUCP

Une partie importante de la configuration UUCP est la configuration des fichiers qui composent la base de données UUCP. Ces fichiers se trouvent dans le répertoire `/etc/uucp`. Vous devez modifier ces fichiers pour configurer UUCP ou `asppp` sur votre machine. Les fichiers incluent les éléments suivants :

`Config`	Contient une liste des paramètres des variables. Vous pouvez définir manuellement ces paramètres pour configurer le réseau.
`Devconfig`	Utilisé pour configurer les communications au sein du réseau.
`Devices`	Utilisé pour configurer les communications au sein du réseau
`Dialcodes`	Contient les abréviations dial-code que vous pouvez utiliser dans le champ du numéro de téléphone des entrées de fichier `Systems`. Bien que ce ne soit pas obligatoire, le fichier `Dialcodes` peut être utilisé par `asppp`, ainsi que par UUCP.
`Dialers`	Contient des chaînes de caractpres requises pour négocier avec les modems afin d'établir la connexion avec un ordinateur distant. Le fichier `Dialers` est utilisé par `asppp`, ainsi que par UUCP.
`Grades`	Définit les niveaux des travaux et les autorisations associées à chaque niveau, que les utilisateurs peuvent spécifier pour mettre des travaux en file d'attente sur un ordinateur distant.
`Limites`	Définit le nombre maximum de`uucicos`, `uuxqts` et`uuscheds` simultanés autorisés sur votre ordinateur.
`Autorisations`	Permet de définir le niveau d'accès accordé à des hôtes distants qui tentent de transférer des fichiers ou d'exécuter des commandes sur votre ordinateur.
`Poll`	Définit des ordinateurs intrrogés par votre système avec le moment de l'interrogation.
`Sysfiles`	Affecte des fichiers multiples ou différents à utiliser par `uucico` et `cu` comme `fichiers système`, `de périphériques` et `de dialers`.

`Sysname` Vous permet de définir un nom UUCP unique UUCP pour chaque ordinateur, en plus du nom d'hôte TCP/IP.

`Systems` Contient des informations requises par le démon `uucico`, `cu` et `asppp` pour établir un lien vers un ordinateur distant. Les éléments suivants sont inclus :

- Nom de l'hôte distant
- Nom du périphérique de connexion associé à l'hôte distant
- Heure à laquelle l'hôte peut être contacté
- Numéro de téléphone
- ID de connexion
- Mot de passe

Plusieurs autres fichiers peuvent être considérés comme faisant partie de la base de données de prise en charge mais ne sont pas directement impliqués dans l'établissement d'un lien et le transfert des fichiers.

Configuration des fichiers de base de données UUCP

La base de données UUCP est constituée des fichiers présentées à la section “Fichiers de base de données UUCP” à la page 165. Toutefois, la configuration UUCP de base implique uniquement les fichiers critiques suivants :

- `/etc/uucp/Systems`
- `/etc/uucp/Devices`
- `/etc/uucp/Dialers`

La commande `asppp` utilisant certaines des bases de données UUCP, vous devez comprendre un minimum les fichiers de bases de données importants si vous envisagez de configurer `asppp`. Une fois ces bases de données configurées, l'administration UUCP est relativement simple. En règle générale, vous modifiez d'abord le fichier `Systems`, puis le fichier `Devices`. En général, vous pouvez utiliser le fichier `/etc/uucp/Dialers` par défaut, sauf si vous envisagez d'ajouter des dialers qui ne se trouvent pas dans le fichier par défaut. En outre, vous pouvez également souhaiter utiliser les fichiers suivants pour la configuration UUCP et `asppp` de base :

- `/etc/uucp/Sysfiles`
- `/etc/uucp/Dialcodes`
- `/etc/uucp/Sysname`

Etant donné que ces fichiers travaillent en étroite collaboration, vous devez comprendre l'ensemble de leur contenu avant d'apporter des modifications. Une modification apportée à une

entrée dans un des fichiers peut nécessiter d'appliquer une modification à une entrée associée dans un autre fichier. Les autres fichiers répertoriés à la section “Fichiers de base de données UUCP” à la page 165 ne sont pas aussi dépendants les uns des autres.

Remarque - `asppp` utilise uniquement les fichiers décrits dans cette section. `asppp` n'utilise pas les autres fichiers de base de données UUCP.

♦ ♦ ♦ CHAPITRE 11

Administration d'UNIX-to-UNIX Copy Program

Ce chapitre explique comment démarrer les opérations UUCP après avoir modifié le fichier de base de données qui est pertinent pour vos machines. Le chapitre contient des procédures et des informations sur le dépannage de la configuration et de la maintenance du protocole UUCP sur les machines qui exécutent le système d'exploitation Oracle Solaris, telles que les opérations suivantes :

Administration du protocole UUCP (liste des tâches)

Le tableau ci-dessous fournit des liens vers les procédures qui sont traitées dans ce chapitre, ainsi qu'une brève description de chaque procédure.

TABLEAU 11-1 Liste des tâches pour l'administration du protocole UUCP

Tâche	Description	Pour obtenir des instructions
Autorisation des machines distantes à accéder à votre système	Modifiez le fichier `/etc/passwd` pour ajouter des entrées afin d'identifier les machines qui sont autorisées à accéder à votre système.	"Ajout de connexions UUCP" à la page 170
Démarrage d'UUCP	Utilisez les scripts shell fournis pour démarrer UUCP.	"Démarrage d'UUCP" à la page 171
Activation d'UUCP pour travailler avec TCP/IP	Editez `/etc/uucp/Systems` pour modifier les fichiers pour activer UUCP pour TCP / IP .	"Activation du protocole UUCP pour TCP/IP" à la page 173
Dépannage de problèmes UUCP communs	Utilisez les étapes de diagnostic pour rechercher les modems ou ACU défectueux.	"Recherche de modems ou d'ACU défectueux" à la page 176
	Utilisez les étapes de diagnostic pour déboguer les transmissions.	"Débogage des transmissions" à la page 176

Ajout de connexion UUCP

Pour que les requêtes UUCP (`uucico`) entrantes des ordinateurs distants puissent être traitées correctement, chaque ordinateur doit avoir une connexion à votre système.

▼ Ajout de connexions UUCP

Pour permettre à une machine distante d'accéder à votre système, vous devez ajouter une entrée au fichier `/etc/passwd` comme suit :

1. **Connectez-vous en tant qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Modifiez le fichier `/etc/passwd` et ajoutez l'entrée afin d'identifier la machine qui est autorisée à accéder à votre système.**

   Ci-dessous, une entrée type que vous pourriez placer dans le fichier `/etc/passwd` pour une machine distante autorisée à accéder à votre système avec une connexion UUCP :

   ```
   Ugobi:*:5:5:gobi:/var/spool/uucppublic:/usr/lib/uucp/uucico
   ```

   Par convention, le nom de connexion d'une machine distante est le nom de machine précédé par la lettre majuscule `U`. Notez que le nom ne doit pas dépasser huit caractères. Sinon, vous devrez peut-être le tronquer ou l'abréger.

   L'entrée précédente montre qu'une demande de connexion par `Ugobi` est résolue par `/usr/lib/uucp/uucico`. Le répertoire personnel est `/var/spool/uucppublic`. Le mot de passe est obtenu à partir du fichier `/etc/shadow`. Vous devez accorder du mot de passe et du nom de connexion avec l'administrateur UUCP de la machine distante. L'administrateur distant doit ensuite ajouter une entrée appropriée, avec le nom de connexion et le mot de passe non chiffré, dans le fichier `Systems` de la machine distante.

3. **Accordez du nom de votre machine avec les administrateurs UUCP sur d'autres systèmes.**

   De manière analogue, vous devez coordonner le nom et le mot de passe de votre ordinateur avec les administrateurs UUCP de tous les ordinateurs que vous voulez atteindre par le biais d'UUCP.

Démarrage du protocole UUCP

UUCP comprend quatre scripts shell pour interroger les ordinateurs distants, replanifier les transmissions et nettoyer les fichiers de journal anciens et transmissions non réussies. Les scripts se présentent comme suit :

- `uudemon.poll`
- `uudemon.hour`
- `uudemon.admin`
- `uudemon.cleanup`

Ces scripts shell doivent être exécutés périodiquement afin de vérifier si l'UUCP fonctionne sans problèmes. Le fichier `crontab` permettant d'exécuter les scripts est automatiquement créé dans `/usr/lib/uucp/uudemon.crontab` dans le cadre du processus d'installation de Oracle Solaris, si vous sélectionnez l'installation complète. Sinon, le fichier est créé lorsque vous installez le package UUCP.

Vous pouvez également exécuter les scripts shell UUCP manuellement. Vous pouvez personnaliser le fichier `uudemon.crontab` prototype ci-après pour une machine donnée :

```
#
#ident  "@(#)uudemon.crontab    1.5     97/12/09 SMI"
#
# This crontab is provided as a sample. For systems
# running UUCP edit the time schedule to suit, uncomment
# the following lines, and use crontab(1) to activate the
# new schedule.
#
#48 8,12,16 * * * /usr/lib/uucp/uudemon.admin
#20 3 * * * /usr/lib/uucp/uudemon.cleanup
#0 * * * * /usr/lib/uucp/uudemon.poll
#11,41 * * * * /usr/lib/uucp/uudemon.hour
```

Remarque - Par défaut, les opérations UUCP sont désactivées. Pour activer UUCP, modifiez le calendrier et supprimez le commentaire des lignes appropriées dans le fichier `uudemon.crontab` .

▼ Démarrage d'UUCP

Pour activer le fichier `uudemon.crontab`, effectuez les opérations suivantes :

1. **Connectez-vous en tant qu'administrateur.**
   Pour plus d'informations, reportez-vous à la section “ A l’aide de vos droits administratifs attribués ” du manuel “ Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ”.

2. **Modifiez le fichier `/usr/lib/uucp/uudemon.crontab` et modifiez les entrées selon les besoins.**

3. **Activez le fichier `uudemon.crontab` en exécutant la commande suivante :**

```
crontab < /usr/lib/uucp/uudemon.crontab
```

Script shell `uudemon.sondage`

The default `uudemon.poll`le script shell lit le fichier `/etc/uucp/Poll` une fois chaque heure. S'il est prévu que des machines dans le fichier `Poll` soient interrogées, un fichier de travail (`C.` *sysnxxxx*) est placé dans le répertoire `/var/spool/uucp/`*nodename*. *nodename* représente le nom de noeud UUCP de la machine.

Le script shell est planifié pour s'exécuter une fois par heure, avant `uudemon.hour`, de sorte que les fichiers de travail sont en place lorsque `uudemon.hour` est appelé.

Script shell `uudemon.hour`

Par défaut, le script shell `uudemon.hour` exécute ce qui suit :

- Appelle le programme `uusched` afin de rechercher les répertoires de spool pour les fichiers de travail (`C.`) qui n'ont pas été traités. Le script programme ensuite le transfert de ces fichiers vers une machine distante.
- Appelle le démon `uuxqt` afin de rechercher les répertoires de spool pour exécuter des fichiers (`X.`) qui ont été transférés à votre ordinateur et n'ont pas été traités à ce moment-là.

Par défaut, `uudemon.hour` s'exécute deux fois par heure. Il se peut que vous souhaitiez que `uudemon.hour` soit exécuté plus souvent si vous prévoyez un très fort taux d'échec des appels à des machines distantes.

Script shell `uudemon.admin`

Par défaut, le script shell `uudemon.admin` exécute ce qui suit :

- Exécute la commande `uustat` avec les options `p` et `q`. L'option `q` donne des informations sur l'état des fichiers de travail (`C.`), des fichiers de données (`D.`) et exécute les fichiers (`X.`) qui sont mis en file d'attente. L'option `p` imprime les informations sur les traitements réseau qui sont répertoriés dans les fichiers de verrouillage (`/var/spool/locks`).
- Envoie les informations d'état générés à la connexion administrative `uucp` à l'aide du `mail`.

`uudemon.cleanup`, script shell

Par défaut, le script shell `uudemon.cleanup` exécute ce qui suit :

- Collecte les fichiers journaux de machines individuelles dans le répertoire `/var/uucp/.Log`, fusionne ces fichiers et les place dans le répertoire `/var/uucp/.Old` avec les autres informations sur des journaux antérieurs.
- Supprime les fichiers de travail (`C.`) vieux de sept jours ou plus, les fichiers de données (`D.`) vieux de sept jours ou plus et les fichiers d'exécution (`X.`) vieux de deux jours ou plus des fichiers spool
- Renvoie à l'expéditeur le courrier qui ne peut pas être distribué.
- Envoie un courriel avec la synthèse des informations d'état collectées durant la journée en cours à la connexion UUCP administrative (`uucp`)

Exécution du protocole UUCP sur TCP/IP

Pour exécuter UUCP sur un réseau TCP/IP, vous devez effectuer quelques modifications, comme décrit dans cette section.

▼ Activation du protocole UUCP pour TCP/IP

1. **Connectez-vous en tant qu'administrateur.**
   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Editez le fichier `/etc/uucp/Systems` afin de vous assurer que les entrées ont les champs suivants :**
   System-Name Time TCP Port networkname Standard-Login-Chat
   Une entrée standard ressemble à ceci :

   ```
   rochester Any TCP - ur-seneca login: Umachine password: xxx
   ```

   Notez que le champ *networkname* vous permet de spécifier explicitement le nom d'hôte TCP/IP. Cette capacité est importante pour certains sites. Dans l'exemple précédent, le site a le nom de noeud UUCP `rochester`, qui est différent de son nom d'hôte TCP/IP `ur-seneca`. En outre, une toute autre machine pourrait facilement exécuter UUCP et avoir le nom d'hôte TCP/IP de `rochester`.
   Le champ port du fichier `Systèmes` doit contenir l'entrée `-`. Cette syntaxe revient à répertorier l'entrée comme `uucp`. Dans la plupart des cas, le champ *networkname* contient la même valeur

que le nom de système et le champ Port est `-`, qui dit d'utiliser le port uucp standard à partir de la base de données `services`. Le démon `in.uucpd` s'attend à ce que la machine distante envoie son ID de connexion et mot de passe pour authentification et `in.uucpd` vous invite à les renseigner, de la même façon que `getty` et `login`.

3. **Editez le fichier `/etc/inet/services` afin de définir un port pour UUCP :**

```
uucp    540/tcp    uucpd        # uucp daemon
```

Normalement, vous n'avez pas besoin de modifier l'entrée. Cependant, si votre machine exécute NIS en tant que service de noms, vous devez vous assurer que `config/service` du service `svc:/system/name-service/switch` vérifie d'abord `files`, puis `nis`. Si la propriété `config/service` n'est pas définie, vérifiez la propriété `config/default`.

4. **Vérifiez qu'UUCP est activé.**

```
# svcs network/uucp
```

Le service UUCP est géré par l'utilitaire de gestion des services (Service Management Facility). Pour lancer une interrogation sur l'état de ce service, vous pouvez utiliser la commande `svcs`. Pour obtenir un aperçu de l'application, reportez-vous au “ Gestion des instances de service SMF ” du manuel “ Gestion des services système dans Oracle Solaris 11.2 ”

5. **(Facultatif) Si nécessaire, activez UUCP en tapant la commande suivante :**

```
# inetadm -e network/uucp
```

Sécurité et maintenance du protocole UUCP

Une fois que vous avez configuré UUCP, sa maintenance est relativement simple. Cette section explique les tâches UUCP continues liées à la sécurité, à la maintenance et au dépannage.

Configuration de la sécurité du protocole UUCP

Le fichier par défaut `/etc/uucp/Permissions` offre une sécurité maximale pour vos liaisons UUCP. Le fichier `Permissions` par défaut ne contient aucune entrée.

Pour chaque machine distante, vous pouvez définir d'autres paramètres pour définir ce qui suit :

- Les moyens par lesquels la machine distante peut recevoir les fichiers à partir de votre machine
- Les répertoires pour lesquels la machine distante dispose d'une autorisation d'accès en lecture et en écriture
- Les commandes que l'ordinateur distant peut utiliser pour une exécution à distance

Ci-dessous, une entrée du fichier `Permissions` standard :

```
MACHINE=datsun LOGNAME=Udatsun VALIDATE=datsun
COMMANDS=rmail REQUEST=yes SENDFILES=yes
```

Cette entrée permet aux fichiers d'être envoyés vers et reçus de répertoires UUCP "normaux", et non à partir de n'importe où dans le système. L'entrée permet également la validation du nom d'utilisateur UUCP au moment de la connexion.

Maintenance régulière du protocole UUCP

UUCP ne demande pas beaucoup de maintenance. Toutefois, vous devez vous assurer que le fichier `crontab` est en place, comme décrit dans la section “Démarrage d'UUCP” à la page 171. Votre devez surveiller l'augmentation de la taille des fichiers de courrier et du répertoire public.

E-mail pour UUCP

Tous les courriels générés par les programmes et scripts UUCP sont envoyés à l'ID d'utilisateur `uucp`. Si vous ne vous connectez pas fréquemment sous l'identité de cet utilisateur, vous n'aurez peut-être pas conscience du fait que le courrier s'accumule et consomme l'espace disque. Pour résoudre ce problème, créez un alias dans `/etc/mail/aliases` et redirigez ce courrier vers l'utilisateur `root` ou vers vous-même et les autres personnes chargées de la maintenance d'UUCP. N'oubliez pas d'exécuter la commande `newaliases` après avoir modifié le fichier `aliases`.

Répertoire public UUCP

Le répertoire `/var/spool/uucppublic` est un emplacement au sein de chaque système vers lequel UUCP est capable, par défaut, de copier des fichiers. Chaque utilisateur a l'autorisation de modifier `/var/spool/uucppublic`, ainsi que de lire et d'écrire des fichiers du répertoire. Toutefois, le sticky bit du répertoire étant défini, le mode de ce répertoire est 01777. Par conséquent, les utilisateurs ne peuvent pas supprimer les fichiers qui ont été copiés sur celui-ci et qui appartiennent à `uucp`. Vous seul, en tant qu'administrateur UUCP connecté comme utilisateur `root` ou `uucp`, pouvez supprimer des fichiers de ce répertoire. Afin d'éviter l'accumulation incontrôlée des fichiers dans ce répertoire, vous devez vous assurer que vous en supprimez régulièrement.

Si cette maintenance ne convient pas aux utilisateurs, encouragez-les à utiliser `uuto` et `uupick` au lieu d'enlever l'élément binaire permanent, défini pour des raisons de sécurité. Reportez-vous à la page de manuel `uuto`(1C) pour obtenir plus d'instructions sur l'utilisation des commandes `uuto` et `uupick`. Vous pouvez également restreindre le mode du répertoire sur un seul groupe de

personnes. Si vous ne souhaitez pas prendre le risque que quelqu'un sature votre disque, vous pouvez même refuser l'accès UUCP à ce disque.

Dépannage du protocole UUCP

Ces procédures décrivent la résolution des problèmes d'UUCP courants.

▼ Recherche de modems ou d'ACU défectueux

Vous pouvez vérifier de différentes manières si les modems ou autres ACU ne fonctionnent pas correctement.

1. **Connectez-vous en tant qu'administrateur.**
   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Obtenir des décomptes et raisons de la défaillance de contact en exécutant la commende suivante :**

   ```
   # uustat -q
   ```

3. **Appelez via une ligne particulière et imprimez les informations relatives à la tentative de débogage.**
   La ligne doit être définie comme `direct` dans le fichier `/etc/uucp/Devices`. Vous devez ajouter un numéro de téléphone à la fin de la ligne de commande si la ligne est connectée à un composeur automatique, ou le périphérique doit être configuré comme `direct`. Entrez :

   ```
   # cu -d -l line
   ```

   line est `/dev/cua/un`.

▼ Débogage des transmissions

Si vous ne pouvez pas contacter un ordinateur particulier, vous pouvez contrôler les communications avec cet ordinateur moyennant `Uutry` et `uucp`.

1. **Connectez-vous en tant qu'administrateur.**
   Pour plus d'informations, reportez-vous à la section " A l'aide de vos droits administratifs attribués " du manuel " Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.2 ".

2. **Tentez d'établir le contact :**

   ```
   # /usr/lib/uucp/Uutry -r machine
   ```

   Remplacez *machine* par le nom d'hôte de la machine que vous n'êtes pas en mesure de contacter. Cette commande effectue les opérations suivantes :

   - Démarre le démon de transfert (`uucico`) au moment du débogage. Vous pouvez obtenir des informations de débogage si vous êtes utilisateur `root`.
   - Dirige les résultats du débogage vers `/tmp/` *machine*.
   - Imprime les résultats du débogage vers votre terminal en émettant la commande suivante :

     ```
     # tail -f
     ```

     Appuyez sur Ctrl-C pour arrêter l'émission des résultats. Vous pouvez copier les résultats de `/tmp/` *machine* si vous souhaitez les enregistrer.

3. **Si `Uutry` ne peut pas séparer le problème, essayez de mettre la tache en attente :**

   ```
   # uucp -r file machine\!/dir/file
   ```

file	Utilisez le nom du fichier que vous souhaitez transférer.
machine	Utilisez le nom de la machine vers laquelle vous voulez effectuer la copie.
/dir/file	Spécifiez l'emplacement du fichier pour l'autre machine.

4. **Exécutez la commande suivante :**

   ```
   # Uutry
   ```

   Si vous ne parvenez toujours pas à résoudre le problème, il vous faudra peut-être appeler votre représentant du support technique local. Enregistrez les résultats du débogage, qui peuvent vous aider à diagnostiquer le problème.

Remarque - Vous pouvez également augmenter ou réduire le niveau de débogage qui est fourni par `Uutry` via l'option `-x` *n*. *n* indique le niveau de débogage. Le niveau de débogage par défaut pour `Uutry` est 5.

Le débogage du niveau 3 fournit les informations debase concernant le moment et la manière de l'établissement de la connexion, mais ne fournit pas beaucoup d'informations sur la transmission. Le niveau de débogage 9, cependant, fournit des informations exhaustives sur le processus de transmission. N'oubliez pas que le débogage se produit aux deux extrémités de la transmission. Si vous avez l'intention d'utiliser un niveau supérieur à 5 sur un texte relativement grand, contactez l'administrateur de l'autre site et déterminez à quel moment modifier le niveau.

Fichier `/etc/uucp/Systems` UUCP

Vérifiez si vos informations dans le fichiers `Systèmes` est à jour si avez du mal à établir le contact avec un ordinateur en particulier. Certaines informations susceptibles d'être obsolètes pour une machine sont les suivantes :

- Numéro de téléphone
- ID de connexion
- Mot de passe

Vérification des messages d'erreur UUCP

UUCP a deux types de messages d'erreur : `ASSERT` et `STATUS`.

- Quand un processus est annulé, les messages d'erreur `ASSERT` sont enregistrées dans `/var/uucp/.Admin/errors`. Ces messages incluent le nom de fichier, `sccsid`, le numéro de ligne et le texte. Ces messages sont généralement le résultat de problèmes au niveau du système.
- `Les messages d'erreur STATUS` sont enregistrées dans le répertoire `/var/uucp/.Status`. Le répertoire contient un fichier distinct pour chaque machine distante avec laquelle votre ordinateur tente de communiquer. Ces fichiers contiennent des informations d'état à propos de tentatives de communication et indiquant si la communication a été effectuée avec succès.

Vérification des informations de base

Plusieurs commande sont disponibles pour le contrôle d'informations de base sur la mise en réseau :

- Utilisez la commande `uuname` pour répertorier les machines que votre machine peut contacter.
- Utilisez la commande `uulog` pour afficher le contenu des répertoires des journaux d'hôtes particuliers.
- Utilisez la commande `uucheck -v` pour vérifier la présence de fichiers et répertoires requis par`uucp`. Cette commande vérifie également le fichier `Permissions` et affiche des informations sur les autorisations que vous avez configurés.

♦ ♦ ♦ CHAPITRE 12

Fichiers d'UNIX-to-UNIX Copy Program

Ce chapitre fournit des informations de référence pour l'utilisation d'UUCP. Il aborde les sujets suivants :

Fichier `/etc/uucp/Systems` UUCP

Le fichier `/etc/uucp/Systems` contient les informations requises par le démon `uucico` pour établir un lien de communication vers un ordinateur distant. Le fichier `/etc/uucp/Systems` est le premier fichier que vous devez modifier pour configurer UUCP.

Chaque entrée du fichier `Systems` représente un ordinateur distant avec lequel votre hôte communique. Un hôte particulier peut avoir plusieurs entrées. Les entrées supplémentaires représentent d'autres chemins de communication qui sont testés dans un ordre séquentiel. En outre, par défaut, UUCP empêche tout ordinateur qui n'apparaît pas dans le fichier `/etc/uucp/Systems` de se connecter à votre hôte.

A l'aide du fichier `Sysfiles`, vous pouvez définir plusieurs fichiers à utiliser comme fichiers `Systems`. Reportez-vous à la section “Fichier `/etc/uucp/Sysfiles` UUCP” à la page 198 pour obtenir une description des fichiers `Sysfiles`.

Ci-après, vous trouverez la syntaxe d'une entrée dans le fichier Systems :

```
System-Name    Time    Type    Speed    Phone    Chat Script
```

Consultez l'exemple suivant d'entrée du fichier Systems.

EXEMPLE 12-1 Entrées du fichier /etc/uucp/Systems

```
Arabian     Any  ACUEC 38400 111222  ogin: Puucp ssword:beledi
```

Arabian	Entrée pour le champ System-Name (Nom du système). Pour plus d'informations, reportez-vous à la section “Champ de nom du système dans le fichier /etc/uucp/Systems” à la page 180.
Tous	Entrée pour le champ Time (Date et heure). Pour plus d'informations, reportez-vous à la section “Champ Time du fichier /etc/uucp/Systems” à la page 181.
ACUEC	Entrée pour le champ Type. Pour plus d'informations, reportez-vous à la section “Champ Type du fichier /etc/uucp/Systems” à la page 182.
38400	Entrée pour le champ Speed (Vitesse). Pour plus d'informations, reportez-vous à la section “Champ Speed du fichier /etc/uucp/Systems” à la page 182.
111222	Entrée pour le champ Phone (Téléphone). Pour plus d'informations, reportez-vous à la section “Champ Phone du fichier /etc/uucp/Systems” à la page 183.
ogin: Puucp ssword:beledi	Entrée pour le champ Chat Script (script de discussion). Pour plus d'informations, reportez-vous à la section “Champ Phone du fichier /etc/uucp/Systems” à la page 183.

Champ de nom du système dans le fichier /etc/uucp/Systems

Ce champ contient le nom de noeud de l'ordinateue distant. Sur les réseaux TCP/IP, ce nom peut être le nom d'hôte de l'ordinateur ou un nom spécialement créé pour les communications UUCP via le fichier /etc/uucp/Sysname. Reportez-vous à la section “Fichier /etc/uucp/Systems UUCP” à la page 179. Dans l'Exemple 12-1, “Entrées du fichier /etc/uucp/Systems”, le champ System-Name contient une entrée pour l'hôte distant Arabian.

Champ Time du fichier /etc/uucp/Systems

Ce champ spécifie le jour de la semaine et l'heure autorisés pour l'appel de l'ordinateur distant. Le format du champ Time est le suivant :

```
daytime[;retry]
```

Portion *day* du champ Time

La portion *day* peut être une liste contenant certaines des entrées suivantes.

`Su Mo Tu We Th Fr Sa`	Pour des jours distincts.
`Wk`	Pour n'importe quel jour de la semaine.
`Tous`	Pour n'importe quel jour.
`Jamais`	Votre hôte n'appelle jamais l'ordinateur distant. L'appel doit être initié par l'ordinateur distant. Votre hôte fonctionne ensuite en *mode passif*.

Portion *time* du champ Time

L'Exemple 12-1, “Entrées du fichier /etc/uucp/Systems” présente la valeur `Any` dans le champ Time, ce qui indique que l'hôte `Arabian` peut être appelé à tout moment.

La portion *time* doit être une plage d'heures spécifiées au format 24 heures, par exemple `0800-1230` pour la période allant de 8:30h à 00:30h. Si aucune portion *time* n'est spécifiée, on part du principe que les appels peuvent être effectués à tout moment de la journée.

Une plage d'heures qui s'étend sur 0000 est autorisée. Par exemple, `0800-0600` signifie que, mis à part la période entre 6h et 8h du matin, toutes les heures sont autorisées.

Portion *retry* du champ Time

Le sous-champ *retry* vous permet de spécifier la durée minimale (en minutes) avant une nouvelle tentative, après l'échec de la précédente. L'attente par défaut est de 60 minutes. Le séparateur de sous-champ est un point-virgule (;). Par exemple, `Any;9` est interprété suit : possibilité d'appeler l'ordinateur à tout moment, mais attente d'au moins 9 minutes avant la tentative suivante en cas de défaillance.

Si vous ne spécifiez pas d'entrée *retry*, un algorithme back-off exponentiel est utilisé. Cela signifie que UUCP démarre après un temps d'attente par défaut qui augmente à mesure que le nombre d'échecs augmente. Par exemple, supposons que le délai initial entre les nouvelles tentatives est de 5 minutes. Si aucune réponse ne se produit, la tentative suivante a lieu 10 minutes plus tard. La tentative suivante aura ensuite lieu 20 minutes plus tard, et ainsi de suite jusqu'à ce que le délai maximal (23 heures) soit atteint. Si *retry* est spécifié, la valeur indiquée spécifie toujours la durée avant le prochain essai. Sinon, l'algorithme back-off est utilisé.

Champ Type du fichier /etc/uucp/Systems

Ce champ contient le type de périphérique à utiliser pour établir la liaison de communication à l'ordinateur distant. Le mot-clé utilisé dans ce champ est mis en correspondance avec le premier champ des entrées du fichier `Devices`.

EXEMPLE 12-2 Mot-clé associé au champ Type

```
Arabian    Any    ACUEC, g    38400    1112222    ogin: Puucp ssword:beledi
```

Vous pouvez définir le protocole utilisé pour établir le contact avec le système en ajoutant le protocole au champ Type. L'exemple précédent montre comment attacher le protocole `g` pour le type de périphérique `ACUEC`. Pour plus d'informations sur les protocoles, reportez-vous à la section “Définitions de protocole dans le fichier /etc/uucp/Devices” à la page 192.

Champ Speed du fichier /etc/uucp/Systems

Ce champ, également connu sous le nom de champ de Classe spécifie la vitesse de transfert du périphérique utilisé pour la laison de communication. Le champ de vitesse UUCP peut contenir une lettre et une vitesse, `C1200` ou `D1200` par exemple, pour faire la différence entre les classes de dialers. Reportez-vous à la section “Champ Class dans le fichier /etc/uucp/Devices” à la page 189.

Certains périphériques peuvent être utilisés à n'importe quelle vitesse, de sorte que le mot-clé `Any` peut être utilisé. Ce champ doit correspondre au champ Class de l'entrée du fichier `Périphériques` associée.

EXEMPLE 12-3 Entrée dans le champ Speed

```
eagle    Any    ACU, g    D1200    NY3251    ogin: nuucp ssword:Oakgrass
```

Si les informations de ce champ ne sont pas requises, vous pouvez utiliser un trait d'union (`-`) comme caractère générique du champ.

Champ Phone du fichier /etc/uucp/Systems

Ce champ vous permet de spécifier le numéro de téléphone connu comme un *marqueur*, de l'ordinateur distant pour les dialers automatiques, appelés également *sélecteurs de port*. Le numéro de téléphone est constitué d'une abréviation alphabétique facultative et d'une partie numérique. Si une abréviation est utilisé, elle doit être répertoriée dans le fichier `Dialcodes`.

EXEMPLE 12-4 Entrée du champ Phone

```
nubian    Any    ACU       2400    NY555-1212    ogin: Puucp ssword:Passuan
eagle     Any    ACU, g    D1200   NY=3251       ogin: nuucp ssword:Oakgrass
```

Dans le champ `Phone`, un signe égale (`=`) indique à l'`ACU` d'attendre une seconde tonalité d'invitation à numéroter avant de composer les numéros suivants. Un tiret (`-`) dans la chaîne indique à l'`ACU` d'effectuer une pause de quatre secondes avant de composer le prochain numéro.

Si votre ordinateur est connecté à un sélecteur de port, vous pouvez accéder à d'autres ordinateurs connectés à ce sélecteur. Les entrées du fichier `Systems` pour ces machines distantes ne doivent pas posséder de numéro de téléphone dans le champ `Phone`. Au lieu de cela, ce champ doit contenir le jeton à transmettre au commutateur. De cette façon, le sélecteur de port connaît l'ordinateur distant avec lequel votre hôte souhaite communiquer, généralement simplement le nom du système. L'entrée du fichier `Devices` associé doit avoir un `\D` à la fin de l'entrée afin de s'assurer que ce champ n'est pas traduit à l'aide du fichier `Dialcodes`.

Champ Phone du fichier /etc/uucp/Systems

Ce champ. égaglement appelé champ de connexion (Login) contient une chaîne de caractères appelée un *chat-script*. Le script de discussion contient les caractères que les ordinateurs locaux et distants doivent se transmettre lors de leur première conversation. Les scripts de discussion ont le format suivant :

expect send [expect send] ....

expect représente la chaîne que l'hôte local s'attend à recevoir de l'hôte distant pour lancer la conversation. *send* est la chaîne que l'hôte local envoie une fois que l'hôte local a reçu la chaîne *expect* de l'hôte distant. Un script de discussion peut avoir plus d'une séquence Send-Expect.

Un script de discussion de base peut contenir les éléments suivants :

- Invite de connexion que l'hôte local s'attend à recevoir de l'ordinateur distant
- Nom de connexion que l'hôte local envoie à l'ordinateur distant afin d'établir la connexion
- Invite de mot de passe que l'hôte local s'attend à recevoir de l'ordinateur distant
- Mot de passe que l'hôte local envoie à l'ordinateur distant

Le champ *expect* peut être composé de sous-champs de la forme suivante :

expect[-send-expect]...

L'option -*send* est envoyée si la valeur *expect* précédente n'est pas lue correctement. L'option -*expect* qui suit -*send* est la chaîne attendue suivante.

Par exemple, avec les chaînes `login--login`, l'UUCP sur l'hôte local attend `login`. Si l'UUCP reçoit `login` à partir de l'ordinateur distant, l'UUCP passe au champ suivant. Si l'UUCP ne reçoit pas `login`, l'UUCP envoie un retour chariot, puis recherche de nouveau `login`. Si l'ordinateur local n'attend pas initialement de caractères, utilisez les caractères `""`, pour la chaîne NULL, dans le champ *expect*. Tous les champs *send* sont envoyés avec un retour chariot à la fin, sauf si la chaîne *send* se termine par un `\c`.

Ce qui suit est un exemple d'entrée du fichier `Systems` qui utilise une chaîne *expect-send* :

```
sonora Any ACUEC 9600 2223333 "" \r \r ogin:-BREAK-ogin: Puucpx ssword:xyzzy
```

Cet exemple indique à l'UUCP sur l'hôte local d'envoyer deux retours chariot et d'attendre `ogin:` (pour `Login:`). Si `ogin`: n'est pas reçu, envoyez un `BREAK`. Lorsque vous recevez `ogin:`, envoyez le nom de connexion `Puucpx`. Lorsque vous recevez `ssword:` (pour `Password:`), envoyez le mot de passe `xyzzy`.

La table suivante comporte quelques caractères d'échappement utiles.

TABLEAU 12-1 Caractères d'échappement utilisés dans le champ Chat-Script du fichier `Systems`

Caractère d'échappement	Explication
`\b`	Envoie ou attend un caractère de retour arrière.
`\c`	Placé à la fin d'une chaîne, supprime le retour chariot normalement envoyé. Sinon il est ignoré.
`\d`	Attend 1 à 3 secondes avant d'envoyer d'autres caractères.
`\E`	Démarre la vérification d'écho. A partir de ce point, chaque fois qu'un caractère est transmis, l'UUCP attend que le caractère soit reçu avant de poursuivre ses vérifications.
`\e`	Renvoie des marques en écho.
`\H`	Ignore une déconnexion. Utilisez cette option pour les modems de rappel automatique.
`\K`	Envoie un caractère BREAK.
`\M`	Active un indicateur `CLOCAL`.
`\m`	Désactive l'indicateur `CLOCAL`.
`\n`	Envoie ou attend un caractère de nouvelle ligne.
`\N`	Envoie un caractère NUL (ASCII NUL).
`\p`	Effectue une pause pendant environ 1/4 à 1/2 seconde.
`\r`	Envoie ou attend un retour chariot.
`\s`	Envoie ou attend un caractère d'espace.

Caractère d'échappement	Explication
\t	Envoie ou attend un caractère de tabulation.
EOT	Envoie un EOT, suivi d'une nouvelle ligne, deux fois.
BREAK	Envoie un caractère BREAK.
ddd	Envoie ou attend le caractère représenté par les nombres octaux (*ddd*).

Activation du rappel automatique par l'intermédiaire du script de discussion

Certaines sociétés configurent des serveurs d'appels entrants afin de gérer les appels à partir des ordinateurs distants. Par exemple, votre société peut avoir un serveur d'appels entrants avec un modem de rappel automatique que les employés peuvent appeler à partir de leurs ordinateurs personnels. Une fois que le serveur d'appels entrants a identifié l'ordinateur distant, le serveur d'appels entrants déconnecte le lien vers l'ordinateur distant, puis le rappelle. Le lien de communication est alors rétabli.

Vous pouvez faciliter le rappel automatique en utilisant l'option \H dans le script de discussion du fichier Systems à l'endroit où le rappel automatique doit se produire. Incluez l'option \H dans une chaîne Expect à l'endroit où le serveur d'appels entrants devrait raccrocher.

Par exemple, supposons que le script de discussion qui appelle un serveur d'appels entrants contienne la chaîne suivante :

```
INITIATED\Hogin:
```

La fonction de numérotation UUCP sur l'ordinateur local s'attend à recevoir les caractères, INITIATED, depuis le serveur d'appels entrants. Une fois les caractères INITIATED mis en correspondance, l'utilitaire de numérotation vide tous les caractères suivants que l'utilitaire de numérotation reçoit jusqu'à ce que le serveur d'appels entrants raccroche. L'utilitaire de numérotation local attend jusqu'à ce qu'il reçoive la partie suivante de la chaîne attendue, les caractères ogin:, à partir du serveur d'appels entrants. Une fois ogin: reçu, l'utilitaire de numérotation continue alors à exécuter le script de discussion.

Une chaîne de caractères ne doit pas nécessairement précéder ou suivre directement le \H, comme le montre la chaîne modèle précédente.

Contrôle du flux matériel dans le fichier /etc/uucp/Systems

Vous pouvez également utiliser la chaîne de *valeur* pseudo-envoi STTY= pour définir les caractérisques du modem. Par exemple, STTY=crtscts active le contrôle de flux matériel

sortant. STTY accepte tous les modes stty. Reportez-vous aux pages du manuel stty(1) et termio(7I) pour tous les détails.

L'exemple suivant active le contrôle de flux matériel dans une entrée du fichier Systems :

```
unix Any ACU 2400 12015551212 "" \r ogin: Puucp ssword:Passuan "" \ STTY=crtscts
```

Cette chaîne pseudo-send peut également être utilisée dans les entrées dans le fichier Dialers.

Définition de la parité dans le fichier /etc/uucp/Systems

Dans certaines situations, vous devez réinitialiser la parité car le système que vous appelez vérifie la parité des ports et supprime la ligne si elle est incorrecte. La paire expect-send, "" P_ZERO, définit le bit de gauche (bit de parité) sur 0. Consultez la paire expect-send dans l'exemple suivant :

```
unix Any ACU 2400 12015551212 "" P_ZERO "" \r ogin: Puucp ssword:Passuan
```

Les éléments suivants sont des paires de parité qui peuvent suivre la paire expect-send, "" P_ZERO :

"" P_EVEN	Définit la parité sur pair, qui est la valeur par défaut
"" P_ODD	Définit la parité sur impair
"" P_ONE	Définit le bit de parité sur 1

Ces paires de parité peuvent être insérées n'importe où dans le script de discussion. Les paires de parité s'appliquent à toutes les informations du script de discussion qui suivent "" P_ZERO, la paire expect-send. Une paire de parité peut également être utilisée dans le fichier Dialers. L'exemple suivant inclut les données de la paire de parité, "" P_ONE :

```
unix Any ACU 2400 12015551212 "" P_ZERO "" P_ONE "" \r ogin: Puucp ssword:Passuan
```

Fichier /etc/uucp/Devices UUCP

Le fichier /etc/uucp/Devices contient des informations relatives à tous les périphériques pouvant être utilisés pour établir un lien vers un ordinateur distant. Ces périphériques incluent les ACU (dont les modems haut-débit), les liens directs et les connexions réseau.

Une entrée du fichier /etc/uucp/Devices respecte la syntaxe suivante :

```
Type   Line   Line2   Class   Dialer-Token-Pairs
```

L'entrée ci-dessous est une entrée du fichier Devices pour un modem U.S. Robotics V.32bis connecté au port A et en cours d'exécution à 38 400 bit/s.

```
ACUEC   cua/a   -   38400   usrv32bis-ec
```

ACUEC	Entrée du champ Type. Pour plus d'informations, reportez-vous à la section “Champ Type du fichier /etc/uucp/Devices” à la page 187.
cua/a	Entrée du champ Line (Ligne). Pour plus d'informations, reportez-vous à la section “Champ Line dans le fichier /etc/uucp/Devices” à la page 188.
-	Entrée du champ Line2 (Ligne 2). Pour plus d'informations, reportez-vous à la section “Champ Line2 dans le fichier /etc/uucp/Devices” à la page 189.
38400	Entrée du champ Class. Pour plus d'informations, reportez-vous à la section “Champ Class dans le fichier /etc/uucp/Devices” à la page 189.
usrv32bis-ec	Entrée du champ Dialer-Token-Pair (Paire jeton-dialer). Pour plus d'informations, reportez-vous à la section “Champ Dialer-Token-Pairs dans le fichier /etc/uucp/Devices” à la page 190.

Chaque champ est décrit dans la section suivante.

Champ Type du fichier /etc/uucp/Devices

Ce champ décrit le type de liaison établi par le périphérique. Le champ Type UUCP peut contenir l'un des mots-clés décrits dans les sections suivantes.

Mot-clé Direct

Le mot-clé Direct apparaît principalement dans les entrées pour les connexions cu . Il indique que le lien est un lien direct vers un autre ordinateur ou un sélecteur de port. Créez une entrée distincte pour chaque ligne à laquelle vous voulez faire référence à l'aide de l'option -l de cu.

Mot-clé ACU

Le mot-clé ACU indique que le lien vers un ordinateur distant (via cu, UUCP, asppp, ou Solaris PPP 4.0) est effectué par le biais d'un modem. Ce modem peut être connecté directement à votre ordinateur ou indirectement via un sélecteur de port.

Sélecteur de port

Le sélecteur de port est une variable qui est remplacé dans le champ Type par le nom d'un sélecteur de port. Les sélecteurs de port sont des périphériques connectés à un réseau qui invitent à fournir le nom d'un modem appelant, puis y fournissent l'accès. Le fichier /etc/uucp/Dialers contient les scripts appelant uniquement pour les sélecteurs de port micom et develcon. Vous pouvez ajouter vos propres entrées de sélecteur de port au fichier Dialers. Pour plus d'informations, reportez-vous à la section “Fichier /etc/uucp/Dialers UUCP” à la page 193.

Variable System-Name

Cette variable est remplacée par le nom d'un ordinateur dans le champ Type, ce qui indique que le lien est un lien direct vers cet ordinateur. Ce schéma est utilisé pour associer la ligne dans cette entrée du fichier Périphériques avec une entrée du fichier /etc/uucp/Systems pour l'ordinateur *nom du système* .

Champs Type des fichiers Devices et Systems

Exemple 12-5, “Comparaison des champs Type dans les fichiers Devices et Systems” montre une comparaison entre les champs dans /etc/uucp/Devices et les champs dans /etc/uucp/Systems. Le mot-clé utilisé dans le champ Type du fichier Devices est comparé au troisième champ des entrées du fichier Systems. Dans le fichier Devices, le champ Type dispose d'une entrée ACUEC, qui indique une unité d'appel automatique, dans cet exemple un modem V.32bis. Cette valeur est mise en correspondance avec le champ Type du fichier Systems qui contient également l'entrée ACUEC. Pour plus d'informations, reportez-vous à la section “Fichier /etc/uucp/Systems UUCP” à la page 179.

EXEMPLE 12-5 Comparaison des champs Type dans les fichiers Devices et Systems

Vous trouverez ci-dessous un exemple d'entrée dans le fichier Devices.

```
ACUEC cua/a - 38400 usrv32bis-ec
```

Vous trouverez ci-dessous un exemple d'entrée dans le fichier Systems.

```
Arabian Any ACUEC 38400 111222 ogin: Puucp ssword:beledi
```

Champ Line dans le fichier /etc/uucp/Devices

Ce champ contient le nom de périphérique de la ligne (connu comme port) associé avec l'entrée Devices. Si le modem associé à une entrée spécifique était connecté à un périphérique /dev/

cua/a (port série A), le nom saisi dans ce champ serait cua/a. Un indicateur de contrôle de modem facultatif, M, peut être utilisé dans le champ Line pour indiquer que le périphérique doit être ouvert sans attendre de porteuse. Ainsi,

```
cua/a,M
```

Champ Line2 dans le fichier /etc/uucp/Devices

Ce champ est un caractère générique. Utilisez toujours un trait d'union (-) ici. Les dialers de type 801, qui ne sont pas pris en charge dans le système d'exploitation Oracle Solaris, utilisent le champ Line2. Les autres dialers n'utilisent normalement pas cette configuration, mais nécessitent tout de même un trait d'union dans ce champ.

Champ Class dans le fichier /etc/uucp/Devices

Le champ Class contient la vitesse du périphérique si mot clé ACU ou Direct est utilisé dans le champ Type. Cependant, le champ Class peut contenir une lettre et une vitesse, C1200 ou D1200 par exemple, pour faire la différence entre les classes de dialers (Centrex ou Dimension PBX par exemple).

Cette distinction est nécessaire car de nombreux bureaux de grande taille possèdent plusieurs types de réseaux téléphoniques. Un réseau peut être dédié aux communications internes d'un bureau uniquement, tandis qu'un autre réseau gère les communications externes. Dans une telle situation, vous devez distinguer la ou des lignes utilisée(s) pour les communications internes et pour les communications externes.

Le mot-clé utilisé dans le champ Class du fichier Périphériques est mis en correspondance avec le champ Speed du fichier Systems.

EXEMPLE 12-6 Champ Class du fichier Devices

```
ACU   cua/a   -   D2400  hayes
```

Certains périphériques peuvent être utilisés à n'importe quelle vitesse, de sorte que le mot-clé Any peut être utilisé dans le champ Class. Si l'option Any est utilisée, la ligne correspond à n'importe quelle vitesse demandée dans le champ Speed du fichier Systems. Si ce champ porte la valeur Any et le champ Speed du fichier Systems également, la vitesse par défaut est de 2 400 bit/s.

Champ Dialer-Token-Pairs dans le fichier /etc/uucp/Devices

Le champ Dialer-Token-Pairs (DTP) contient le nom d'un dialer et le marqueur pour le transférer. Le champ DTP présente la syntaxe suivante :

dialer token [dialer token]

La partie *dialer* peut être le nom d'un modem, d'un port moniteur ou le mot-clé `Direct` ou `Uudirect` pour un périphérique avec lien direct. Il n'existe aucune limite au nombre de paires dialer-jeton. Si la partie *dialer* n'est pas présente, elle est tirée d'une entrée associée dans le fichier `Systems`. La partie *token* peut être fournie immédiatement après la partie dialer.

La dernière paire dialer-jeton peut ne pas être présente, selon le dialer associé. Dans la plupart des cas, la dernière paire comporte uniquement une partie *dialer*. La partie *token* est récupérée à partir du champ Phone de l'entrée du fichier `Systems` associé.

Une entrée valide dans la partie *dialer* partie peut être définie dans le fichier `Dialers` ou peut être l'un de plusieurs types de dialers. Ces types de dialers spéciaux sont compilés dans le logiciel et sont donc disponibles sans qu'aucune entrée ne soit présente dans le fichier `Dialers`. La liste ci-dessous présente les types de dialers spéciaux.

`TCP` Réseau TCP/IP

`TLI` Réseau Transport Level Interface (sans STREAMS)

`TLIS` Réseau Transport Level Interface (avec STREAMS)

Pour plus d'informations, reportez-vous à la section “Définitions de protocole dans le fichier /etc/uucp/Devices” à la page 192.

Structure du champ Dialer-Token-Pairs dans le fichier /etc/uucp/Devices

Le champ DTP peut être structuré de quatre manières différentes, selon le périphérique associé à l'entrée.

Voici la première manière de structurer le champ DTP :

Modem connecté directement : si un modem est connecté directement à un port de votre ordinateur, le champ DTP de l'entrée du fichier `Devices` associé ne dispose que d'une

seule paire. Cette paire porte normalement le nom du modem. Ce nom permet de mettre en correspondance l'entrée du fichier `Devices` avec une entrée du fichier `Dialers`. Par conséquent, le champ Dialer doit correspondre au premier champ d'une entrée du fichier `Dialers`.

EXEMPLE 12-7 Champ Dialers pour un modem connecté directement

```
Dialers   hayes =,-,  ""          \\dA\pTE1V1X1Q0S2=255S12=255\r\c
                                  \EATDT\T\r\c CONNECT
```

Notez que seule la partie dialer (`hayes`) est présente dans le champ DTP de l'entrée du fichier `Périphériques`. Cela signifie que le *jeton* à transmettre au dialer (dans cet exemple, le numéro de téléphone) est tiré du champ Phone d'une entrée du fichier `Systems`. (`\T` est implicite, comme décrit dans l'Exemple 12-9, “Champ Dialers UUCP pour les modems connectés au sélecteur de port”.)

Voici la seconde et la troisième manières de structurer le champ DTP :

- **Lien direct** : pour créer un lien direct vers un ordinateur particulier, le champ DTP de l'entrée associée doit contenir le mot-clé `Direct`. Cette condition s'applique aux deux types d'entrées de lien direct, `direct` et *System-Name*. Reportez-vous à la section “Champ Type du fichier /etc/uucp/Devices” à la page 187.
- **Ordinateurs sur le même sélecteur de port** : si un ordinateur avec lequel vous avez l'intention de communiquer se trouve sur le même commutateur de sélecteur de port que votre ordinateur, vous devez d'abord accéder au commutateur. Le commutateur établit ensuite la connexion à l'autre ordinateur. Ce type d'entrée n'a qu'une seule paire. La partie *dialer* permet de faire correspondre une entrée du fichier `Dialers`.

EXEMPLE 12-8 Champ Dialers UUCP pour les ordinateurs sur le même sélecteur de port

```
Dialers    develcon ,""   ""           \pr\ps\c est:\007 \E\D\e \007
```

Comme indiqué, la partie *jeton* n'est pas renseignée. Cette désignation indique que le jeton est tiré du fichier `Systems`. L'entrée du fichier `Systems` pour cet ordinateur contient le jeton dans le champ Phone, qui est normalement réservé au numéro de téléphone de l'ordinateur. Pour plus d'informations, reportez-vous à la section “Fichier /etc/uucp/Systems UUCP” à la page 179. Ce type de DTP contient un caractère d'échappement (`\D`), ce qui permet de s'assurer que le contenu du champ Phone n'est pas interprété comme une entrée valide dans le fichier `Dialcodes`.

Voici la quatrième manière de structurer le champ DTP :

Modems connectés au sélecteur de port : si un modem haut-débit est connecté à un port d'un sélecteur, votre ordinateur doit d'abord accéder au commutateur du sélecteur de port. Le commutateur établit la connexion au modem. Ce type d'entrée nécessite deux paires dialer-jeton. La partie *dialer* de chaque paire (cinquième et septième champs de l'entrée) permet de mettre en correspondance les entrées dans le fichier `Dialers`, comme suit.

EXEMPLE 12-9 Champ Dialers UUCP pour les modems connectés au sélecteur de port

```
develcon ""     ""    \pr\ps\c  est:\007    \E\D\e      \007
ventel   =&-%   t""   \r\p\r\c  $           <K\T%\r>\c  ONLINE!
```

Dans la première paire, `develcon` est le dialer et `vent` le jeton transmis au commutateur Develcon afin de lui indiquer quel périphérique, tel qu'un modem Ventel, connecter à votre ordinateur. Ce jeton est unique pour chaque sélecteur de port, chaque commutateur pouvant être défini différemment. Une fois le modem Ventel connecté, la seconde paire est accessible. Ventel est le dialer et le jeton est extrait du fichier `Systems`.

Deux caractères d'échappement peuvent s'afficher dans un champ DTP :

- `\T` : indique que le champ Phone (*jeton*) doit être traduit en utilisant le fichier `/etc/uucp/Dialcodes`. Ce caractère d'échappement est normalement placé dans le fichier `/etc/uucp/Dialers` fichier pour chaque script appelant associé à un modem (Hayes et U.S. Robotics par exemple). Par conséquent, aucune traduction n'a lieu avant l'accès au script appelant.
- `\D` – Indique que le champ Phone (*token*) ne doit pas être traduit à l'aide du fichier `/etc/uucp/Dialcodes`. Si aucun caractère d'échappement n'est spécifié à la fin d'une entrée `Devices`, l'option `\D` est appliquée (par défaut). Une option `\D` est également utilisée dans le fichier `/etc/uucp/Dialers` avec les entrées associées aux commutateurs réseau `develcon` et `micom`.

Définitions de protocole dans le fichier `/etc/uucp/Devices`

Vous pouvez définir le protocole à utiliser avec chaque périphérique dans`/etc/uucp/Devices`. Cette spécification est généralement inutile car vous pouvez utiliser la valeur par défaut ou définir le protocole à l'aide du système spécifique que vous appelez. Pour plus d'informations, reportez-vous à la section “Fichier /etc/uucp/Systems UUCP” à la page 179. Si vous spécifiez un protocole, utilisez la forme suivante :

Type`,`*Protocol* *[parameters]*

Par exemple, vous pouvez utiliser l'option `TCP,te` pour spécifier le protocole TCP/IP.

Le tableau suivant montre les protocoles disponibles pour le fichier `Devices`.

TABLEAU 12-2 Protocoles utilisés dans `/etc/uucp/Devices`

Protocole	Description
`t`	Ce protocole est couramment utilisé pour les transmissions des données sur TCP/IP et autres connexions fiables. `t` suppose des transmissions sans erreur.
`g`	Ce protocole est le protocole UUCP natif. `g` est lent, fiable et adapté pour la transmission sur des lignes téléphoniques perturbées.

Protocole	Description
e	Ce protocole suppose la transmission sur des canaux exempts d'erreur orientés message (par opposition aux canaux orientés flux d'octets), tels que TCP/IP.
f	Ce protocole est utilisé pour la transmission sur des connexions X.25. La valeur f s'appuie sur le contrôle du flux de données et est destinée à fonctionner sur des liens qui peuvent (presque) être garantis comme étant exempts d'erreurs, plus particulièrement les liens X.25/PAD. Une somme de contrôle est appliquée sur un fichier dans son intégralité uniquement. Si un transport échoue, le récepteur peut requérir la ou les retransmission(s).

Voici un exemple qui montre une désignation de protocole pour une entrée de périphérique :

```
TCP,te - - Any TCP -
```

Cet exemple indique que, pour le TCP du périphérique, vous devez essayer d'utiliser le protocole t. Si l'autre extrémité de la transmission refuse, utilisez le protocole e.

Ni e ni t ne convient pour l'utilisation sur un modem. Même si le modem garantit une transmission exempte d'erreur, les données peuvent toujours être perdues entre le modem et l'UC.

Fichier /etc/uucp/Dialers UUCP

Le /etc/uucp/Dialers fichier contient des instructions de numérotation pour les modems fréquemment utilisés. Il est probable que vous n'ayez pas besoin de modifier ou d'ajouter d'entrées à ce fichier, sauf si vous prévoyez d'utiliser un modem non standard ou si vous envisagez de personnaliser votre environnement UUCP. Néanmoins, vous devez connaître le contenu de ce fichier et comment il se rapporte aux fichiers Systems et Devices.

Le texte rapporte la conversation initiale qui doit se produire sur une ligne avant la ligne qu'elle ne soit mise à disposition pour le transfert de données. Cette conversation, connue comme un script de discussion, est généralement une séquence de chaînes ASCII expect-send. Un script de discussion est souvent utilisé pour composer un numéro de téléphone.

Comme indiqué dans les exemples de la section “Fichier /etc/uucp/Devices UUCP” à la page 186, le cinquième champ d'une entrée du fichier Devices est un index renvoyant au fichier Dialers ou un type de dialer spécial, tel que TCP, TLI ou TLIS. Le démon uucico tente de faire correspondre le cinquième champ du fichier Devices avec le premier champ de chaque entrée du fichier Dialers. En outre, tous les champs impairs du fichier Devices, à partir de la septième position, sont utilisés comme un index vers le fichier Dialers. Si la correspondance est établie, l'entrée du fichier Dialers est interprétée afin d'effectuer la conversation avec le dialer.

Les entrées du fichier Dialers suivent la syntaxe suivante :

```
dialer   substitutions   expect-send
```

L'exemple suivant montre l'entrée d'un modem U.S. Robotics V.32bis.

EXEMPLE 12-10 Entrée dans le fichier /etc/uucp/Dialers

```
usrv32bis-e    =,-,  ""    dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
                           \EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
```

`usrv32bis-e`

Entrée du champ Dialer. Le champ Dialer correspond au cinquième champ et aux champs impairs supplémentaires du fichier `Devices`.

`=,-, ""`

Entrée du champ Substitutions. Le champ Substitutions est une chaîne de translation. Le premier caractère de chaque paire est mappé avec le second caractère de la paire. Ce mappage est généralement utilisé pour traduire = et - au format requis par le dialer pour "attendre la tonalité" et "effectuer une pause".

`dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r`

Entrée dans le champ Expect-Send. Les champs Expect-Send sont des chaînes de caractères.

`\EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts`

Plus de détails du champ Expect-Send.

L'exemple ci-dessous présente des échantillons d'entrées du fichier `Dialers`, comme distribuées lorsque vous installez UUCP dans le cadre du programme d'installation Oracle Solaris.

EXEMPLE 12-11 Extraits du fichier /etc/uucp/Dialers

```
penril =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK

ventel =&-% "" \r\p\r\c $ <K\T%%\r>\c ONLINE!

vadic =K-K "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE

develcon "" "" \pr\ps\c est:\007

\E\D\e \n\007 micom "" "" \s\c NAME? \D\r\c GO

hayes =,-, "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT

#   Telebit TrailBlazer
tb1200 =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=2\r\c OK\r
\EATDT\T\r\c CONNECT\s1200
tb2400 =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=3\r\c OK\r
\EATDT\T\r\c CONNECT\s2400
```

```
tbfast =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=255\r\c OK\r
\EATDT\T\r\c CONNECT\sFAST

# USrobotics, Codes, and DSI modems

dsi-ec  =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts,crtsxoff

dsi-nec =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E0*F3*M1*S1\r\c OK\r \EATDT\T\r\c CONNECT
STTY=crtscts,crtsxoff

usrv32bis-ec =,-,  "" \dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r \EATDT\T\r\c
CONNECT\s14400/ARQ STTY=crtscts,crtsxoff

usrv32-nec =,-, "" \dA\pT&FE1V1X1Q0S2=255S12=255&A0&H1&M0&B0&W\r\c OK\r \EATDT\T\r\c
CONNECT STTY=crtscts,crtsxoff

codex-fast =,-, "" \dA\pT&C1&D2*MF0*AA1&R1&S1*DE15*FL3S2=255S7=40S10=40*TT5&W\r\c OK\r
\EATDT\T\r\c CONNECT\s38400 STTY=crtscts,crtsxoff

tb9600-ec =W-,  "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6\r\c OK\r
\EATDT\T\r\cCONNECT\s9600 STTY=crtscts,crtsxoff

tb9600-nec =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6S180=0\r\c OK\r \EATDT\T\r\c
CONNECT\s9600 STTY=crtscts,crtsxoff
```

Le tableau suivant répertorie les caractères d'échappement couramment utilisés dans les chaînes send du fichier `Dialers`.

TABLEAU 12-3 Caractères backslash pour le fichier `/etc/uucp/Dialers`

Caractère	Description
`\b`	Envoie ou attend un caractère de retour arrière.
`\c`	Aucune nouvelle ligne ni aucun retour chariot.
`\d`	Applique un délai d'environ 2 secondes.
`\D`	Numéro de téléphone ou jeton sans translation dans le fichier `Dialcodes`.
`\e`	Désactive la vérification d'écho.
`\E`	Active la vérification d'écho pour les périphériques lents.
`\K`	Insère un caractère de saut.
`\n`	Envoie une nouvelle ligne.
`\nnn`	Envoie un nombre octal. Des caractères d'échappement supplémentaires pouvant être utilisés sont répertoriés à la section “Fichier `/etc/uucp/Systems` UUCP” à la page 179.
`\N`	Envoie ou attend un caractère NUL (ASCII NUL).
`\p`	S'interrompt pendant environ 12 à 14 secondes.
`\r`	Renvoie.
`\s`	Envoie ou attend un caractère d'espace.
`\T`	Numéro de téléphone ou jeton avec translation dans le fichier `Dialcodes`.

Voici une entrée penril dans le fichier Dialers :

```
penril =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
```

Tout d'abord, le mécanisme de substitution pour l'argument de numéro de téléphone est établi afin que tout signe = soit remplacé par un W (attendre la tonalité) et tout signe - par un P (pause).

La procédure d'établissement de connexion donnée par le reste de la ligne fonctionne comme indiqué :

- "" : n'attend rien, ce qui signifie passer à l'étape suivante.
- \d : applique un délai d'attente de 2 secondes, puis envoie un retour chariot.
- > : attend un >.
- Q\c : envoie un caractère Q sans retour chariot.
- : : attend un :.
- \d- : applique un délai de 2 secondes, envoie un signe - et un retour chariot.
- > : attend un >.
- s\p9\c : envoie un signe s, effectue une pause, envoie un caractère 9 sans retour chariot.
-)-W\p\r\ds\p9\c-) : attend un signe) . Si) n'est pas reçu, traite la chaîne entre caractères - comme suit. Envoie un caractère W, effectue une pause, envoie un retour chariot, applique des délais, envoie un caractère s, effectue une pause, envoie un caractère 9 sans retour chariot, puis attend le caractère).
- y\c : envoie un caractère y sans retour chariot.
- : : attend un :.
- \E\TP : \E permet la vérification d'écho. A partir de ce point, chaque fois qu'un caractère est transmis, l'UUCP attend que le caractère soit reçu avant de poursuivre. Ensuite, UUCP envoie le numéro de téléphone. Le caractère \T indique de prendre le numéro de téléphone transmis sous la forme d'un argument. Le caractère \T applique la translation du fichier Dialcodes et la translation de la fonction du modem spécifiée par le champ 2 de cette entrée. Le caractère \T envoie alors un caractère P et un retour chariot.
- > : attend un >.
- 9\c : envoie un caractère 9 sans nouvelle ligne.
- OK : attend la chaîne OK.

Activation du contrôle de flux matériel dans le fichier /etc/uucp/Dialers

Vous pouvez également utiliser la chaîne de pseudo-envoi STTY=*valeur* pour définir les caractéristiques du modem. Par exemple, STTY=crtscts active le contrôle de flux matériel sortant. STTY=crtsxoff active le contrôle de flux matériel entrant. STTY=crtscts,crtsxoff active le contrôle de flux matériel à la fois entrant et sortant.

STTY accepte tous les modes stty. Reportez-vous aux pages de manuel stty(1) et termio(7I).

L'exemple suivant activerait le contrôle de flux matériel dans une entrée du fichier Dialers :

```
dsi =,–, "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts
```

Cette chaîne de pseudo-envoi peut également être utilisée dans les entrées du fichier Systems.

Définition de la parité dans le fichier /etc/uucp/Dialers

Dans certaines situations, vous devez réinitialiser la parité car le système que vous appelez vérifie la parité des ports et supprime la ligne si elle est incorrecte. La paire Expect-Send P_ZERO définit la parité à zéro :

```
foo =,-, "" P_ZERO "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r\EATDT\T\r\c CONNECT
```

Vous trouverez ci-dessous les paires de parité pouvant suivre la paire Expect-Send :

"" P_EVEN	Définit la parité sur pair, qui est la valeur par défaut
"" P_ODD	Définit la parité sur impair
"" P_ONE	Définit la parité sur un

Cette chaîne de pseudo-envoi peut également être utilisée dans les entrées du fichier Systems.

Autres fichiers de configuration UUCP de base

Vous pouvez utiliser les fichiers de cette section en plus des fichiers Systems, Périphériques et Dialers lorsque vous effectuez la configuration de base d'UUCP.

Fichier /etc/uucp/Dialcodes UUCP

Le fichier /etc/uucp/Dialcodes permet de définir les abréviations d'accès direct pouvant être utilisées dans le champ Phone du fichier /etc/uucp/Systems. Vous pouvez utiliser le fichier Dialcodes pour fournir des informations supplémentaires sur un numéro de téléphone de base utilisé par plusieurs systèmes sur le même site.

Chaque entrée applique la syntaxe suivante :

```
Abbreviation   Dial-Sequence
```

`Abbreviation` Ce champ fournit l'abréviation utilisée dans le champ Phone du fichier `Systems`.

`Dial-Sequence` Ce champ indique la séquence de numérotation transmise au dialer lors de l'accès à cette entrée particulière du fichier `Systems`.

Comparez les champs dans les deux fichiers. Les champs suivants sont ceux du fichier `Dialcodes`.

`Abbreviation` `Dial-Sequence`

Les champs suivants sont ceux du fichier `Systems`.

`System-Name  Time  Type  Speed` **`Phone`** `Chat Script`

Le tableau ci-après contient un exemple de contenu pour les champs d'un `Dialcodes`.

TABLEAU 12-4 Entrées dans le fichier `Dialcodes`

Abréviation	Séquence de numérotation
`NY`	`1=212`
`jt`	`9+847`

Dans la première ligne, NY est l'abréviation qui s'affichera dans le champ Phone du fichier `Systems`. Le fichier `System` peut par exemple contenir l'entrée suivante :

```
NY5551212
```

Lorsque le démon `uucico` lit `NY` dans le fichier `Systems`, `uucico` recherche `NY` dans le fichier `Dialcodes` et obtient la séquence de numérotation `1=212` . `1=212` est la séquence de numérotation requise pour tout appel téléphonique à New York. Cette séquence inclut le nombre `1`, un signe égale (`=`) qui indique d'effectuer une pause et d'attendre une tonalité secondaire, et l'indicatif de zone `212`. `uucico` envoie ces informations au dialer, puis revient au fichier `Systems` pour le reste du numéro de téléphone, `5551212`.

L'entrée `jt 9=847-` fonctionnerait avec un champ Phone tel que `jt7867` dans le fichier `Systems`. Quand `uucico` lit l'entrée qui contient `jt7867` dans le fichier `Systems`, `uucico` envoie la séquence `9=847-7867` au dialer, si le jeton dans la paire dialer-jeton est `\T`.

Fichier `/etc/uucp/Sysfiles` UUCP

Le fichier `/etc/uucp/Sysfiles` vous permet d'affecter différents fichiers à utiliser par `uucp` et `cu` comme les fichiers `Systems`, `Devices` et `Dialers`. Pour plus d'informations concernant `cu`,

reportez-vous à la page du manuel cu(1C). Vous pouvez utiliser le fichier Sysfiles pour l'un des éléments suivants :

- Différents fichiers Systems de façon à ce que les demandes de services de connexion puissent être effectuées à d'autres adresses que les services uucp.
- Différents fichiers Dialers de façon à ce que vous puissiez affecter différents protocoles d'établissement de connexion aux commandes cu et uucp.
- Fichiers Systems, Dialers et Devices multiples. Le fichier Systems en particulier peut devenir important, de sorte qu'il s'avère plus pratique de le diviser en plusieurs fichiers de plus petite taille.

La syntaxe du fichier Sysfiles est :

```
service=w systems=x:x dialers=y:y devices=z:z
```

w	Représente uucico, cu ou les deux commandes séparées par deux-points
x	Représente un ou plusieurs fichiers à utiliser comme fichier Systems, les noms de fichiers étant séparés par une virgule et lus dans l'ordre dans lequel ils se présentent
y	Représente un ou plusieurs fichiers à utiliser comme fichier Périphériques
z	Représente un ou plusieurs fichiers à utiliser comme fichier Devices

On suppose que le nom de chaque fichier est relatif au répertoire /etc/uucp, sauf si un chemin d'accès complet est fourni.

L'exemple suivant, /etc/uucp/Sysfiles, définit un fichier Systems local (Local_Systems) en plus du fichier /etc/uucp/Systems standard :

```
service=uucico:cu systems=Systems :Local_Systems
```

Lorsque cette entrée se trouve dans le fichier /etc/uucp/Sysfiles, les commandes uucico et cu vérifient d'abord dans le fichier /etc/uucp/Systems standard. Si le système appelé ne possède pas d'entrée dans ce fichier ou si les entrées dans le fichier échouent, les deux commandes vérifient le fichier /etc/uucp/Local_Systems.

Comme indiqué dans l'entrée précédente, les commandes cu et uucico partagent les fichiers Dialers et Périphériques.

Quand différents fichiers système sont définis pour les services uucico et cu, votre ordinateur enregistre deux listes différentes de systèmes. Vous pouvez imprimer la liste uucico en utilisant la commande uuname ou la liste cu en utilisant la commande uuname-C. Voici un autre exemple de fichier, qui indique que d'autres fichiers sont consultés en premier, puis les fichiers par défaut sont consultés si nécessaire :

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
devices=Devices.cico:Devices
  service=cu systems=Systems.cu:Systems \
dialers=Dialers.cu:Dialers \
  devices=Devices.cu:Devices
```

Fichier /etc/uucp/Sysname UUCP

Chaque ordinateur utilisaton UUCP doit avoir un identifiant, souvant appelé le *nom de noeud*. Le nom du noeud apparaît dans le fichier /etc/uucp/Systems de l'ordinateur distant, de même que le script de discussion et d'autres informations d'identification. Normalement, UUCP utilise le même nom de noeud que celui renvoyé par la commande uname -n, également utilisé par le protocole TCP/IP.

Vous pouvez spécifier un nom de noeud UUCP indépendant du nom d'hôte TCP/IP en créant le fichier /etc/uucp/Sysname. Le fichier possède une entrée d'une ligne qui contient le nom du noeud UUCP pour votre système.

Fichier /etc/uucp/Permissions UUCP

Le fichier /etc/uucp/Permissions spécifie les autorisations des ordinateurs distants en matière de connexion, d'accès aux fichiers et d'exécution des commandes. Certaines options restreignent la capacité de l'ordinateur distant à envoyer des demandes aux fichiers et sa capacité à recevoir les fichiers mis en file d'attente par l'ordinateur local. Une autre option disponible permet de spécifier les commandes qu'un ordinateur distant peut exécuter sur l'ordinateur local.

Structuration des entrées UUCP

Chaque entrée est une ligne logique, avec des lignes physiques qui se terminent avec une barre oblique (\) pour indiquer la continuation. Les entrées sont composés d'options délimitées par une espace. Chaque option est une paire nom-valeur dans le format suivant :

name=value

values peut consister en des listes séparés par deux points. Aucune espace n'est autorisée au sein d'une affectation d'option.

Les lignes de commentaires commencent par le signe dièse (#) et occupent l'intégralité de la ligne jusqu'à un caractère de nouvelle ligne. Les lignes vides sont ignorées, même au sein d'entrées à plusieurs lignes.

Les types d'entrées du fichier Permissions sont les suivants :

- LOGNAME – Spécifie les autorisations qui entrent en vigueur quand un ordinateur distant se connecte à votre ordinateur (l'appelle).

Remarque - Lorsqu'un ordinateur distant vous appelle, son identité est douteuse sauf si l'ordinateur distant possède un identifiant de connexion unique et un mot de passe vérifiable.

- MACHINE – Spécifie les autorisations qui entrent en vigueur quand votre ordinateur se connecte à un ordinateur distant (l'appelle).

Les entrées LOGNAME contiennent une option LOGNAME. Les entrées MACHINE contiennent une option MACHINE. Une entrée peut contenir les deux options.

Eléments à prendre en compte relatifs au protocole UUCP

Lors de l'utilisation du fichier Permissions pour limiter les autorisations accordées à des ordinateurs distants, vous devez prendre en compte les éléments suivants :

- Tous les ID de connexion utilisés par les ordinateurs distants pour se connecter pour les communications UUCP doivent apparaître dans une seule et unique entrée LOGNAME.
- Tout site appelé avec un nom qui ne figure pas dans une entrée MACHINE a les autorisations ou restrictions par défaut suivantes :
  - Les demandes d'envoi et de réception locales sont exécutées.
  - L'ordinateur distant peut envoyer des fichiers au répertoire /var/spool/uucppublic de votre ordinateur.
  - Les commandes envoyées par l'ordinateur distant pour exécution sur votre ordinateur doivent faire partie des commandes par défaut, normalement rmail.

Option REQUEST UUCP

Quand un ordinateur distant appelle votre ordinateur et avec la demande de recevoir un fichier, la demande peut être acceptée ou refusée. L'option REQUEST indique si l'ordinateur distant peut envoyer une demande afin de configurer les transferts de fichiers à partir de votre ordinateur. La chaîne REQUEST=yes indique que l'ordinateur distant peut demander à transférer des fichiers à partir de votre ordinateur. La chaîne REQUEST=no indique que l'ordinateur distant ne peut pas demander à recevoir de fichiers depuis votre ordinateur. REQUEST=no, la valeur par défaut, est utilisée si l'option REQUEST n'est pas spécifiée. L'option REQUEST peut apparaître dans une entrée

LOGNAME, de sorte que l'ordinateur distant vous appelle, ou dans l'entrée MACHINE, de sorte que vous pouvez appeler l'ordinateur distant.

Option SENDFILES UUCP

Quand un ordinateur distant appelle votre ordinateur pour terminer ses opérations, l'ordinateur distant peut tenter d'extraire le travail que votre ordinateur a mis en attente. L'option SENDFILES indique si votre ordinateur peut envoyer le travail mis en file d'attente pour l'ordinateur distant.

La chaîneSENDFILES=yes spécifie que votre ordinateur peut envoyer le travail mis en attente pour l'ordinateur distant s'il est connecté avec un des noms figurant dans l'option LOGNAME. Cette chaîne est *obligatoire* si vous avez saisi Never dans le champ Time du fichier /etc/uucp/Systems. Cette désignation configure votre machine locale en mode passif, mais ne l'autorise pas à lancer un appel vers cet ordinateur distant. Pour plus d'informations, reportez-vous à la section “Fichier /etc/uucp/Systems UUCP” à la page 179.

La chaîne SENDFILES=call indique que les fichiers en attente sur votre ordinateur sont envoyés uniquement lorsque votre ordinateur appelle l'ordinateur distant. La valeur call est la valeur par défaut pour l'option SENDFILES. Cette option est significative uniquement dans les entrées LOGNAME, car les entrées MACHINE s'appliquent lorsque des appels sont envoyés vers des ordinateurs distants. Si l'option est utilisée avec une entrée MACHINE, elle est ignorée.

Option MYNAME UUCP

Cette option vous permet de désigner un nom de noeud unique UUCP pour votre ordinateur, en plus du nom de l'hôte TCP/IP suite à la commande hostname. Par exemple, si vous avez involontairement donné à votre hôte le même nom que celui d'un autre système, vous pouvez définir l'option MYNAME du fichier Permissions. Supposons que vous souhaitiez que votre société soit connue sous le nom widget. Si tous les modems sont connectés à une machine avec le nom d'hôte gadget , vous pouvez avoir une entrée dans le fichier Permissions de gadgettelle que la suivante

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
  devices=Devices.cico:Devices
service=cu systems=Systems.cu:Systems \
  dialers=Dialers.cu:Dialers \
  devices=Devices.cu:Devices
```

A présent, le système world peut se connecter à l'ordinateur gadget de la même manière que si il se connectait à widget. Afin que la machine world vous connaisse également par l'alias widget lorsque vous appelez, vous pouvez avoir une entrée similaire à la suivante :

```
MACHINE=world MYNAME=widget
```

Vous pouvez également utiliser l'option MYNAME à des fins de test, étant donné que cette option permet à votre ordinateur de s'appeler lui-même. Toutefois, étant donné que cette option pourrait être utilisée pour masquer l'identité réelle d'un ordinateur, vous devez utiliser l'option VALIDATE, tel que décrit à la section “Option VALIDATE UUCP” à la page 206.

Options READ et WRITE UUCP

Ces options spécifient diverses partie du système de chichiers que uucico peut utiliser pour écritude ou lecture. Vous pouvez désigner les options READ et WRITE avec une entrée MACHINE ou LOGNAME.

La valeur par défaut des options READ et WRITE est le répertoire uucppublic, comme indiqué dans les chaînes suivantes :

```
READ=/var/spool/uucppublic WRITE=/var/spool/uucppublic
```

Les chaînes READ=/ et WRITE=/ indiquent l'autorisation d'accéder à tous les fichiers accessibles par un utilisateur local disposant d'autorisations Other.

La valeur de ces entrées est une liste séparée par deux-points de noms de chemin. L'option READ permet de demander des fichiers et l'option WRITE de déposer des fichiers. L'une des valeurs doit être le préfixe du nom du chemin d'accès complet d'un fichier entrant ou sortant. Pour accorder l'autorisation de déposer des fichiers dans /usr/news, ainsi que dans le répertoire public, utilisez les valeurs suivantes avec l'option WRITE :

```
WRITE=/var/spool/uucppublic:/usr/news
```

Si les options READ et WRITE sont utilisées, tous les noms de chemin doivent être spécifiés car ils ne sont pas ajoutés à la liste par défaut. Par exemple, si le nom de chemin /usr/news était le seul chemin spécifié dans une option WRITE, l'autorisation de déposer des fichiers dans le répertoire public serait refusée.

Soyez prudent avec les répertoires que vous rendez accessibles aux systèmes ditants pour lecture et écriture. Par exemple, le répertoire /etc contient de nombreux fichiers système critiques. Les utilisateurs distants ne doivent pas être autorisés à déposer des fichiers dans ce répertoire.

Options NOREAD et NOWRITE UUCP

Les options NOREAD et NOWRITE spécifient des exceptions des options ou valeurs par défaut READ et WRITE. L'entrée suivante autorise la lecture de n'importe quel fichier, à l'exception des fichiers

présents dans le répertoire /etc (et ses sous-répertoires). N'oubliez pas que ces options sont des préfixes.

```
READ=/ NOREAD=/etc WRITE=/var/spool/uucppublic
```

Cette entrée permet d'écrire directement dans le répertoire par défaut /var/spool/uucppublic. L'option NOWRITE fonctionne de la même manière que l'option NOREAD. Vous pouvez utiliser les options NOREAD et NOWRITE dans les entrées LOGNAME et MACHINE.

Option CALLBACK UUCP

Vous pouvez utiliser l'option CALLBACK des entrées LOGNAME pour spécifier qu'aucune transaction n'aura lieu jusqu'à ce que le système appelant est rappelé. Les raisons de configurer l'option CALLBACK sont les suivantes :

- Sécurité : si vous rappelez un ordinateur, vous pouvez être sûr qu'il s'agit du bon ordinateur.
- Comptabilité : si vous effectuez de longues transmissions de données, vous pouvez choisir l'ordinateur facturé pour l'appel le plus long.

La chaîne CALLBACK=yes indique que votre ordinateur doit rappeler l'ordinateur distant avant que le transfert de fichiers ne se produise.

La valeur par défaut pour l'option CALLBACK est CALLBACK=no. Si vous définissez l'option CALLBACK sur yes, les autorisations qui ont une incidence sur le reste de la conversation doivent être spécifiées dans l'entrée MACHINE correspondant à l'appelant. N'indiquez pas ces autorisations dans l'entrée LOGNAME ou dans l'entrée LOGNAME que l'ordinateur distant peut avoir défini pour votre hôte.

Remarque - Si deux sites ont configuré l'option CALLBACK mutuellement, une conversation ne démarre jamais.

Option COMMANDS UUCP

Attention - L'option COMMANDS peut représenter un risque pour votre système. Utilisez-la avec une extrême précaution.

Vous pouvez utiliser l'option COMMANDS des entrées MACHINE pour spécifier les commandes qu'un ordinateur distant peut exécuter sur votre ordinateur. Le programme uux génère des demandes d'exécution à distance et établit des files d'attente des demandes à transférer vers l'ordinateur distant. Les commandes et fichiers sont envoyés à l'ordinateur cible pour une exécution à

distance, ce qui est une exception à la règle selon laquelle les entrées MACHINE s'appliquent uniquement lorsque votre système appelle.

Notez que l'option COMMANDS n'est pas utilisée dans une entrée LOGNAME. L'option COMMANDS dans les entrées MACHINE définit les autorisations des commandes, que vous appeliez le système distant ou vice-versa.

La chaîne COMMANDS=rmail spécifie les commandes par défaut qu'un ordinateur distant peut exécuter sur votre ordinateur. Si une chaîne de commande est utilisée dans une entrée MACHINE, les commandes par défaut sont remplacées. Par exemple, l'entrée suivante remplace l'option COMMAND par défaut, de sorte que les ordinateurs nommés owl, raven, hawk et dove peuvent désormais exécuter les commandes rmail, rnews et lp sur votre ordinateur.

```
MACHINE=owl:raven:hawk:dove COMMANDS=rmail:rnews:lp
```

En plus des noms, tels que ceux de l'exemple précédent, vous pouvez spécifier des noms du chemin d'accès complet de commandes. Par exemple, l'entrée suivante indique que la commande rmail utilise le chemin de recherche par défaut.

```
COMMANDS=rmail:/usr/local/rnews:/usr/local/lp
```

Le chemin de recherche par défaut pour UUCP est /bin et /usr/bin. Lorsque l'ordinateur distant spécifie rnews ou /usr/local/rnews pour la commande à exécuter, la commande /usr/local/rnews est exécutée indépendamment de ce chemin d'accès par défaut. De même, /usr/local/lp est la commande lp qui est exécutée.

L'inclusion de la valeur ALL dans la liste signifie que toute commande émise par les ordinateurs distants spécifiés dans l'entrée est exécutée. Si vous utilisez cette valeur, vous donnez aux ordinateurs distants un accès complet à votre ordinateur.

Attention - Cette valeur autorise davantage d'accès que celui qu'ont les utilisateurs standard. N'utilisez cette valeur que lorsque les deux ordinateurs se trouvent sur le même site, sont étroitement liés et que les utilisateurs sont de confiance.

Voici la chaîne avec la valeur ALL ajoutée :

```
COMMANDS=/usr/local/rnews:ALL:/usr/local/lp
```

Cette chaîne illustre deux points :

- La valeur ALL peut figurer n'importe où dans la chaîne.
- Les noms de chemin d'accès spécifiés pour rnews et lp sont utilisés (au lieu du nom par défaut) si la commande demandée ne contient pas les noms de chemin d'accès complets pour rnews ou lp.

Vous devez toujours utiliser l'option VALIDATE option quand vous spécifiez des commandes potentiellement dangereuses, comme cat et uucp avec l'option COMMANDS. Toute commande qui

lit ou écrit des fichiers présente un danger potentiel pour la sécurité locale lorsque la commande est exécutée par le démon d'exécution à distance UUCP (uuxqt).

Option VALIDATE UUCP

Utilisez toujours l'option VALIDATE en association avec l'option COMMANDS quand vous spécifiez des commandes potentiellement dangereuses pour la sécurité de votre ordinateur. L'option VALIDATE est simplement un niveau de sécurité supplémentaire ajouté à l'option COMMANDS, bien qu'elle représente un moyen plus sécurisé d'ouvrir l'accès aux commandes que l'option ALL.

L'option VALIDATE fournit un certain degré de vérification de l'identité de l'appelant en effectuant un contrôle croisé du nom d'hôte d'un ordinateur appelant par rapport au nom de connexion qu'il utilise. La chaîne suivante garantit que si un ordinateur autre que widget ou gadget tente de se connecter en tant que Uwidget, la connexion sera refusée.

```
LOGNAME=Uwidget VALIDATE=widget:gadget
```

L'option VALIDATE requiert que les ordinateurs disposant de privilèges aient un identifiant de connexion unique et un mot de passe pour les transactions UUCP. L'un des aspects importants de cette validation est que l'identifiant de connexion et le mot de passe associés à cette entrée soient protégés. Si un intrus obtient ces informations, cette option VALIDATE particulière ne peut plus être considérée comme sécurisée.

Réfléchissez bien aux ordinateurs distants auxquels vous accordez des identifiants et des mots de passe disposant de privilèges pour les transactions UUCP. L'attribution d'un identifiant de connexion et d'un mot de passe spéciaux à un ordinateur distant avec la possibilité d'accéder aux fichiers et d'exécuter des commandes à distance revient à donner à une personne sur cet ordinateur un identifiant de connexion et un mot de passe normaux sur votre ordinateur. Par conséquent, si vous ne pouvez pas faire confiance à quelqu'un sur l'ordinateur distant, vous ne devez pas fournir d'identifiant de connexion disposant de privilèges et de mot de passe à cet ordinateur.

L'entrée LOGNAME suivante spécifie que si l'un des ordinateurs distants qui prétend être eagle, owl ou hawk se connecte sur votre ordinateur, il doit avoir utilisé l'identifiant de connexion uucpfriend :

```
LOGNAME=uucpfriend VALIDATE=eagle:owl:hawk
```

Si un intrus obtient l'identifiant et le mot de passe uucpfriend, l'usurpation d'identité est facile.

Quel est le rapport de cette entrée avec l'option COMMANDS, qui apparaît uniquement dans les entrées MACHINE ? Cette entrée lie l'entrée MACHINE (et l'option COMMANDS) à une entrée LOGNAME associée à un identifiant de connexion disposant de privilèges. Ce lien est nécessaire car le démon d'exécution n'est pas exécuté pendant que l'ordinateur distant est connecté. En

fait, le lien est un processus asynchrone qui ne sait pas quel ordinateur a envoyé la demande d'exécution. Par conséquent, la vraie question est celle-ci : comment votre ordinateur connaît-il la provenance des fichiers d'exécution ?

Chaque ordinateur distant dispose de son propre répertoire spool sur votre machine locale. Ces répertoires spool disposent d'une autorisation d'écriture qui est uniquement accordée aux programmes UUCP. Les fichiers d'exécution issus de l'ordinateur distant sont placés dans son répertoire spool après avoir été transférés sur votre ordinateur. Lorsque le démon `uuxqt` s'exécute, il peut utiliser le nom du répertoire spool pour rechercher l'entrée `MACHINE` dans le `Permissions` et obtenir la liste `COMMANDS`. Ou, si le nom de l'ordinateur n'apparaît pas dans le fichier `Permissions`, la liste par défaut est utilisée.

Cet exemple montre la relation entre les entrées `MACHINE` et `LOGNAME` :

```
MACHINE=eagle:owl:hawk REQUEST=yes \
COMMANDS=rmail:/usr/local/rnews \
READ=/ WRITE=/
LOGNAME=uucpz VALIDATE=eagle:owl:hawk \
REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

La valeur dans l'option `COMMANDS` signifie que les utilisateurs distants peuvent exécuter les commandes `rmail` et `/usr/local/rnews` .

Dans la première entrée, vous devez vous baser sur l'hypothèse que si vous souhaitez appeler un des ordinateurs listés, vous appelez en réalité `eagle`, `owl` ou `hawk`. Par conséquent, tous les fichiers placés dans l'un des répertoires spool `eagle`, `owl` ou `hawk` l'est par l'un de ces ordinateurs. Si un ordinateur distant se connecte et dit qu'il s'agit de l'un de ces trois ordinateurs, ses fichiers d'exécution sont également placés dans le répertoire spool disposant de privilèges. Par conséquent, vous devez confirmer que l'ordinateur possède l'identifiant de connexion disposant de privilège `uucpz`.

Entrée `MACHINE` UUCP pour l'option `OTHER`

Vous pourriez spécifier des valeurs d'option différentes pour les ordinateurs distants non mentionnés dans des entrées de `MACHINE` spécifiques. Cela peut s'avérer nécessaire lorsque de nombreux ordinateurs appellent votre hôte et que l'ensemble de commandes change de temps en temps. Le nom `OTHER` pour le nom de l'ordinateur est utilisée pour cette entrée comme indiqué dans cet exemple :

```
MACHINE=OTHER \
COMMANDS=rmail:rnews:/usr/local/Photo:/usr/local/xp
```

Toutes les autres options disponibles pour l'entrée `MACHINE` peuvent également être définies pour les ordinateurs qui ne sont pas mentionnées dans d'autres entrées `MACHINE`.

Combinaison des entrées MACHINE et LOGNAME pour UUCP

Vous pouvez combiner les entrées MACHINE et LOGNAME en une seule entrée quand elles ont des options communes. Par exemple, les deux ensembles d'entrées qui suivent partagent les mêmes options REQUEST, READ et WRITE :

```
MACHINE=eagle:owl:hawk REQUEST=yes \
READ=/ WRITE=/
```

et

```
LOGNAME=uupz REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

Vous pouvez fusionner ces entrées, comme indiqué ci-dessous :

```
MACHINE=eagle:owl:hawk REQUEST=yes \
logname=uucpz SENDFILES-yes \
READ=/ WRITE=/
```

La combinaison des entrées MACHINE et LOGNAME facilite la gestion et améliore l'efficacité du fichier Permissions.

Transfert UUCP

Lors de l'envoi de fichiers à travers une série d'ordinateurs, les ordinateurs intermédiaires doivent avoir la commande uucp parmi les options de COMMANDES. Si vous saisissez la commande suivante, l'opération de transfert ne fonctionnera que si l'ordinateur willow autorise l'ordinateur oak à exécuter le programme uucp.

```
% uucp sample.txt oak\!willow\!pine\!/usr/spool/uucppublic
```

L'ordinateur oak doit également autoriser votre ordinateur à exécuter le programme uucp. L'ordinateur pine, en tant que dernier ordinateur désigné, n'a pas à autoriser la commande uucp car l'ordinateur n'effectue aucune opération de transfert. Les ordinateurs ne sont généralement pas configurés de cette manière.

Fichier /etc/uucp/Poll UUCP

Le fichier /etc/uucp/Poll contient les informations pour le sondage des ordinateurs distants. Chaque entrée du fichier Poll contient le nom d'un ordinateur distant à appeler, suivi d'un caractère de tabulation ou une espace, puis des heures auxquelles l'ordinateur doit être appelé. Le format des entrées dans le fichier Poll est le suivant :

sys-name hour ...

Par exemple, l'entrée **eagle 0 4 8 12 16 20** définit l'interrogation de l'ordinateur eagle toutes les quatre heures.

Le script uudemon.poll traite le fichier Poll mais n'effectue pas vraiment le sondage. Le script configure simplement un fichier de travail d'interrogation (toujours nommé C.*file*) dans le répertoire spool. Le script uudemon.poll lance l'ordonnanceur, et celui-ci examine tous les fichiers de travail du répertoire spool.

Fichier /etc/uucp/Config UUCP

Le fichier /etc/uucp/Config vous permet d'ignorer certains paramètres manuellement. Chaque entrée du fichier Config adopte le format suivant :

paramètre=valeur

Reportez-vous au fichier Config fourni avec votre système pour une liste complète des noms de paramètres configurables.

L'entrée Config suivante définit l'ordre du protocole par défaut sur Gge et modifie la valeur par défaut du protocole G à 7 fenêtres et paquets de 512 octets.

```
Protocol=G(7,512)ge
```

Fichier /etc/uucp/Grades UUCP

Le fichier /etc/uucp/Grades contient les définitions pour les niveaux de travail utilisables pour envoyer des tâches en attente à un ordinateur distant. Ce fichier contient également les autorisations correspondant à chaque niveau de travail. Chaque entrée de ce fichier représente une définition d'un niveau de travail défini par l'administrateur qui permet aux utilisateurs de mettre des travaux en attente.

Chaque entrée du fichier Grades adopte le format suivant :

User-job-grade System-job-grade Job-size Permit-type ID-list

Chaque entrée contient des champs séparés par une espace. Le dernier champ de l'entrée est composé de sous-champs également séparés par des espaces. Si une entrée occupe plus d'une ligne physique, vous pouvez utiliser un backslash pour continuer l'entrée sur la ligne suivante. Les lignes de commentaires commencent par le signe dièse (#) et occupent l'intégralité de la ligne. Les lignes vides sont toujours ignorées.

Champ User-job-grade UUCP

Ce champ contient un nom user-job-grade défini par l'administrateur de 64 caractères maximum.

Champ System-job-grade UUCP

Ce champ contient un niveau de travail à un seul caractère avec lequel *User-job-grade* est mis en correspondance. La liste des caractères valides est A à Z, a à z, A ayant la priorité la plus élevée et z la plus basse.

Relations entre les niveaux de travail utilisateur et système

Le niveau de travail de l'utilisateur peut être lié à plusieurs niveaux de travail de la tâche. Notez que les occurrences d'un niveau de travail utilisateur sont recherchée de manière séquentielle dans le fichier `Grades`. Par conséquent, les occurrences multiples d'un niveau de travail système doivent être répertoriées conformément aux restrictions en termes de taille maximale d'un travail.

Bien qu'aucun nombre maximal n'existe pour les niveaux de travail utilisateur, le nombre maximal de niveaux de travail système autorisé est de 52. La raison en est que plusieurs *User-job-grade* peuvent être mappés à un *System-job-grade*, mais chaque *User-job-grade* doit figurer sur une ligne distincte dans le fichier. Voici un exemple concret :

```
mail N Any User Any netnews N Any User Any
```

Si cette configuration se trouve dans un fichier `Grades`, ces deux champs *User-job-grade* partagent le même niveau *System-job-grade* . Les autorisations pour un *Job-grade* étant associées à un *User-job-grade* et non un *System-job-grade*, deux *User-job-grade* peuvent partager le même *System-job-grade* et avoir deux ensembles d'autorisations différents.

Niveau par défaut

Vous pouvez définir un *User-job-grade* lié par défaut à un niveau de travail système. Vous devez utiliser le mot-clé par défaut en tant que niveau de travail utilisateur dans le champ *User-job-grade* du fichier `Grades` et le niveau de travail système auquel il est lié. Les champs Restrictions et ID devraient être définis sur `Any` de sorte que tous les utilisateurs et les travaux de toutes tailles puissent être mis en attente à ce niveau. Voici un exemple concret :

```
default a Any User Any
```

Si vous ne définissez pas le niveau de travail de la tâche utilisateur par défaut, le niveau de travail incorporé par défau, `Z`, est utilisé. La valeur par défaut du champ Restriction étant `Any`, les occurrences multiples du niveau par défaut ne sont pas vérifiées.

Champ Job-size UUCP

Ce champ spécife la taille maximale de la tâche que vous pouvez mettre dans la file d'attente. La valeur *Job-size* est mesurée en octets et peut être une liste des options décrites dans la liste suivante.

nnnn	Nombre entier qui spécifie la taille maximale d'un travail pour ce niveau de travail
*n*K	Nombre décimal qui représente le nombre de kilo-octets (K est l'abréviation de kilo-octets)
*n*M	Nombre décimal qui représente le nombre de méga-octets (M est l'abréviation de méga-octets)
Tous	Mot-clé qui indique qu'aucune la taille maximale de travail ne s'applique

Voici quelques exemples :

- 5000 représente 5000 octets
- 10K représente 10 Ko
- 2M représente 2Mo

Champ Permit-type UUCP

Ce champ contient un mot clé dénotant comment interpréter la liste d'ID. Le tableau suivant répertorie les mots-clés et leur signification.

TABLEAU 12-5 Champ Permit-type

Mot clé	Contenu de la liste d'identifiants
User	Identifiants de connexion des utilisateurs autorisés à utiliser ce niveau de travail
Non-user	Identifiants de connexion des utilisateurs qui ne sont pas autorisés à utiliser ce niveau de travail
Group	Noms des groupes dont les membres sont autorisés à utiliser ce groupe
Non-group	Noms des groupes dont les membres ne sont pas autorisés à utiliser ce niveau de travail

Champ ID-list UUCP

Ce champ contient une liste de noms d'identiants de connexion ou noms de groupe autorisés ou refusés pour mettre cette tâche dans la file d'attente de ce niveau de travail. Les noms de la liste sont séparés par une espace et elle se termine par un caractère de saut de ligne. Le mot-clé Any

est utilisé pour indiquer que tout le monde est autorisé à mettre des travaux en attente pour ce niveau de travail.

Autres fichiers de configuration UUCP

Cette section décrit trois fichiers plus rarement modifiés qui ont un impact sur l'utilisation des équipements UUCP.

Fichier `/etc/uucp/Devconfig` UUCP

Le fichier `/etc/uucp/Devconfig` pemet de configurer des périphériques par service, comme `uucp` ou `cu`. Les entrées `Devconfig` définissent les modules STREAMS utilisés pour un périphérique donné. Ces entrées ont le format suivant :

`service=`*x* `périphérique=`*y* `push=`*z*[:*z*...]

x peut adopter la valeur `cu`, `uucico` ou les deux services séparés par deux-points. *y* est le nom d'un réseau et doit correspondre à une entrée dans le fichier `Périphériques`. *z* est remplacé par les noms des modules STREAMS dans l'ordre dans lequel ils doivent être insérés dans le flux de données. Différents modules et périphériques peuvent être définis pour les services `cu` et `uucp`.

Les entrées suivantes s'appliquent à un réseau STARLAN et seraient plus couramment utilisées dans le fichier :

```
service=cu       device=STARLAN     push=ntty:tirdwr
service=uucico   device=STARLAN     push=ntty:tirdwr
```

Cet exemple insère d'abord `ntty`, puis `tirdwr`.

Fichier `/etc/uucp/Limits` UUCP

Le fichier `/etc/uucp/Limits` contrôle le nombre maximum de `uucicos`, `uuxqt` et `uusched` exécutés simultanément dans le réseau `uucp`. Dans la plupart des cas, les valeurs par défaut sont acceptables et aucune modification n'est nécessaire. Si vous souhaitez toute de même les modifier, utilisez un éditeur de texte.

Le format du fichier `Limits` est :

`service=`*x* `max=`*y*:

x peut être `uucico`, `uuxqt` ou `uusched`, et *y* est la limite autorisée pour ce service. Les champs peuvent se trouver dans n'importe quel ordre et en minuscules.

Les entrées suivantes doivent généralement être utilisées dans le fichier `Limits` :

```
service=uucico max=5
service=uuxqt max=5
service=uusched max=2
```

L'exemple permet l'exécution simultanée de cinq commandes `uucico`, cinq commandes `uuxqt` et deux commandes `uusched` sur votre ordinateur.

Fichier `remote.unknown` UUCP

L'autre fichier qui a une incidence sur l'utilisation des fonctions de communication est le fichier `remote.unknown`. Ce fichier est un programme binaire qui s'exécute lorsqu'aucun ordinateur n'est trouvé lorsque l'un des fichiers `Systems` lance une conversation. Ce programme enregistre la tentative de conversation et abandonne la connexion.

Attention - Si vous changez les autorisations du fichier `remote.unkown` de sorte qu'il ne puisse pas s'exécuter, votre système accepte les connexions à partir de n'importe quel système.

Ce programme s'exécute lorsqu'un ordinateur qui ne se trouve pas dans l'un des fichiers `Systems` démarre une conversation. Le programme enregistre la tentative de conversation, mais ne parvient pas à établir une connexion. Si vous modifiez les autorisations de ce fichier de sorte qu'il ne puisse pas s'exécuter (`chmod 000 remote.unknown`), votre système accepte toutes les demandes de conversation. Cette modification n'est pas sans impact. Vous devez avoir de bonnes raisons pour procéder à cette modification.

Fichiers d'administration UUCP

Les fichiers d'administration UUCP sont décrits ci-après. Ces fichiers sont créés dans les répertoires spool pour verrouiller les périphériques, maintenir les données temporaires ou conserver les informations relatives aux transferts ou exécutions à distance.

- *Fichier de données temporaire* (`TM`) : ces fichiers de données sont créés par les processus UUCP sous le répertoire spool `/var/spool/uucp/`*x* lorsqu'un fichier est reçu depuis un autre ordinateur. Le répertoire *x* porte le même nom que l'ordinateur distant qui envoie le fichier. Les noms des fichiers de données temporaires ont le format suivant :

  `TM.`*pid.ddd*

  pid est un ID de processus et *ddd* est un nombre séquentiel à trois chiffres qui commence à 0.

  Lorsque le fichier entier est reçu, le fichier `TM`*pid.ddd* est déplacé vers le nom du chemin d'accès spécifié dans le fichier `C.`*sysnxxx* (présenté par la suite) qui a lancé la transmission. Si la transformation se termine de manière anormale, le fichier `TM.`*pid.ddd* peut rester dans

le répertoire *x*. Ces fichiers sont normalement automatiquement supprimés par la commande `uucleanup`.

- *Fichier de verrouillage* (`LCK`) : les fichiers de verrouillage sont créés dans le répertoire `/var/spool/locks` pour chaque périphérique en cours d'utilisation. Les fichiers de verrouillage empêchent les conversations dupliquées et les tentatives multiples d'utilisation du même périphérique appelant. Le tableau suivant présente les différents types de fichiers de verrouillage UUCP.

TABLEAU 12-6 Fichiers de verrouillage UUCP

Nom de fichier	Description
`LCK.`*sys*	*sys* représente le nom de l'ordinateur qui utilise le fichier
`LCK.`*dev*	*dev* représente le nom d'un périphérique qui utilise le fichier
`LCK.`*LOG*	*LOG* représente un fichier journal UUCP verrouillé

Ces fichiers peuvent rester dans le répertoire spool si le lien de communication est inopinément coupé, comme par exemple lorsque votre ordinateur tombe en panne. Le fichier de verrouillage est ignoré (supprimé) une fois que le processus parent n'est plus actif. Le fichier de verrouillage contient l'ID de processus du processus qui a créé le verrou.

- *Fichier de travail* (`C.`) : les fichiers de travail sont créés dans un répertoire spool lorsqu'un travail (transfert de fichiers ou exécutions de commandes à distance par exemple) a été mis en attente pour un ordinateur distant. Les noms des fichiers de travail ont le format suivant :

  `C.`*sysnxxxx*

  sys est le nom de l'ordinateur distant, *n* est le caractère ASCII qui représente le niveau (priorité) du travail et *xxxx* est le numéro séquentiel à quatre chiffres du travail affecté par UUCP. Les fichiers de travail contiennent les informations suivantes :

  - Nom du chemin d'accès complet du fichier à envoyer ou à requérir.
  - Nom du chemin d'accès complet de la destination, utilisateur ou nom de fichier.
  - Nom de connexion de l'utilisateur.
  - Liste d'options.
  - Nom des fichiers de données associés dans le répertoire spool. Si l'option `uucp-C` ou `uuto-p` a été spécifiée, un faux nom (`D.0`) est utilisé.
  - Bits de mode du fichier source.
  - Nom de connexion de l'utilisateur distant à notifier de l'achèvement du transfert.
- *Fichier de données*(`D.`) : les fichiers de données sont créés lorsque vous indiquez sur la ligne de commande de copier le fichier source dans le répertoire spool. Les noms des fichiers de données ont le format suivant :

  `D.` *systmxxxxyyy* : *systm* représente les cinq premiers caractères du nom de l'ordinateur distant. *xxxx* est le numéro séquentiel à quatre chiffres du travail affecté par `uucp`. Ce numéro peut être suivi d'un autre nombre. *yyy* est utilisé lorsque plusieurs fichiers `D.` sont créés pour un fichier de travail (`C.`).

- `X.`*(execute file)* : les fichiers d'exécution sont créés dans le répertoire spool avant les exécutions de commandes à distance. Les noms des fichiers d'exécution ont le format suivant :

  `X.`*sysnxxxx*

  sys est le nom de l'ordinateur distant. *n* est le caractère qui représente le niveau (priorité) du travail. *xxxx* est un numéro de séquence à quatre chiffres assigné par UUCP. Les fichiers d'exécution contiennent les informations suivantes :

  - Identifiant de connexion et nom de l'ordinateur du demandeur
  - Noms des fichiers requis pour l'exécution
  - Entrée à utiliser comme entrée standard pour la chaîne de commande
  - Nom de l'ordinateur et du fichier qui recevront une sortie standard après exécution de la commande
  - Chaîne de commande
  - Lignes d'option pour les demandes d'état de retour

Messages d'erreur UUCP

Cette section répertorie les messages d'erreur associés avec UUCP.

Messages d'erreur UUCP ASSERT

Le tableau suivant répertorie les messages d'erreur ASSERT.

TABLEAU 12-7 Messages d'erreur ASSERT

Message d'erreur	Description ou action
`CAN'T OPEN`	Une commande `open()` ou `fopen()` a échoué.
`CAN'T WRITE`	Une commande `write()`, `fwrite()`, `fprint()` ou une autre commande similaire a échoué.
`CAN'T READ`	Une commande `read()`, `fgets()` ou une autre commande similaire a échoué.
`CAN'T CREATE`	Un appel `creat()` a échoué.
`CAN'T ALLOCATE`	Une allocation dynamique a échoué.
`CAN'T LOCK`	Une tentative de création d'un fichier `LCK` (fichier de verrouillage) a échoué. Dans certains cas, cette erreur est fatale.
`CAN'T STAT`	Un appel `stat()` a échoué.
`CAN'T CHMOD`	Un appel `chmod()` a échoué.
`CAN'T LINK`	Un appel `link()` a échoué.
`CAN'T CHDIR`	Un appel `chdir()` a échoué.
`CAN'T UNLINK`	Un appel `unlink()` a échoué.
`WRONG ROLE`	Il s'agit d'un problème de logique interne.

Message d'erreur	Description ou action
CAN'T MOVE TO CORRUPTDIR	Une tentative de déplacer des fichiers C. ou X. corrompus vers le répertoire /var/spool/uucp/.Corrupt a échoué. Le répertoire est probablement manquant ou le mode ou le propriétaire est incorrect.
CAN'T CLOSE	Un appel close() ou fclose() a échoué.
FILE EXISTS	La création d'un fichier C. ou D. a été tentée, mais le fichier existe déjà. Cette erreur se produit lorsqu'un problème survient avec la séquence d'accès aux fichiers, ce qui indique généralement une erreur du logiciel.
NO uucp SERVICE NUMBER	Un appel TCP/IP est tenté, mais aucune entrée ne se trouve dans le fichier /etc/services pour UUCP.
BAD UID	L'ID de l'utilisateur ne figure pas dans la base de données de mots de passe. Vérifiez la configuration du service de noms.
BAD LOGIN_UID	Identique à la description précédente.
BAD LINE	Une ligne incorrecte se trouve dans le fichier Devices. Pas assez d'arguments sur une ou plusieurs lignes.
SYSLST OVERFLOW	Une table interne dans le fichier gename.c est saturée. Un travail unique a tenté de communiquer avec plus de 30 systèmes.
TOO MANY SAVED C FILES	Identique à la description précédente.
RETURN FROM fixline ioctl	Une commande ioctl(2), qui ne devrait jamais échouer, a échoué. Un problème s'est produit au niveau du pilote système.
BAD SPEED	Une vitesse de ligne erronée s'affiche dans le fichier Périphériques ou Systems (champ Class ou Speed).
BAD OPTION	Une ligne ou une option incorrecte se trouve dans le fichier Permissions. Cette erreur doit être corrigée immédiatement.
PKCGET READ	L'ordinateur distant est probablement bloqué. Aucune action n'est nécessaire.
PKXSTART	L'ordinateur distant a été interrompu de manière irrécupérable. Généralement, cette erreur peut être ignorée.
TOO MANY LOCKS	Un problème interne s'est produit. Contactez votre fournisseur système.
XMV ERROR	Un problème avec un fichier ou un répertoire s'est produit. Le répertoire spool est la cause probable, puisque les modes des destinations sont censés être vérifiés avant que ce processus ne soit lancé.
CAN'T FORK	Une tentative de création de commandes fork et exec a échoué. Le travail en cours ne sera pas perdu, mais retenté ultérieurement (uuxqt). Aucune action n'est nécessaire.

Messages d'erreur UUCP STATUS

Le tableau suivant répertorie les principaux messages d'erreur STATUS.

TABLEAU 12-8 Messages UUCP STATUS

Message d'erreur	Description/Action
OK	Le statut est acceptable.
NO DEVICES AVAILABLE	Aucun périphérique n'est actuellement disponible pour l'appel. Vérifiez si un périphérique se trouve dans le fichier Devices pour le système spécifique. Recherchez le périphérique à utiliser pour appeler le système dans le fichier Systems.
WRONG TIME TO CALL	Un appel a été passé sur le système à un moment autre que celui spécifié dans le fichier Systems.
TALKING	Explicite.
LOGIN FAILED	La connexion à un ordinateur spécifique a échoué. La cause peut être un identifiant de connexion ou mot de passe incorrect, un mauvais numéro, un ordinateur lent ou une erreur d'exécution du script DTP.

Message d'erreur	Description/Action
CONVERSATION FAILED	La conversation a échoué après un démarrage réussi. Cette erreur signifie généralement qu'un côté s'est arrêté, le programme a été interrompu ou la ligne (le lien) a été supprimée.
DIAL FAILED	L'ordinateur distant n'a jamais répondu. La cause peut être un dialer incorrect ou un numéro de téléphone erroné.
BAD LOGIN/MACHINE COMBINATION	L'ordinateur a été appelé avec un identifiant de connexion/nom d'ordinateur qui ne respecte pas le fichier Permissions. Cette erreur peut être une tentative d'usurpation d'identité.
DEVICE LOCKED	Le périphérique appelant à utiliser est actuellement verrouillé et en cours d'utilisation par un autre processus.
ASSERT ERROR	Une erreur ASSERT s'est produite. Vérifiez le fichier /var/uucp/.Admin/errors afin de connaître le message d'erreur et reportez-vous à la section “Messages d'erreur UUCP ASSERT” à la page 215.
SYSTEM NOT IN Systems FILE	Le système n'apparaît pas dans le fichier Systems.
CAN'T ACCESS DEVICE	Le périphérique ayant fait l'objet d'une tentative n'existe pas ou les modes sont incorrects. Vérifiez les entrées correspondantes dans les fichiers Systems et Périphériques.
DEVICE FAILED	Le périphérique n'a pas pu être ouvert.
WRONG MACHINE NAME	L'ordinateur appelé porte un autre nom que celui attendu.
CALLBACK REQUIRED	L'ordinateur appelé nécessite d'appeler votre ordinateur.
REMOTE HAS A LCK FILE FOR ME	L'ordinateur distant possède un fichier LCK pour votre ordinateur. L'ordinateur distant pourrait être en train d'essayer d'appeler votre ordinateur. Si l'ordinateur distant dispose d'une version plus ancienne d'UUCP, le processus qui s'adressait à votre ordinateur peut avoir échoué, en laissant le fichier LCK. Si l'ordinateur distant dispose de la nouvelle version d'UUCP et ne communique pas avec votre ordinateur, le processus possédant un fichier LCK est bloqué.
REMOTE DOES NOT KNOW ME	L'ordinateur distant n'a pas le nom de noeud de votre ordinateur dans son fichier Systems.
REMOTE REJECT AFTER LOGIN	L'identifiant de connexion utilisé par votre ordinateur pour la connexion ne correspond pas à ce que l'ordinateur distant attendait.
REMOTE REJECT, UNKNOWN MESSAGE	L'ordinateur distant a rejeté la communication avec votre ordinateur pour une raison inconnue. L'ordinateur distant n'exécute peut-être pas une version standard d'UUCP.
STARTUP FAILED	La connexion a réussi, mais la procédure d'établissement de connexion initiale a échoué.
CALLER SCRIPT FAILED	Cette erreur est généralement identique à l'erreur DIAL FAILED. Toutefois, si cette erreur se produit souvent, considérez le script appelant dans le fichier Dialers. Utilisez Uutry pour procéder à la vérification.

Messages d'erreur numériques UUCP

Le tableau ci-dessous répertorie les numéros de code de sortie que les messages de statut d'erreur produites par le fichier /usr/include/sysexits.h. Ils ne sont pas tous actuellement utilisés par uucp .

TABLEAU 12-9 Messages d'erreur UUCP par numéro

Numéro du message	Description	Explication
64	Valeur de base pour les messages d'erreur	Les messages d'erreur commencent par cette valeur.

Numéro du message	Description	Explication
64	Erreur d'utilisation de la ligne de commande	La commande a été utilisée de façon incorrecte, par exemple, avec un nombre d'arguments incorrect, un mauvais indicateur ou une syntaxe erronée.
65	Erreur de formatage des données	Les données d'entrée étaient incorrectes d'une manière ou d'une autre. Ce format de données doit uniquement être utilisé pour les données d'utilisateur et non pas les fichiers système.
66	Impossible d'ouvrir l'entrée	Un fichier d'entrée, et non un fichier système, n'existe pas ou n'a pas pu être lu. Ce problème peut également inclure des erreurs telles que "Aucun message" pour un logiciel de messagerie.
67	Adresse inconnue	L'utilisateur qui a été spécifié n'existe pas. Cette erreur peut s'appliquer aux adresses électroniques ou aux connexions distantes.
68	Nom d'hôte inconnu	L'hôte n'existe pas. Cette erreur s'applique aux adresses électroniques ou aux demandes réseau.
69	Service non disponible	Un service n'est pas disponible. Cette erreur peut se produire si un programme d'assistance ou un fichier n'existe pas. Ce message peut également simplement indiquer que quelque chose ne fonctionne pas et que la cause n'est actuellement pas identifiable.
70	Erreur logicielle interne	Une erreur logicielle interne a été détectée. Cette erreur doit être limitée aux erreurs qui ne sont pas relatives au système d'exploitation, dans la mesure du possible.
71	Erreur système	Une erreur du système d'exploitation a été détectée. Ce message d'erreur est destiné à être utilisé lorsque des erreurs telles que les "impossible d'effectuer un clonage", "impossible de créer des tubes". Par exemple, cette erreur inclut un retour `getuid` d'un utilisateur qui n'existe pas dans le fichier. `passwd`
72	Fichier critique du système d'exploitation manquant	Un système de fichiers tel que `/etc/passwd` ou `/var/admin/utmpx` n'existe pas, ne peut pas être ouvert ou possède une erreur, telle qu'une erreur de syntaxe.
73	Impossible de créer le fichier de sortie	Un fichier de sortie spécifié par l'utilisateur ne peut pas être créé.
74	Erreur d'entrée/sortie	Une erreur s'est produite lors de l'E/S sur certains fichiers.
75	Panne temporaire. L'utilisateur est invité à procéder à une nouvelle tentative	Panne temporaire qui n'est pas vraiment une erreur. Dans la commande `sendmail`, cela signifie qu'un logiciel de messagerie, par exemple, n'a pas pu établir de connexion et que la demande doit être réessayée ultérieurement.
76	Erreur distance dans le protocole	Le système distant a renvoyé un élément "impossible" au cours d'un protocole d'échange.
77	Autorisation refusée	Vous ne disposez pas des autorisations suffisantes pour exécuter cette opération. Ce message n'est pas conçu pour les problèmes de système de fichiers, qui doivent utiliser `NOINPUT` ou `CANTCREAT`, mais plutôt pour les autorisations de niveau plus élevé. Par exemple, `kre` utilise ce message pour limiter les élèves pouvant leur envoyer des e-mail.
78	Erreur de configuration	Le système a détecté une erreur dans la configuration.
79	Entrée non trouvée	Entrée non trouvée.
79	Valeur maximale répertoriée	Valeur la plus élevée pour les messages d'erreur.

Index

B

C

D

E

F

G

H

I

N

O

P

Q

R

S

T

U

V

W

X