Gestión de redes seriales con UUCP y PPP en Oracle® Solaris 11.2

Referencia: E53885
Julio de 2014

ORACLE

Contenido

Uso de esta documentación

- **Descripción general**: describe cómo activar los servicios PPP y UUCP para proporcionar redes en serie.
- **Destinatarios**: administradores de sistemas.
- **Conocimientos necesarios**: básicos y algunos conocimientos avanzados sobre redes.

Biblioteca de documentación del producto

En la biblioteca de documentación (http://www.oracle.com/pls/topic/lookup?ctx=E36784), se incluye información de última hora y problemas conocidos para este producto.

Acceso a My Oracle Support

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

Comentarios

Envíenos comentarios acerca de esta documentación mediante http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Acerca de Solaris Point-to-Point Protocol 4.0

En esta sección se tratan temas de redes en serie. Redes en serie hace referencia al uso de una interfaz en serie, como un puerto RS-232 o V.35 para conectar dos o más equipos para transferencia de datos. A diferencia de las interfaces LAN, como Ethernet, estas interfaces se utilizan para conectar sistemas separados por grandes distancias. PPP (protocolo punto a punto) y UUCP (copia de UNIX a UNIX) son tecnologías distintas que pueden utilizarse para implementar redes en serie. Cuando una interfaz en serie está configurada para red, está disponible para varios usuarios, de la misma forma que cualquier otra interfaz de red, como Ethernet.

En este capítulo, se presenta Solaris PPP 4.0. Esta versión de PPP activa dos equipos en diferentes ubicaciones físicas para comunicarse entre sí mediante PPP a través de diversos medios. Solaris PPP 4.0 se incluye como parte de la instalación base.

Se explican los siguientes temas:

Información básica de Solaris PPP 4.0

Solaris PPP 4.0 implementa el protocolo punto a punto (PPP), un protocolo de enlace de datos que es un miembro del conjunto de protocolos TCP/IP. PPP describe cómo se transmiten los datos entre dos equipos de punto final a través de medios de comunicación, como líneas telefónicas.

Desde principios de 1990, PPP ha sido un estándar de Internet ampliamente utilizado para el envío de datagramas a través de un enlace de comunicaciones. El grupo de trabajo de punto a punto del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force) describe el estándar de PPP en RFC 1661. PPP se utiliza comúnmente cuando los equipos remotos llaman a un proveedor de servicios de Internet (ISP) o a un proveedor corporativo configurado para recibir llamadas entrantes.

Solaris PPP 4.0 se basa en el PPP–2.4 de la Universidad Nacional de Australia (ANU, Australian National University) disponible públicamente e implementa el estándar de PPP. Se admiten enlaces de PPP síncronos y asíncronos.

Compatibilidad de Solaris PPP 4.0

Varias versiones de PPP estándar están disponibles y se utilizan ampliamente en toda la comunidad de Internet. PPP-2.4 de ANU es una opción muy utilizada para Linux, Tru64, UNIX y las tres principales variantes de BSD:

- FreeBSD
- OpenBSD
- NetBSD

Solaris PPP 4.0 brinda funciones ampliamente configurables de PPP-2.4 de ANU para máquinas que ejecutan el sistema operativo Oracle Solaris. Las máquinas que ejecutan Solaris PPP 4.0 pueden configurar fácilmente enlaces de PPP a cualquier máquina que ejecuta una implementación de PPP estándar.

Algunas implementaciones de PPP que no se basan en ANU que interoperan correctamente con Solaris PPP 4.0 incluyen lo siguiente:

- Solaris PPP (también conocido como `asppp`) disponible desde la versión Solaris 2.4 hasta la versión Solaris 8
- Solstice™ PPP 3.0.1
- Microsoft Windows 98 DUN
- Cisco IOS 12.0 (síncrono)

Cómo determinar qué versión de Solaris PPP se debe usar

La implementación de PPP que se admite es Solaris PPP 4.0. La versión Solaris 9 y las versiones subsiguientes no incluyen el software de Solaris PPP asíncrono anterior (`asppp`). Para obtener más información, consulte el Capítulo 9, Migración desde Solaris PPP asíncrono a Solaris PPP 4.0 (tareas).

¿Por qué utilizar Solaris PPP 4.0?

Si actualmente utiliza `asppp`, considere la posibilidad de migrar a Solaris PPP 4.0. Tenga en cuenta las siguientes diferencias entre las dos tecnologías de Solaris PPP:

- **Modos de transferencia**

  `asppp` admite sólo comunicaciones asíncronas. Solaris PPP 4.0 admite comunicaciones síncronas y asíncronas.
- **Proceso de configuración**

  La configuración de `asppp` necesita la configuración del archivo de configuración `asppp.cf`, tres archivos de UUCP y el comando `ipadm`. Además, debe preconfigurar interfaces para todos los usuarios que posiblemente inicien sesión en el equipo.

  La configuración de Solaris PPP 4.0 necesita opciones de definición para los archivos de configuración de PPP o la emisión del comando `pppd` con opciones. También puede utilizar una combinación del archivo de configuración y los métodos de línea de comandos. Solaris PPP crea y elimina interfaces de manera dinámica. No tiene que configurar directamente las interfaces de PPP para cada usuario.
- **Funciones de Solaris PPP 4.0 no disponibles desde asppp**
  - Autenticación MS-CHAPv1 y MS-CHAPv2
  - PPP a través de Ethernet (PPPoE) para admitir puentes de Línea de abonado digital asimétrica (ADSL)
  - Autenticación PAM
  - Módulos de conexión
  - Direcciones IPv6
  - Compresión de datos que utiliza compresión Deflate o BSD
  - Compatibilidad de devolución de llamada por parte del cliente de Microsoft

Ruta de actualización de Solaris PPP 4.0

Si convierte una configuración de `asppp` existente para Solaris PPP 4.0, puede utilizar la secuencia de comandos de traducción que se proporciona con esta versión. Para obtener instrucciones completas, consulte Cómo convertir de `asppp` a Solaris PPP 4.0 [161].

Dónde ir para obtener más información acerca de PPP

Muchos recursos con información sobre PPP se pueden encontrar impresos y en línea. Las siguientes subsecciones brindan algunas sugerencias.

Manuales de referencia profesional sobre PPP

Para obtener más información sobre implementaciones de PPP muy utilizadas, incluido PPP de ANU, consulte los siguientes manuales:

- Carlson, James. *PPP Design, Implementation, and Debugging.* 2nd ed. (Diseño, implementación y depuración de PPP 2.ª edición). Addison-Wesley, 2000.
- Sun, Andrew. *Using and Managing PPP* (Uso y gestión de PPP). O'Reilly & Associates, 1999.

Solicitudes de comentarios (RFC) sobre PPP

Algunas solicitudes de comentarios de Internet útiles sobre PPP incluyen lo siguientes:

- 1661 y 1662, que describen las principales características de PPP
- 1334, que describe protocolos de autenticación, como el Protocolo de autenticación de contraseña (PAP) y Protocolo de autenticación por desafío mutuo (CHAP)
- 1332, RFC informativa que describe PPP a través de Ethernet (PPPoE)

Para obtener copias de RFC de PPP, especifique el número de la RFC en la página web RFC de IETF en http://www.ietf.org/rfc.html.

Páginas del comando man sobre PPP

Para obtener información técnica acerca de la implementación de Solaris PPP 4.0, consulte las siguientes páginas del comando man:

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

También, consulte la página del comando man para `pppdump`(1M). Puede buscar páginas del comando man relacionadas con PPP mediante el comando `man`.

Configuraciones y terminología de PPP

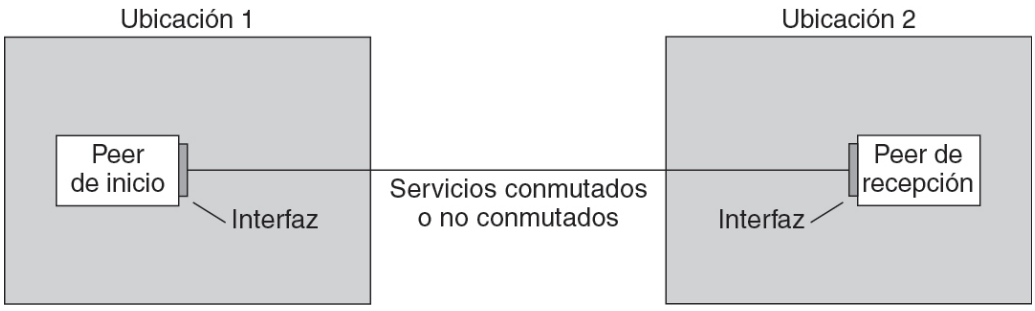
Esta sección presenta configuraciones de PPP. Esta sección también define los términos que se utilizan en esta guía.

Solaris PPP 4.0 admite un número de configuraciones.

- Acceso conmutado o configuraciones *de marcación telefónica*

- Configuraciones de *línea arrendada* o conexión fija

FIGURA 1-1 Partes del enlace de PPP



La figura anterior muestra un enlace de PPP básico. El enlace tiene las siguientes partes:

- Dos máquinas, normalmente en distintas ubicaciones físicas, denominadas *pares*. Un par podría ser un equipo personal, una estación de trabajo de ingeniería, un servidor grande o incluso un enrutador comercial, según los requisitos del sitio.
- Interfaz en serie en cada par. En equipos que ejecutan Oracle Solaris, esta interfaz podría ser `cua`, `ihp` u otra interfaz, según si configura PPP asíncrono o síncrono.
- Enlace físico, como un cable de serie, una conexión de módem o una línea arrendada de un proveedor de red, como una línea T1 o T3.

Descripción general de PPP de acceso telefónico

La configuración de PPP más utilizada es el *enlace de acceso telefónico*. En un enlace por marcación telefónica, el par local *llama* al par remoto para establecer la conexión y ejecutar PPP. En el proceso de marcación telefónica, el par local llama al número de teléfono del par remoto para iniciar el enlace.

Un escenario de marcación telefónica común incluye un equipo que llama a un par en un ISP, configurado para recibir llamadas entrantes. Otro escenario es un sitio corporativo donde un equipo local transmite datos a través de un enlace de PPP para un par en otro edificio.

En esta guía, al par local que inicia la conexión de acceso telefónico se lo denomina *máquina de marcación de salida*. Al par que recibe la llamada entrante se lo denomina como *servidor de marcación de entrada*. Este equipo es en realidad el par de destino del equipo de marcación de salida y es posible o no que sea un servidor verdadero.

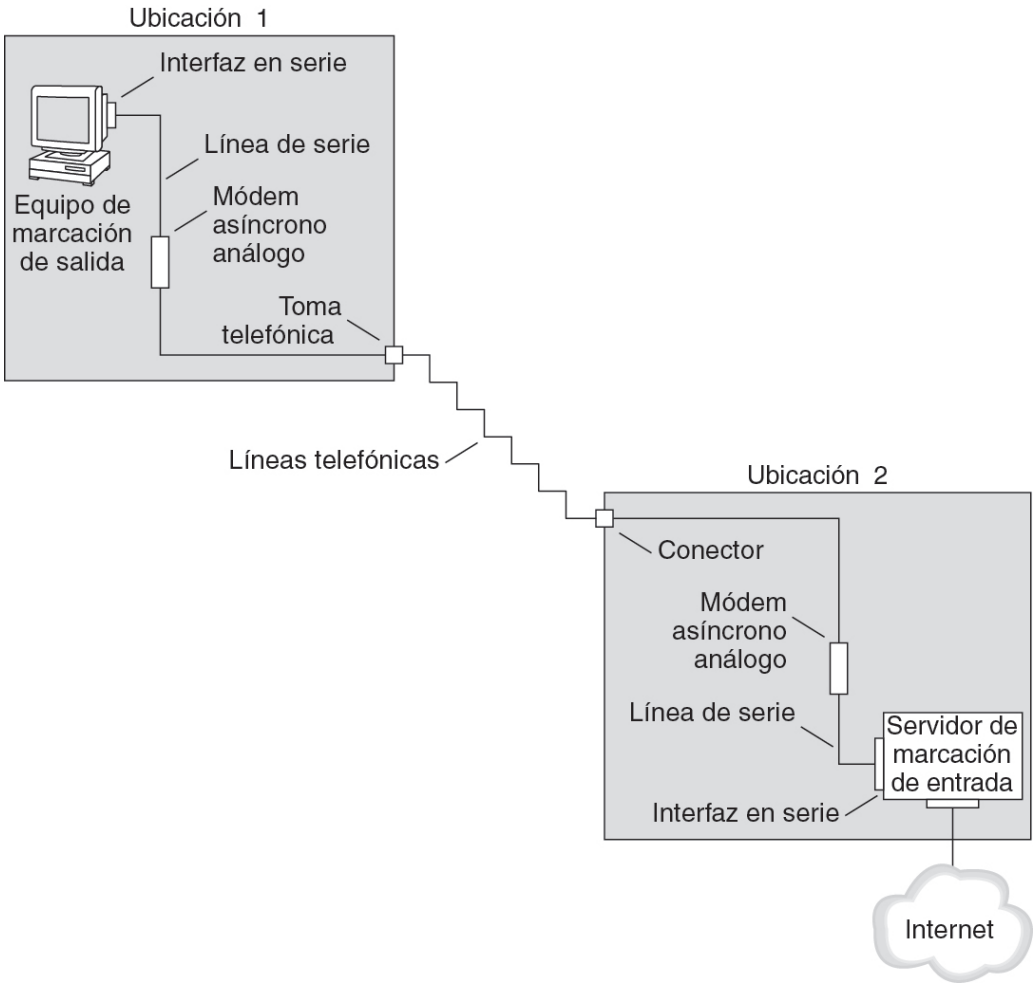
PPP no es un protocolo cliente-servidor. Algunos documentos de PPP utilizan los términos “cliente” y “servidor” para referirse al establecimiento de la llamada telefónica. Un servidor de marcación de entrada no es un servidor verdadero, como un servidor de archivos o un servidor

de nombres. El servidor de marcación de entrada es un término de PPP muy utilizado, debido a que los equipos de marcación de entrada, por lo general, “sirven” accesibilidad de red a más de un equipo de marcación de salida. No obstante, el servidor de marcación de entrada es el par de destino del equipo de marcación de salida.

Partes de un enlace de PPP por marcación telefónica

Consulte la siguiente figura.

FIGURA 1-2 Enlace de PPP por marcación telefónica analógico básico



La configuración de Ubicación 1, el lado de marcación de salida del enlace, se compone de los siguientes elementos:

- Equipo de marcación de salida, normalmente, un equipo personal o una estación de trabajo en el hogar de un individuo.
- Interfaz en serie en la máquina de marcación de salida. `/dev/cua/a` o `/dev/cua/b` es la interfaz en serie estándar para llamadas salientes en máquinas que ejecutan el software de Oracle Solaris.
- Módem asíncrono o adaptador de terminal (TA) RDSI que está conectado a un conector de teléfono.
- Líneas telefónicas y servicios de una compañía telefónica.

La configuración de Ubicación 2, el lado de marcación de entrada del enlace, se compone de los siguientes elementos:

- Conector de teléfono o conector similar, que está conectado a la red de teléfono.
- Módem asíncrono o adaptador de terminal RDSI.
- Interfaz en serie en el servidor de marcación de entrada, ya sea `ttya` o `ttyb` para las llamadas entrantes.
- Servidor de marcación de entrada, que está conectado a una red, como una intranet corporativa, o en la instancia de un ISP, Internet global.

Uso de adaptadores de terminal RDSI con un equipo de marcación de salida

Los adaptadores de terminal RSDI poseen una velocidad superior a los módems, pero los adaptadores de terminal se configuran básicamente de la misma manera. La diferencia principal en la configuración de un adaptador de terminal RDSI está en la secuencia de comandos de chat, que requiere comandos específicos para el fabricante del adaptador de terminal. Consulte “Secuencia de comandos de chat para adaptador de terminal RDSI externo” [132] para obtener información sobre secuencias de comandos de chat para adaptadores de terminal RDSI.

Qué sucede durante comunicaciones de marcación telefónica

Los archivos de configuración de PPP de los iguales de marcación de salida y de marcación de entrada contienen instrucciones para la configuración del enlace. El siguiente proceso se produce cuando se inicia el enlace por marcación telefónica.

1. El usuario o el proceso en la máquina de marcación de salida ejecuta el comando `pppd` para iniciar el enlace.
2. El equipo de marcación de salida lee sus archivos de configuración de PPP. El equipo de marcación de salida envía instrucciones a través de la línea de serie al módem, incluido el número de teléfono del servidor de marcación de entrada.

3. El módem marca el número de teléfono para establecer una conexión telefónica con el módem del servidor de marcación de entrada.

   Las series de cadenas de texto que el equipo de marcación de salida envía al módem y al servidor de marcación de entrada se encuentran en un archivo llamado *secuencia de comandos de chat*. Si es necesario, el equipo de marcación de salida envía comandos al servidor de marcación de entrada para que invoque PPP en el servidor.
4. El módem conectado al servidor de marcación de entrada inicia una negociación de enlace con el módem del equipo de marcación de salida.
5. Cuando la negociación módem a módem se completa, el módem en el equipo de marcación de salida muestra “CONECTAR”.
6. El PPP en ambos iguales ingresa a la fase *Establecer*, donde el Protocolo de control de enlace (LCP) negocia parámetros de enlace básicos y el uso de autenticación.
7. Si es necesario, los pares se autentican recíprocamente.
8. Los Protocolos de control de red (NCP) de PPP negocian el uso de protocolos de red, como IPv4 o IPv6.

El equipo de marcación de salida puede ejecutar `telnet` o un comando similar para un host que se puede alcanzar mediante el servidor de marcación de entrada.

Descripción general de PPP de línea arrendada

Una configuración de PPP de *línea arrendada*, de conexión fija, implica dos pares conectados mediante un enlace. Este enlace consiste en un servicio digital conmutado o no conmutado arrendado de un proveedor. Solaris PPP 4.0 funciona a través de cualquier medio de línea arrendada de punto a punto de dúplex completo. Normalmente, una compañía alquila un enlace de conexión fija de un proveedor de red para conectarse a un ISP u otro sitio remoto.

Comparación de enlaces de líneas arrendadas y por marcación telefónica

En los enlaces de líneas arrendadas y por marcación telefónica participan dos iguales que se conectan por un medio de comunicación. La siguiente tabla hace un resumen de las diferencias entre los tipos de enlace.

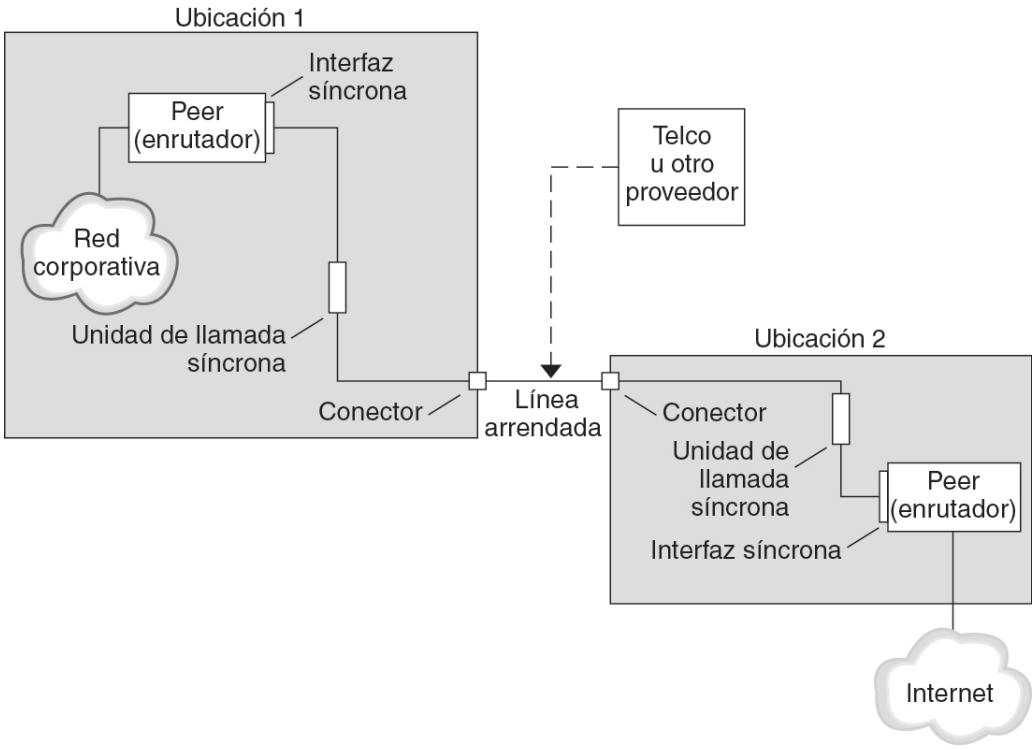
Línea arrendada	Línea de acceso telefónico
Siempre conectada, a menos que un administrador del sistema o un fallo en la alimentación eléctrica la desconecten.	Iniciada a petición, cuando un usuario intenta llamar a un par remoto.
Utiliza comunicaciones síncronas y asíncronas. Para comunicaciones asíncronas, se utiliza por lo general un módem de larga distancia.	Utiliza comunicaciones asíncronas.
Alquilado de un proveedor.	Utiliza líneas telefónicas existentes.

Línea arrendada	Línea de acceso telefónico
Requiere unidades síncronas.	Utiliza módems menos costosos.
Requiere puertos síncronos, que son comunes en la mayoría de los sistemas SPARC. Sin embargo, los puertos síncronos no son comunes en los sistemas x86 ni en los sistemas SPARC más recientes.	Utiliza interfaces en serie estándar que se incluyen en la mayoría de los equipos.

Partes de un enlace de PPP de línea arrendada

Consulte la siguiente figura.

FIGURA 1-3 Configuración de línea arrendada básica



El enlace de línea arrendada contiene las siguientes partes:

- **Dos pares**, cada par en un extremo del enlace. Cada par puede ser una estación de trabajo o un servidor. Con frecuencia el par cumple la función de enrutador entre la red o Internet, y el par opuesto.

- **Interfaz síncrona en cada par**. Algunos equipos que ejecutan el software de Oracle Solaris necesitan que adquiera una tarjeta de interfaz síncrona, como HSI/P, para conectarse a una línea arrendada. Otras máquinas, como las estaciones de trabajo UltraSPARC®, poseen interfaces síncronas incorporadas.
- **Unidad digital síncrona CSU/DSU en cada par**, que conecta el puerto síncrono a la línea arrendada.

  Es posible que una CSU esté incorporada en la DSU, sea de su propiedad o esté arrendada, según su ubicación. La DSU le brinda a un equipo que ejecuta Oracle Solaris una interfaz en serie síncrona estándar. Con Frame Relay, el Dispositivo de acceso Frame Relay (FRAD) realiza la adaptación de interfaz en serie.
- **Línea arrendada**, que proporciona servicios digitales conmutados o no conmutados. Algunos ejemplos son SONET/SDH, Frame Relay PVC y T1.

Qué sucede durante comunicaciones de línea arrendada

En la mayoría de los tipos de líneas arrendadas, los pares en realidad no se llaman entre sí. En su lugar, una compañía adquiere un servicio de línea arrendada para conectarse explícitamente entre dos ubicaciones fijas. A veces, los dos pares en cada extremo de la línea arrendada se encuentran en diferentes ubicaciones físicas de la misma compañía. Otro escenario es una compañía que configura un enrutador en una línea arrendada conectada a un ISP.

Las líneas arrendadas se utilizan con menos frecuencia que los enlaces por marcación telefónica, aunque los enlaces de conexión fija son más fáciles de configurar. Los enlaces de conexión fija no requieren secuencias de comandos de chat. La autenticación no se utiliza con frecuencia porque ambos pares ya se conocen cuando una línea está arrendada. Después de que los dos pares inicien PPP a través de un enlace, el enlace permanece activo. Un enlace de línea arrendada permanece activo a menos que se produzca un fallo en la línea o el par finalice el enlace explícitamente.

Un par en una línea arrendada que ejecuta Solaris PPP 4.0 utiliza la mayoría de los mismos archivos de configuración que definen un enlace de acceso telefónico.

Se produce el siguiente proceso para iniciar la comunicación a través de la línea arrendada:

1. Cada máquina de par ejecuta el comando `pppd` como parte del proceso de inicio u otra secuencia de comandos administrativa.
2. Los pares leen sus archivos de configuración de PPP.
3. Los iguales negocian parámetros de comunicaciones.
4. Se establece un enlace de IP.

Autenticación PPP

Autenticación es el proceso que verifica que el usuario sea quien dice ser. La secuencia de inicio de sesión de UNIX es una forma sencilla de autenticación:

1. El comando `login` solicita al usuario un nombre y una contraseña.
2. `login` intenta autenticar al usuario buscando el nombre de usuario y la contraseña que se introdujeron en la base de datos de contraseñas.
3. Si la base de datos contiene el nombre de usuario y la contraseña, se *autentica* al usuario y se le brinda acceso al sistema. Si la base de datos no contiene el nombre de usuario y la contraseña, se deniega el acceso al sistema.

De manera predeterminada, Solaris PPP 4.0 no solicita autenticación en máquinas que no tienen una ruta predeterminada especificada. Por lo tanto, un equipo local sin una ruta predeterminada no autentica a emisores de llamadas remotos. Por el contrario, si un equipo tiene una ruta predeterminada definida, el equipo remoto siempre autentica a emisores de llamadas remotos.

Puede utilizar protocolos de autenticación PPP para verificar la identidad de los emisores de llamadas que intentan establecer un enlace de PPP a su equipo. Por el contrario, debe configurar la información de autenticación PPP si el equipo local debe llamar a pares que autentican a emisores de llamadas.

Autenticadores y autenticados

La máquina que llama en un enlace de PPP se considera el *autenticado* porque el emisor de llamada debe demostrar su identidad al par remoto. El par se considera el *autenticador*. El autenticador busca la identidad del emisor de llamada en los archivos de PPP adecuados para el protocolo de seguridad y autentica o no al emisor.

Normalmente configura la autenticación PPP para un enlace de acceso telefónico. Cuando se inicia la llamada, el equipo de marcación de salida es el autenticado. El servidor de marcación de entrada es el autenticador. El servidor tiene una base de datos en forma de un archivo *secrets*. Este archivo enumera todos los usuarios a los que se les otorga permiso para configurar un enlace de PPP en el servidor. Considere a estos usuarios como *emisores de llamadas de confianza*.

Algunos equipos de marcación de salida requieren que pares remotos proporcionen información de autenticación al responder la llamada del equipo de marcación de salida. Entonces se invierten los roles: el par remoto se convierte en el autenticado y el equipo de marcación de salida en el autenticador.

Nota - PPP 4.0 no impide la autenticación por parte de iguales de línea arrendada, pero la autenticación no se utiliza con frecuencia en enlaces de líneas arrendadas. La naturaleza de los contratos de líneas arrendadas normalmente implica que los participantes en los extremos de la línea se conocen. Ambos participantes generalmente son de confianza. Sin embargo, ya que la autenticación PPP no es tan difícil de administrar, debe considerar seriamente la implementación de autenticación para líneas arrendadas.

Protocolos de autenticación PPP

Los protocolos de autenticación PPP son: Protocolo de autenticación de contraseña (PAP) y Protocolo de autenticación por desafío mutuo (CHAP). Cada protocolo utiliza una base de datos *secrets* que contiene información de identificación o *credenciales de seguridad*, para cada emisor de llamada al que se le permite establecer un enlace con el equipo local. Para obtener una explicación detallada de PAP, consulte “Protocolo de autenticación de contraseña (PAP)” [135]. Para una explicación de CHAP, consulte “Protocolo de autenticación por desafío mutuo (CHAP)” [139].

¿Por qué utilizar autenticación PPP?

Proporcionar autenticación en un enlace de PPP es opcional. Además, aunque la autenticación verifica que un par es de confianza, la autenticación PPP no proporciona confidencialidad de datos. Para cuestiones de confidencialidad, utilice un software de cifrado, como IPsec, PGP, SSL, Kerberos y Secure Shell.

Nota - Solaris PPP 4.0 no implementa el Protocolo de control de cifrado (ECP) de PPP, que se describe en RFC 1968.

Considere la posibilidad de implementar la autenticación PPP en las siguientes situaciones:

- La compañía acepta llamadas entrantes de usuarios a través de la red telefónica conmutada pública.
- La política de seguridad de la empresa requiere que los usuarios proporcionen credenciales de autenticación al acceder a la red a través de un cortafuegos de la empresa o durante transacciones de seguridad.
- Desea autenticar a los emisores de llamadas según una base de datos de contraseñas de UNIX estándar, como `/etc/passwd`, NIS, LDAP o PAM. Utilice la autenticación PAP para este escenario.
- Los servidores de marcación de entrada de la compañía también proporcionan la conexión a Internet de la red. Utilice la autenticación PAP para este escenario.
- La línea de serie es menos segura que la base de datos de contraseñas del equipo o las redes en cualquiera de los extremos del enlace. Utilice la autenticación CHAP para este escenario.

Compatibilidad para usuarios de DSL a través de PPPoE

Muchos proveedores de red e individuos que trabajan desde casa utilizan tecnología de Línea de suscripción digital (DSL) para proporcionar rápido acceso a la red. Para admitir usuarios

de DSL, Solaris PPP 4.0 incluye la función PPP a través de Ethernet (PPPoE). La tecnología PPPoE permite que varios hosts ejecuten sesiones de PPP a través de un enlace Ethernet para uno o más destinos.

Si uno de los siguientes factores se aplica a su situación, debe utilizar PPPoE:

- Admite usuarios de DSL, posiblemente se lo incluya a usted. Es posible que el proveedor de servicios de DSL requiera que los usuarios configuren un túnel PPPoE para recibir servicios a través de línea DSL.
- Su sitio es un ISP que intenta ofrecer PPPoE a los clientes.

Esta sección presenta términos asociados con PPPoE y una descripción general de la topología de PPPoE básica.

Descripción general de PPPoE

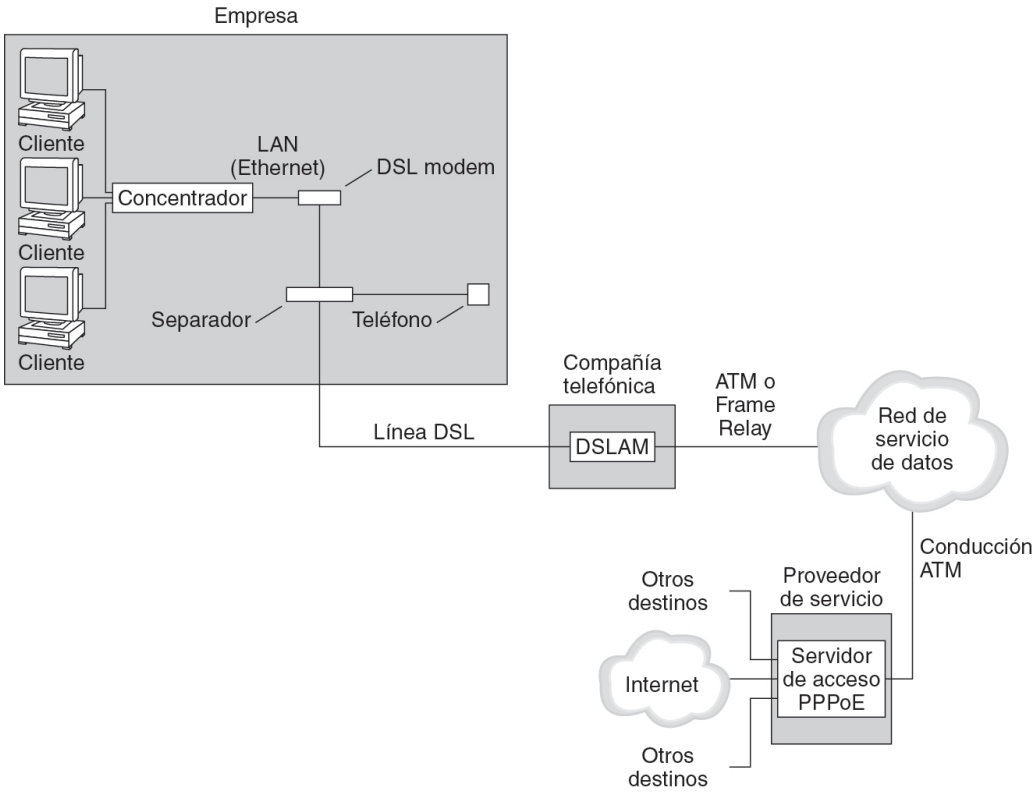
PPPoE es un protocolo de propiedad de RedBack Networks. PPPoE es un protocolo de detección en lugar de otra versión de PPP estándar. En un escenario de PPPoE, un equipo que inicia comunicaciones de PPP primero debe ubicar, o *detectar*, a un par que ejecuta PPPoE. El protocolo de PPPoE utiliza paquetes de difusión Ethernet para localizar al par.

Después del proceso de detección, PPPoE configura un túnel basado en Ethernet del host de inicio, o *cliente PPPoE*, al par, el *servidor de acceso PPPoE*. *Establecimiento de túneles* es la práctica de ejecución de un protocolo encima de otro. Al utilizar PPPoE, Solaris PPP 4.0 crea un túnel de PPP a través de Ethernet IEEE 802.2,, ambos son protocolos de enlace de datos. La conexión de PPP que se obtiene como resultado se comporta como un enlace dedicado entre el cliente PPPoE y el servidor de acceso. Para obtener información detallada sobre PPPoE, consulte “Creación de túneles PPPoE para compatibilidad de DSL” [145].

Partes de una configuración de PPPoE

Tres participantes intervienen en una configuración de PPPoE: un consumidor, una compañía telefónica y un proveedor de servicios, como muestra la siguiente figura.

FIGURA 1-4 Los participantes de un túnel PPPoE



Consumidores de PPPoE

Como administrador del sistema, puede ayudar a los consumidores con sus configuraciones de PPPoE. Un tipo común de consumidor de PPPoE es una persona que necesita ejecutar PPPoE a través de una línea DSL. Otro consumidor de PPPoE es una compañía que compra una línea DSL a través de la cual los empleados pueden ejecutar túneles PPPoE, como se ilustra en la figura anterior.

El motivo principal para que un consumidor corporativo utilice PPPoE es para ofrecer comunicaciones de PPP a través de un dispositivo DSL de alta velocidad a varios hosts. Con frecuencia, un único cliente PPPoE tiene un *módem DSL* individual. O bien, es posible que un grupo de clientes en un concentrador comparta un módem DSL también conectado al concentrador mediante una línea Ethernet.

Nota - Los dispositivos DSL son técnicamente puentes, no módems. Sin embargo, ya que en la práctica común se hace referencia a estos dispositivos como módems, esta guía utiliza el término "módem DSL".

PPPoE ejecuta PPP a través de un túnel en la línea Ethernet conectada al módem DSL. Esa línea está conectada a un separador que, a su vez, se conecta a una línea telefónica.

PPPoE en una compañía telefónica

La compañía telefónica es la capa intermedia del escenario de PPPoE. La compañía telefónica divide la señal que se recibe a través de la línea de teléfono mediante un dispositivo que se denomina *Multiplexor de acceso a la línea digital de abonado (DSLAM)*. DSLAM desglosa las señales en cables independientes, cables analógicos para el servicio telefónico y cables digitales para PPPoE. Desde DSLAM, los cables digitales extienden el túnel a través de una red de datos de ATM al ISP.

PPPoE en un proveedor de servicios

El ISP recibe la transmisión de PPPoE de la red de datos de ATM a través de un puente. En el ISP, un servidor de acceso que ejecuta PPPoE actúa como el par para el enlace de PPP. El servidor de acceso es muy similar en su función al servidor de marcación de entrada que se presentó en la Figura 1-2, “Enlace de PPP por marcación telefónica analógico básico”, pero el servidor de acceso no utiliza módems. El servidor de acceso convierte sesiones de PPPoE individuales en tráfico IP normal, por ejemplo, acceso a Internet.

Si es un administrador del sistema para un proveedor ISP, es posible que sea responsable de la configuración y el mantenimiento de un servidor de acceso.

Seguridad en un túnel PPPoE

El túnel PPPoE es intrínsecamente inseguro. Puede utilizar PAP o CHAP para proporcionar autenticación de usuario para el enlace de PPP que se ejecuta a través del túnel.

♦ ♦ ♦ CAPÍTULO 2

Planificación para el enlace del protocolo punto a punto

La configuración de un enlace de PPP implica una serie de tareas discretas, que incluye tareas de planificación y otras actividades que no están relacionadas con PPP. En este capítulo se explica cómo planificar los enlaces de PPP más comunes, para la autenticación y para PPPoE.

Los capítulos de tareas que siguen al Capítulo 2, Planificación para el enlace del protocolo punto a punto utilizan configuraciones de ejemplo para ilustrar cómo configurar un enlace específico. Estas configuraciones de ejemplo se presentan en este capítulo.

En los temas que se tratan, se incluye lo siguiente:

Planificación de PPP general (mapa de tareas)

PPP requiere tareas de planificación antes de que pueda configurar el enlace. Además, si desea utilizar un establecimiento de túneles PPPoE, primero tiene que configurar el enlace de PPP y, a continuación, proporcionar el establecimiento de túneles. El siguiente mapa de tareas enumera las tareas de planificación que se tratan en este capítulo. Es posible que necesite utilizar sólo la tarea general para el tipo de enlace que se va a configurar. O es posible que requiera la tarea para el enlace, la autenticación y, posiblemente, PPPoE.

TABLA 2-1 Mapa de tareas para planificación de PPP

Tarea	Descripción	Para obtener instrucciones
Plan para enlace de PPP por marcación telefónica	Reunir información necesaria para configurar un equipo de marcación de salida o un servidor de marcación de entrada	"Planificación de un enlace de PPP por marcación telefónica" [30]
Plan para un enlace de línea arrendada	Reunir información necesaria para configurar un cliente en una línea arrendada	"Planificación de un enlace de línea arrendada" [34]

Tarea	Descripción	Para obtener instrucciones
Plan para la autenticación en el enlace de PPP	Reunir información necesaria para configurar autenticación PAP o CHAP en el enlace de PPP	“Planificación para autenticación en un enlace” [37]
Plan para un túnel PPPoE	Reunir información necesaria para configurar un túnel PPPoE a través del cual se puede ejecutar un enlace de PPP	“Planificación de compatibilidad de DSL a través de un túnel PPPoE” [42]

Planificación de un enlace de PPP por marcación telefónica

Los enlaces de acceso telefónico son los enlaces de PPP más usados. Esta sección incluye la siguiente información:

- Información de planificación para un enlace por marcación telefónica
- Explicación del enlace de ejemplo que se utilizará en el Capítulo 3, Configuración de un enlace de protocolo de punto a punto de acceso telefónico

Normalmente, sólo configura el equipo en un solo extremo del enlace de PPP por marcación telefónica, el equipo de marcación de salida o el servidor de marcación de entrada. Para una introducción al PPP por marcación telefónica, consulte “Descripción general de PPP de acceso telefónico” [17].

Antes de configurar el equipo de marcación de salida

Antes de configurar un equipo de marcación de salida, recopile la información que se menciona en la siguiente tabla.

Nota - La información de planificación en esta sección no incluye información para recopilar sobre autenticación o PPPoE. Para obtener detalles sobre la planificación de autenticación, consulte “Planificación para autenticación en un enlace” [37]. Para la planificación de PPPoE, consulte “Planificación de compatibilidad de DSL a través de un túnel PPPoE” [42].

TABLA 2-2 Información para un equipo de marcación de salida

Información	Acción
Velocidad máxima de módem	Consulte la documentación proporcionada por el fabricante del módem.
Comandos de conexión de módem (comandos AT)	Consulte la documentación proporcionada por el fabricante del módem.
Nombre que se utilizará para el servidor de marcación de entrada en el otro extremo del enlace	Cree cualquier nombre que lo ayude a identificar el servidor de marcación de entrada.

Información	Acción
Secuencia de inicio de sesión solicitada por el servidor de marcación de entrada	Póngase en contacto con el administrador del servidor de marcación de entrada o consulte la documentación del ISP si el servidor de marcación de entrada se encuentra en el ISP.

Antes de configurar el servidor de marcación de entrada

Antes de configurar un servidor de marcación de entrada, recopile la información que se muestra en la siguiente tabla.

Nota - La información de planificación en esta sección no incluye información para recopilar sobre autenticación o PPPoE. Para obtener detalles sobre la planificación de autenticación, consulte “Planificación para autenticación en un enlace” [37]. Para la planificación de PPPoE, consulte “Planificación de compatibilidad de DSL a través de un túnel PPPoE” [42].

TABLA 2-3 Información para un servidor de marcación de entrada

Información	Acción
Velocidad máxima de módem	Consulte la documentación proporcionada por el fabricante del módem.
Nombres de usuario de personas a las que se les permite llamar al servidor de marcación de entrada	Obtenga los nombres de los posibles usuarios antes de configurar sus directorios principales, como se ha explicado en Cómo configurar usuarios del servidor de marcación de entrada [57].
Dirección IP dedicada para comunicaciones de PPP	Obtenga una dirección de la persona responsable de delegar direcciones IP en la compañía.

Ejemplo de una configuración para PPP de marcación telefónica

Las tareas que se presentarán en el Capítulo 3, Configuración de un enlace de protocolo de punto a punto de acceso telefónico cumplen los requisitos de una compañía pequeña para permitir que los empleados trabajen en sus casas algunos días de la semana. Algunos empleados necesitan tener el SO Oracle Solaris en los equipos de sus hogares. Esos trabajadores también necesitan iniciar sesión de manera remota en sus equipos de trabajo en la intranet corporativa.

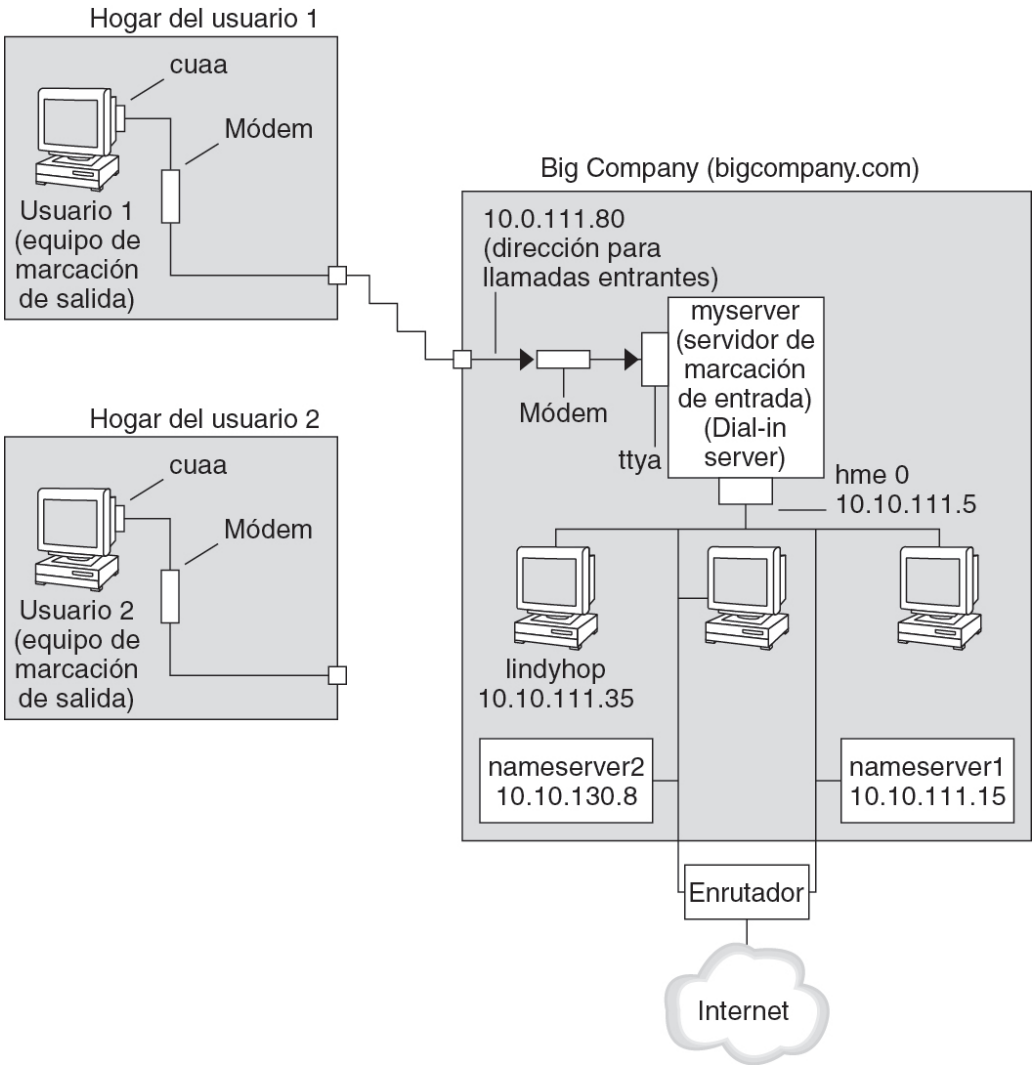
Las tareas configuran un enlace por marcación telefónica básico con las siguientes funciones:

- Los equipos de *marcación de salida* se encuentran en las casas de los empleados que necesitan llamar a la intranet corporativa.

- El servidor de *marcación de entrada* es un equipo en la intranet corporativa que está configurado para recibir llamadas entrantes de los empleados.
- El inicio de sesión de estilo UNIX se utiliza para autenticar el equipo de marcación de salida. La política de seguridad de la compañía no requiere métodos de autenticación de Solaris PPP 4.0 más estrictos.

En la siguiente figura, se muestra el enlace que se configura en el Capítulo 3, Configuración de un enlace de protocolo de punto a punto de acceso telefónico.

FIGURA 2-1 Enlace de acceso telefónico de ejemplo



En esta figura, un host remoto llama mediante su módem a través de la línea telefónica a la intranet de Big Company. Otro host está configurado para llamar a Big Company, pero actualmente está inactivo. Las llamadas de usuarios remotos se contestan en el orden que las recibió el módem que está conectado al servidor de marcación de entrada en Big Company. Una conexión de PPP se establece entre los pares. El equipo de marcación de salida puede entonces iniciar sesión de manera remota en un equipo host en la intranet.

Dónde ir para obtener más información sobre PPP de marcación telefónica

Consulte lo siguiente:

- Para configurar un equipo de marcación de salida, consulte la Tabla 3-2, “Mapa de tareas para configuración de equipo de marcación de salida”.
- Para configurar un equipo de marcación de entrada, consulte la Tabla 3-3, “Mapa de tareas para configuración de servidor de marcación de entrada”.
- Para obtener una descripción general de enlaces por marcación telefónica, consulte “Descripción general de PPP de acceso telefónico” [17].
- Para obtener información detallada sobre comandos y archivos de PPP, consulte “Uso de opciones de PPP en archivos y en la línea de comandos” [113].

Planificación de un enlace de línea arrendada

La configuración de un enlace de línea arrendada implica la configuración del par en un extremo de un servicio conmutado o no conmutado arrendado de un proveedor.

Esta sección incluye la siguiente información:

- Información de planificación para un enlace de línea arrendada
- Explicación del enlace de ejemplo que se muestra en la Figura 2-2, “Ejemplo de una configuración de línea arrendada”

Para obtener una introducción a los enlaces de líneas arrendadas, consulte “Descripción general de PPP de línea arrendada” [20]. Para tareas sobre la configuración de la línea arrendada, consulte el Capítulo 4, Configuración de un enlace de protocolo de punto a punto de línea arrendada.

Antes de configurar el enlace de línea arrendada

Cuando la compañía alquila un enlace de línea arrendada de un proveedor de red, normalmente configura sólo el sistema en su extremo del enlace. Otro administrador mantiene al par en el otro extremo del enlace. Esta persona puede ser un administrador del sistema en una ubicación remota en la compañía o un administrador del sistema en un ISP.

Hardware necesario para un enlace de línea arrendada

Además de los medios de enlace, su extremo del enlace requiere el siguiente hardware:

- Interfaz síncrona para su sistema

- Una unidad síncrona (CSU/DSU)
- Su sistema

Algunos proveedores de red incluyen un enrutador, una interfaz síncrona y una CSU/DSU como parte del equipo local del cliente (CPE). Sin embargo, el equipo necesario varía según el proveedor y cualquier restricción gubernamental en su configuración regional. El proveedor de red puede dar información sobre la unidad que se necesita si este equipo no se proporciona con la línea arrendada.

Información que se recopilará para el enlace de línea arrendada

Antes de configurar el par local, es posible que necesite recopilar los elementos que se enumeran en la siguiente tabla.

TABLA 2-4 Planificación para un enlace de línea arrendada

Información	Acción
Nombre del dispositivo de la interfaz	Consulte la documentación de la tarjeta de interfaz.
Instrucciones de configuración para la tarjeta de interfaz síncrona	Consulte la documentación de la tarjeta de interfaz. Necesita esta información para configurar la interfaz HSI/P. Es posible que no necesite configurar otros tipos de tarjetas de interfaz.
(Opcional) Dirección IP del par remoto	Consulte la documentación del proveedor de servicios. Como alternativa, póngase en contacto con el administrador del sistema del par remoto. Esta información sólo es necesaria si la dirección IP no se negocia entre los dos pares.
(Opcional) Nombre de par remoto	Consulte la documentación del proveedor de servicios. Como alternativa, puede ponerse en contacto con el administrador del sistema del par remoto.
(Opcional) Velocidad del enlace	Consulte la documentación del proveedor de servicios. Como alternativa, puede ponerse en contacto con el administrador del sistema del par remoto.
(Opcional) Compresión que utiliza el par remoto	Consulte la documentación del proveedor de servicios. Como alternativa, puede ponerse en contacto con el administrador del sistema del par remoto.

Ejemplo de una configuración para un enlace de línea arrendada

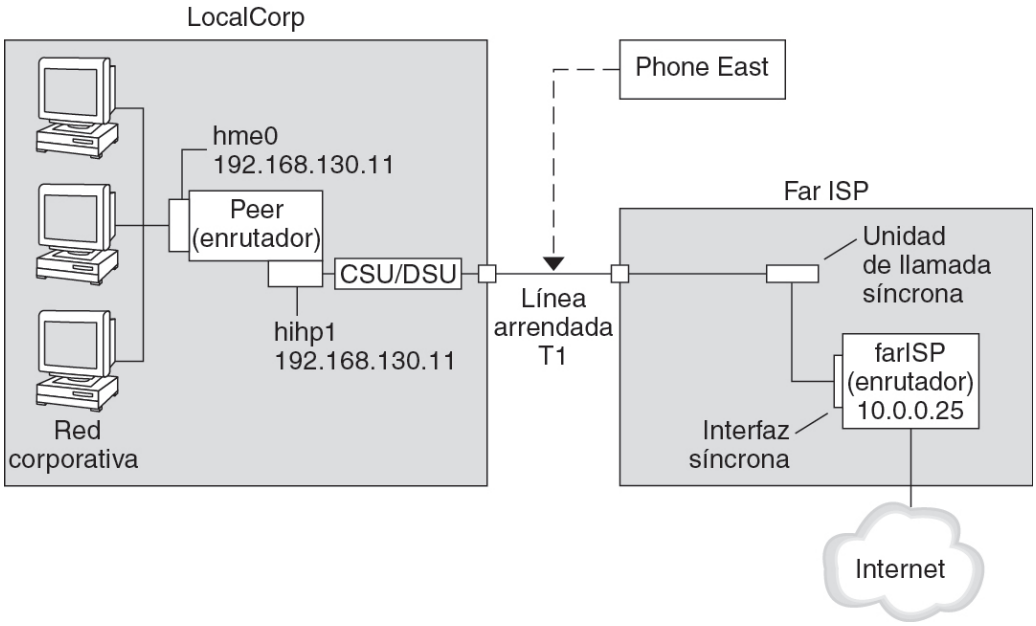
Las tareas del Capítulo 4, Configuración de un enlace de protocolo de punto a punto de línea arrendada muestran cómo implementar el objetivo de una empresa mediana (LocalCorp) para proporcionar acceso a Internet a sus empleados. Actualmente, los equipos de los empleados están conectados a una intranet corporativa privada.

LocalCorp requiere transacciones rápidas y acceso a los muchos recursos de Internet. La organización firma un contrato con Far ISP, un proveedor de servicios que permite a LocalCorp configurar su propia línea arrendada para Far ISP. A continuación, LocalCorp arrenda una línea T1 de Phone East, una compañía telefónica. Phone East coloca la línea arrendada entre LocalCorp y Far ISP. A continuación, Phone East proporciona una CSU/DSU que ya está configurada para LocalCorp.

Las tareas configuran un enlace de línea arrendada con las siguientes características.

- LocalCorp ha configurado un sistema como un enrutador de puerta de enlace, que reenvía paquetes a través de la línea arrendada a hosts en Internet.
- Far ISP también ha configurado un par como un enrutador al cual las líneas arrendadas de clientes están conectadas.

FIGURA 2-2 Ejemplo de una configuración de línea arrendada



En la figura, un enrutador se configura para PPP en LocalCorp. El enrutador se conecta a la intranet corporativa a través de su interfaz `hme0`. La segunda conexión es a través de la interfaz HSI/P (hihp1) del equipo a la unidad digital CSU/DSU. CSU/DSU se conecta a la línea arrendada instalada. El administrador en LocalCorp configura la interfaz HSI/P y los archivos de PPP. El administrador escribe `/etc/init.d/pppd` para iniciar el enlace entre LocalCorp y Far ISP.

Donde ir para obtener más información sobre líneas arrendadas

Consulte lo siguiente:

- Capítulo 4, Configuración de un enlace de protocolo de punto a punto de línea arrendada
- “Descripción general de PPP de línea arrendada” [20]

Planificación para autenticación en un enlace

Esta sección contiene información de planificación para proporcionar autenticación en el enlace de PPP. El Capítulo 5, Configuración de autenticación de protocolo punto a punto contiene tareas para implementar la autenticación PPP en el sitio.

PPP ofrece dos tipos de autenticación, PAP, que se describe en detalle en “Protocolo de autenticación de contraseña (PAP)” [135] y CHAP, que se describe en “Protocolo de autenticación por desafío mutuo (CHAP)” [139].

Antes de configurar la autenticación en un enlace, debe seleccionar qué protocolo de autenticación se adapta mejor a la política de seguridad del sitio. A continuación, configure el archivo secrets y los archivos de configuración de PPP para los equipos de marcación de entrada o los equipos de marcación de salida de los emisores de llamadas, o ambos tipos de equipos. Para obtener información sobre el protocolo de autenticación apropiado para su sitio, consulte “¿Por qué utilizar autenticación PPP?” [24].

Esta sección incluye la siguiente información:

- Información de planificación para autenticación PAP y CHAP
- Explicaciones de escenarios de autenticación de ejemplo que se muestran en la Figura 2-3, “Ejemplo de un escenario de autenticación PAP (al trabajar desde casa)” and Figura 2-4, “Ejemplo de un escenario de autenticación CHAP (llamada a una red privada)”

Para tareas sobre la configuración de la autenticación, consulte el Capítulo 5, Configuración de autenticación de protocolo punto a punto.

Antes de configurar la autenticación PPP

La configuración de la autenticación en el sitio debe ser una parte integral de la estrategia de PPP general. Antes de implementar la autenticación, debe ensamblar el hardware, configurar el software y probar el enlace.

TABLA 2-5 Requisitos previos antes de configurar la autenticación

información	Para obtener instrucciones
Tareas para configurar un enlace por marcación telefónica	Capítulo 3, Configuración de un enlace de protocolo de punto a punto de acceso telefónico.
Tareas para probar el enlace	Capítulo 7, Resolución de problemas comunes del protocolo punto a punto.
Requisitos de seguridad para su sitio	Su política de seguridad corporativa. Si no tiene una política, la configuración de autenticación PPP le ofrece una oportunidad de crear una política de seguridad.
Sugerencias sobre si desea utilizar PAP o CHAP en su sitio	"¿Por qué utilizar autenticación PPP?" [24]. Para obtener información más detallada sobre estos protocolos, consulte "Autenticación de emisores de llamadas en un enlace" [135].

Ejemplos de configuraciones de autenticación PPP

Esta sección contiene ejemplos de autenticación que se utilizarán en los procedimientos del Capítulo 5, Configuración de autenticación de protocolo punto a punto.

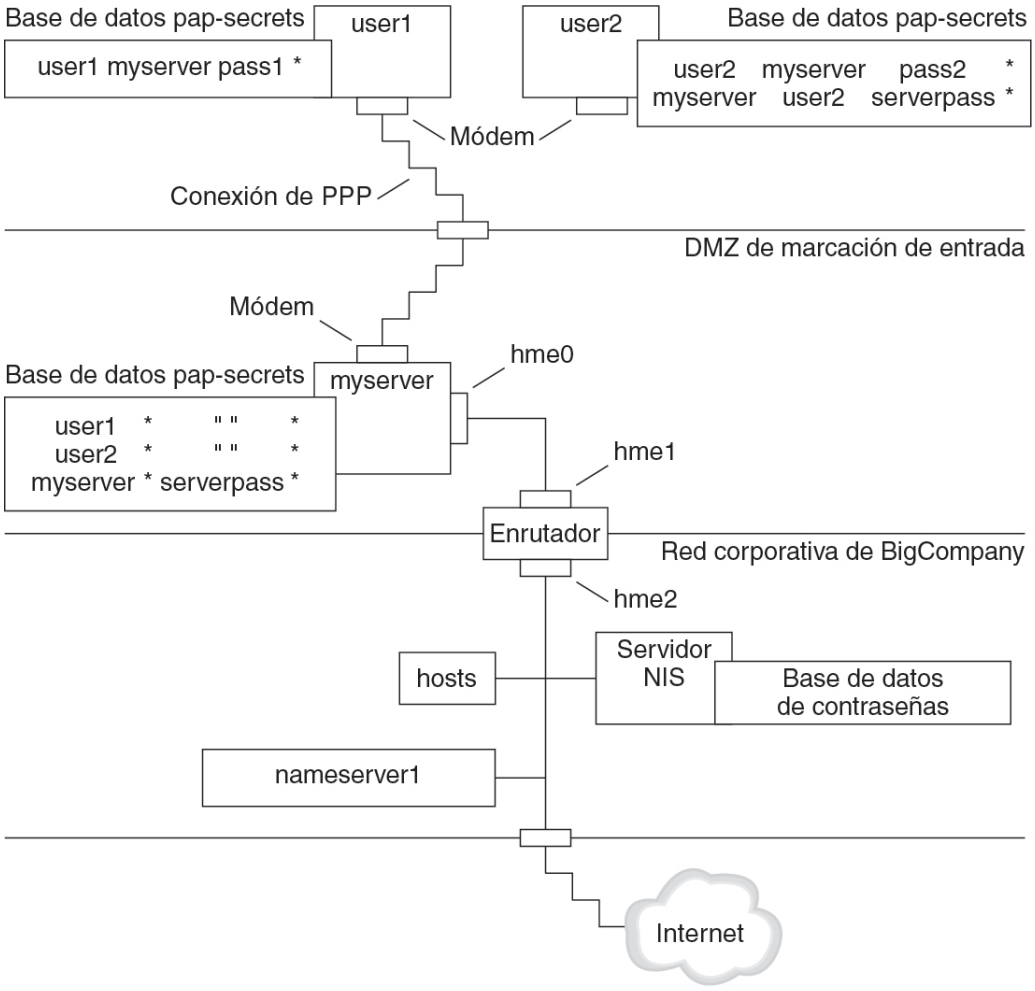
- "Ejemplo de una configuración mediante autenticación PAP" [38]
- "Ejemplo de una configuración mediante autenticación CHAP" [40]

Ejemplo de una configuración mediante autenticación PAP

Las tareas de "Configurar autenticación PAP" [70] muestran cómo configurar la autenticación PAP a través del enlace de PPP. Los procedimientos utilizan como ejemplo un escenario de PAP que se creó para la compañía ficticia "Big Company" en "Ejemplo de una configuración para PPP de marcación telefónica" [31].

Big Company desea permitir que los usuarios trabajen desde casa. Los administradores del sistema desean una solución segura para las líneas de serie al servidor de marcación de entrada. El inicio de sesión de estilo UNIX que utiliza la base de datos de contraseñas NIS ha resultado útil en el pasado para la red de Big Company. Los administradores del sistema desean un esquema de autenticación como UNIX para las llamadas que ingresan a la red a través del enlace de PPP. Por lo tanto, los administradores implementan el siguiente escenario que utiliza autenticación PAP.

FIGURA 2-3 Ejemplo de un escenario de autenticación PAP (al trabajar desde casa)



Los administradores del sistema crean una DMZ de marcación de entrada que está separada del resto de la red corporativa por un enrutador. El término DMZ proviene del término militar “zona desmilitarizada”. La DMZ es una red aislada que se configura por cuestiones de seguridad. La DMZ normalmente contiene los recursos que una compañía ofrece al público, como servidores web, servidores FTP anónimos, bases de datos y servidores de módem. Los diseñadores de red con frecuencia ubican la DMZ entre un cortafuegos y la conexión de Internet de la compañía.

Los únicos ocupantes de la DMZ que se ilustra en la Figura 2-3, “Ejemplo de un escenario de autenticación PAP (al trabajar desde casa)” son el servidor de marcación de entrada `myserver` y el enrutador. El servidor de marcación de entrada requiere que los emisores de llamadas proporcionen credenciales de PAP, incluidos los nombres de usuario y las contraseñas, al configurar el enlace. Además, el servidor de marcación de entrada utiliza la opción `login` de PAP. Por lo tanto, los nombres de usuario y las contraseñas de PAP de los emisores de llamadas deben corresponderse exactamente con los nombres de usuario y las contraseñas de UNIX en la base de datos de contraseñas del servidor de marcación de entrada.

Después de que se establece el enlace de PPP, los paquetes del emisor de llamada se reenvían al enrutador. El enrutador reenvía la transmisión a su destino en la red corporativa o en Internet.

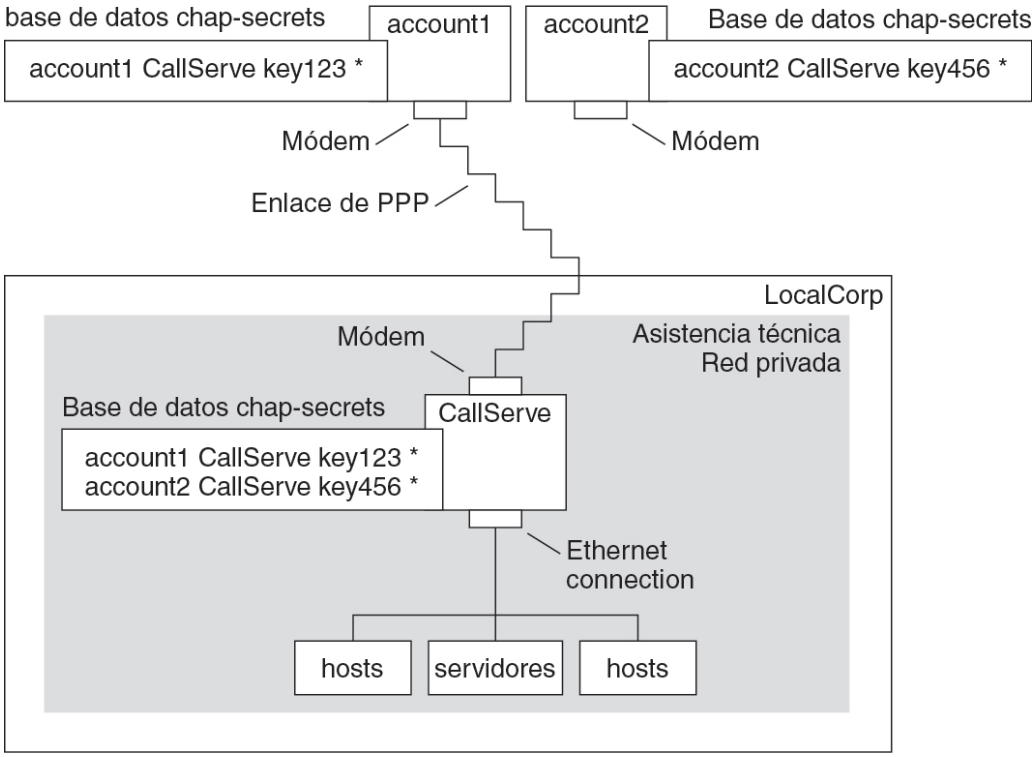
Ejemplo de una configuración mediante autenticación CHAP

Las tareas de “Configuración de autenticación CHAP” [78] muestran cómo configurar la autenticación CHAP. Los procedimientos utilizan como ejemplo un escenario de CHAP que se creará para la compañía ficticia LocalCorp que se presentó en “Ejemplo de una configuración para un enlace de línea arrendada” [35].

LocalCorp proporciona conectividad a Internet a través de una línea arrendada a un ISP. El departamento de asistencia técnica dentro de LocalCorp genera un tráfico de red pesado. Por lo tanto, la asistencia técnica requiere su propia red privada aislada. Los técnicos de campo del departamento viajan mucho y necesitan poder acceder a la red de asistencia técnica desde ubicaciones remotas para obtener información de resolución de problemas. Para proteger la información confidencial en la base de datos de la red privada, se debe autenticar a los emisores de llamadas remotos antes de otorgarles permiso para iniciar sesión.

Por lo tanto, los administradores del sistema implementan el siguiente escenario de autenticación CHAP para una configuración de PPP de acceso telefónico.

FIGURA 2-4 Ejemplo de un escenario de autenticación CHAP (llamada a una red privada)



El único enlace de la red de asistencia técnica al mundo exterior es la línea de serie al extremo del enlace del servidor de marcación de entrada. Los administradores del sistema configuran el equipo portátil de cada representante del servicio de campo para PPP con seguridad de CHAP, incluido un secreto de CHAP. La base de datos chap-secrets en el servidor de marcación de entrada contiene las credenciales de CHAP para todos equipos a los que se les permite llamar a la red de asistencia técnica.

Dónde ir para obtener más información sobre autenticación

Elija entre las siguientes opciones:

- Consulte “Configurar autenticación PAP” [70].
- Consulte “Configuración de autenticación CHAP” [78].

- Consulte “Autenticación de emisores de llamadas en un enlace” [135] y la página del comando man pppd(1M).

Planificación de compatibilidad de DSL a través de un túnel PPPoE

Algunos proveedores de DSL necesitan que configure un túnel PPPoE para su sitio a fin de poder ejecutar PPP a través de líneas DSL de proveedores y redes digitales de alta velocidad. Para obtener una descripción general de PPPoE, consulte “Compatibilidad para usuarios de DSL a través de PPPoE” [24].

En un túnel PPPoE intervienen tres participantes: un consumidor, una compañía telefónica y un ISP. Puede configurar PPPoE para consumidores, como clientes PPPoE en su compañía o consumidores en sus hogares, o bien configurar PPPoE en un servidor en un ISP.

Esta sección contiene información de planificación para ejecutar PPPoE en los clientes y servidores de acceso. Se tratan los temas siguientes:

- Información de planificación para los host PPPoE y el servidor de acceso
- Explicación del escenario PPPoE que se presenta en “Ejemplo de una configuración para un túnel PPPoE” [44]

Para tareas de configuración de túneles PPPoE, consulte el Capítulo 6, Configuración de un túnel de PPP a través de Ethernet.

Antes de configurar un túnel PPPoE

Las actividades de preconfiguración varían según si se configura el lado del cliente o el lado del servidor del túnel. En cualquier caso, el usuario o la organización deben establecer un contrato con una compañía telefónica. La compañía telefónica proporciona las líneas DSL para los clientes y algún tipo de establecimiento de puentes, y posiblemente una conducción ATM para servidores de acceso. En la mayoría de los contratos, la compañía telefónica ensambla los equipos en su sitio.

Antes de configurar un cliente PPPoE

Las implementaciones de un cliente PPPoE constan generalmente de los siguientes equipos:

- Equipo personal u otro sistema que utiliza una persona
- Módem DSL, que generalmente la compañía telefónica o el proveedor de acceso a Internet se encargan de la instalación

- (Optional) Un concentrador, si participa más de un cliente, ya que se aplica para consumidores de DSL corporativos
- (Opcional) Un separador, generalmente lo instala el proveedor

Es posible realizar diferentes configuraciones de DSL, según las necesidades del usuario o de la empresa y los servicios que ofrece el proveedor.

TABLA 2-6 Planificación de clientes PPPoE

Información	Acción
Si configura un cliente PPPoE principal para una persona o para usted, obtenga información de configuración que esté fuera del ámbito de PPPoE.	Pregunte a la compañía telefónica o ISP acerca de los procedimientos de configuración necesarios.
Si configura clientes de PPPoE en un sitio corporativo, recopile los nombres de los usuarios a los que se les asigna sistemas cliente PPPoE. Si configura clientes PPPoE remotos, es posible que sea responsable de proporcionar a los usuarios información acerca de cómo agregar equipos DSL domésticos.	Solicite a la administración de su compañía una lista de usuarios autorizados.
Averigüe qué interfaces están disponibles en el cliente PPPoE.	Ejecute el comando `ipadm show-addr` en cada equipo para los nombres de interfaz.
(Opcional) Obtenga la contraseña para el cliente PPPoE.	Pregunte a los usuarios sus contraseñas predilectas. O bien, asigne contraseñas a los usuarios. Tenga en cuenta que esta contraseña se utiliza para autenticación de enlaces, no para inicio de sesión de UNIX.

Antes de configurar un servidor PPPoE

La planificación para un servidor de acceso PPPoE implica trabajar con la compañía telefónica que proporciona la conexión a su red de servicio de datos. La compañía telefónica instala sus líneas, generalmente conducciones ATM, en su sitio y proporciona algún tipo de establecimiento de puentes a su servidor de acceso. Debe configurar las interfaces Ethernet que acceden a los servicios que ofrece su compañía. Por ejemplo, necesita configurar interfaces para el acceso a Internet, como también interfaces Ethernet del puente de la compañía telefónica.

TABLA 2-7 Planificación de un servidor de acceso PPPoE

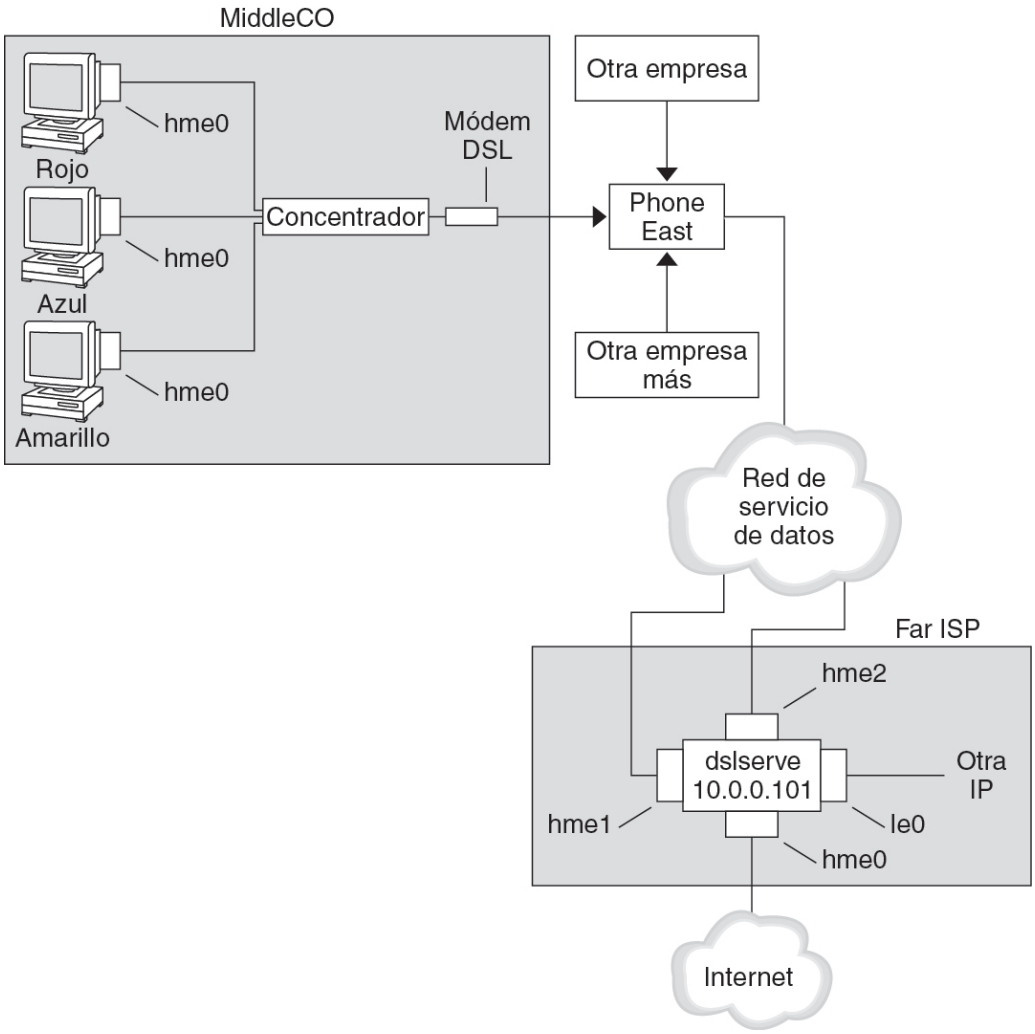
Información	Acción
Interfaces que se utilizan para líneas de red de servicio de datos	Ejecute el comando `ipadm show-addr` para identificar las interfaces.
Tipos de servicios que se proporcionan de un servidor PPPoE	Pregunte a la administración y a los planificadores de redes acerca de los requisitos y solicite sugerencias.
(Opcional) Tipos de servicios para proporcionar a los consumidores	Pregunte a la administración y a los planificadores de redes acerca de los requisitos y solicite sugerencias.
(Opcional) Nombres de host y contraseñas para clientes remotos	Pregunte a los planificadores de redes y a otras personas de su sitio encargadas de las negociaciones de contratos.

Información	Acción
	Los nombres de host y las contraseñas se utilizan para autenticación PAP o CHAP, no para inicio de sesión de UNIX.

Ejemplo de una configuración para un túnel PPPoE

Esta sección contiene un ejemplo de un túnel PPPoE, que se utiliza como una ilustración para las tareas del Capítulo 6, Configuración de un túnel de PPP a través de Ethernet. Aunque la ilustración muestra todos los participantes en el túnel, sólo administra un extremo, ya sea el lado del cliente o del servidor.

FIGURA 2-5 Ejemplo de un túnel PPPoE



En el ejemplo, MiddleCo desea proporcionar a los empleados acceso a Internet de alta velocidad. MiddleCo vende un paquete DSL de Phone East, que, a su vez, establece un contrato con el proveedor de servicios Far ISP. Far ISP ofrece Internet y otros servicios IP para clientes que compran DSL de Phone East.

Ejemplo de una configuración de cliente PPPoE

MiddleCo vende un paquete de Phone East que proporciona una línea DSL para el sitio. El paquete incluye una conexión autenticada dedicada al ISP para clientes PPPoE de MiddleCo. El administrador del sistema conecta a los posibles clientes PPPoE a un concentrador. Los técnicos de Phone East conectan el concentrador a sus equipos DSL.

Ejemplo de una configuración de servidor PPPoE

Para implementar los acuerdos comerciales que FarISP tiene con Phone East, el administrador del sistema en FarISP configura el servidor de acceso `dslserve`. Este servidor tiene las siguientes cuatro interfaces:

- `eri0` – Interfaz de red primaria que se conecta a la red local
- `hme0` – Interfaz a través de la que FarISP proporciona servicio de Internet para sus clientes
- `hme1` – Interfaz contratada por MiddleCo para túneles PPPoE autenticados
- `hme2` – Interfaz contratada por otros clientes para sus túneles PPPoE

Dónde obtener más información sobre PPPoE

Elija entre las siguientes opciones:

- Consulte “Configuración del cliente PPPoE” [86].
- Consulte “Configuración de un servidor de acceso PPPoE” [89].
- Consulte las páginas del comando man “Creación de túneles PPPoE para compatibilidad de DSL” [145], and the `pppoed`(1M), `pppoec`(1M) y `sppptun`(1M) man pages.

♦ ♦ ♦ CAPÍTULO 3

Configuración de un enlace de protocolo de punto a punto de acceso telefónico

En este capítulo se explican las tareas que deben realizarse para configurar el enlace de PPP más común, el enlace por marcación telefónica. Los temas principales incluyen lo siguiente:

- “Configuración del equipo de marcación de salida” [48]
- “Configuración del servidor de marcación de entrada” [55]
- “Llamada al servidor de marcación de entrada” [59]

Tareas principales para configuración de enlace de PPP por marcación telefónica (mapa de tareas)

Se configura el enlace de PPP por marcación telefónica al configurar módems, modificar archivos de base de datos de red y modificar archivos de configuración de PPP que se describen en la Tabla 8-1, “Resumen de comandos y archivos de configuración de PPP”.

La siguiente tabla muestra las principales tareas para configurar ambas partes de un enlace de PPP de acceso telefónico. Normalmente, se configura solamente un extremo del enlace, el equipo de marcación de salida o el servidor de marcación de entrada.

TABLA 3-1 Mapa de tareas para configuración de enlace de PPP por marcación telefónica

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los datos que se necesitan antes de configurar el enlace, como los nombres de host de pares, los números de teléfono de destino y la velocidad del módem.	“Planificación de un enlace de PPP por marcación telefónica” [30]
2. Configurar el equipo de marcación de salida	Configurar el PPP en el equipo que realiza la llamada a través del enlace.	“Tareas para la configuración de un equipo de marcación de salida (mapa de tareas)” [48]
3. Configurar el servidor de marcación de entrada	Configurar el PPP en el equipo que recibe llamadas entrantes.	“Tareas para la configuración de un servidor de marcación de entrada (mapa de tareas)” [55]
4. Llamar al servidor de marcación de entrada	Escribir el comando `pppd` para iniciar comunicaciones.	Cómo llamar al servidor de marcación de entrada [60]

Configuración del equipo de marcación de salida

Las tareas de esta sección explican cómo configurar un equipo de marcación de salida. Las tareas utilizan como ejemplo el escenario de marcación de entrada desde el hogar que se presentó en la Figura 2-1, “Enlace de acceso telefónico de ejemplo”. Puede realizar las tareas de la compañía antes de pasarlas al equipo para un posible usuario. Como alternativa, puede indicar a los usuarios con experiencia acerca de la configuración de los equipos de sus hogares. Cualquier persona que configure un equipo de marcación de salida debe tener permiso root para ese equipo.

Tareas para la configuración de un equipo de marcación de salida (mapa de tareas)

TABLA 3-2 Mapa de tareas para configuración de equipo de marcación de salida

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los datos que se necesitan antes de configurar el enlace, como los nombres de host de pares, los números de teléfono de destino y la velocidad del módem.	“Planificación de un enlace de PPP por marcación telefónica” [30]
2. Configurar el módem y el puerto de serie	Configurar el módem y el puerto de serie.	Cómo configurar el módem y el puerto de serie (equipo de marcación de salida) [50]
3. Configurar la comunicación de línea de serie	Configurar las características de la transmisión a través de la línea de serie.	Cómo definir comunicaciones a través de la línea de serie [51]
4. Definir la conversación entre el equipo de marcación de salida y el par	Recopilar datos de comunicaciones para utilizar al crear la secuencia de comandos de chat.	Cómo crear las instrucciones para llamar a un par [52]
5. Configurar información sobre un par particular	Configurar opciones de PPP para llamar a un servidor de marcación de entrada individual.	Cómo definir la conexión con un par individual [53]
6. Llamar al par	Escribir el comando `pppd` para iniciar comunicaciones.	Cómo llamar al servidor de marcación de entrada [60]

Archivos de plantilla de PPP de marcación telefónica

Solaris PPP 4.0 proporciona archivos de plantilla. Cada plantilla contiene opciones comunes para un determinado archivo de configuración de PPP. La siguiente tabla muestra las plantillas

de ejemplo que se pueden utilizar para la configuración de un enlace de acceso telefónico y sus archivos equivalentes de Solaris PPP 4.0.

Archivo de plantilla	Archivo de configuración de PPP	Para obtener instrucciones
`/etc/ppp/options.tmpl`	`/etc/ppp/options`	“Plantilla `/etc/ppp/options.tmpl`” [118]
`/etc/ppp/options.ttya.tmpl`	`/etc/ppp/options.`*nombre de tty*	“Archivo de plantilla `options.ttya.tmpl`” [120]
`/etc/ppp/myisp-chat.tmpl`	Archivo con el nombre de su elección que contiene la secuencia de comandos de chat	“Plantilla de secuencia de comandos de chat `/etc/ppp/myisp-chat.tmpl`” [128]
`/etc/ppp/peers/myisp.tmpl`	`/etc/ppp/peers/`*nombre de par*	“Archivo de plantilla `/etc/ppp/peers/myisp.tmpl`” [124]

Si decide utilizar uno de los archivos de plantilla, asegúrese de cambiar el nombre de la plantilla a su archivo de configuración de PPP equivalente. La única excepción es la plantilla de archivo de chat `/etc/ppp/myisp-chat.tmpl`. Puede seleccionar cualquier nombre para la secuencia de comandos de chat.

Configuración de dispositivos en el equipo de marcación de salida

La primera tarea para la configuración de un equipo de PPP de marcación de salida es configurar los dispositivos en la línea de serie: el módem y el puerto de serie.

Nota - Las tareas que se aplican a un módem, por lo general, se aplican a un adaptador de terminal (TA) RDSI.

Antes de poder realizar el siguiente procedimiento, debe haber hecho lo siguiente:

- Instalado la versión de Oracle Solaris en los equipos de marcación de salida.
- Determinado la velocidad de módem óptima
- Decidido qué puerto de serie desea utilizar en el equipo de marcación de salida.
- Obtenido la contraseña root para el equipo de marcación de salida.

Para obtener información de planificación, consulte “Antes de configurar el equipo de marcación de salida” [30].

▼ Cómo configurar el módem y el puerto de serie (equipo de marcación de salida)

1. **Programe el módem.**

   Aunque existe una gran variedad de tipos de módem, la mayoría de los módems se envían con la configuración adecuada para Solaris PPP 4.0. La lista siguiente muestra la configuración de parámetros básica para módems que utilizan Solaris PPP 4.0.

   - **DCD:** seguir instrucciones del proveedor
   - **DTR:** establecer en bajo para que el módem finalice la llamada y esté listo para establecer una comunicación
   - **Control de flujo:** establecer a RTS/CTS para control de flujo de hardware dúplex completo
   - **Secuencias de atención:** desactivar

   Si tiene problemas para configurar el enlace y sospecha que el módem es el culpable, consulte primero la documentación del fabricante del módem. Además, varios sitios web ofrecen ayuda con la programación del módem. Por último, puede buscar algunas sugerencias para solucionar problemas del módem en Cómo diagnosticar problemas del módem [103].

2. **Conecte los cables del módem al puerto de serie del equipo de marcación de salida y al conector de teléfono.**

3. **Conviértase en administrador en el equipo de marcación de salida.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

4. **Especificar la dirección del módem como sólo marcación de salida.**

Configuración de comunicaciones en el equipo de marcación de salida

Los procedimientos de esta sección muestran cómo configurar comunicaciones a través de la línea de serie del equipo de marcación de salida. Antes de poder utilizar estos procedimientos, debe haber configurado el módem y el puerto de serie como se describe en Cómo configurar el módem y el puerto de serie (equipo de marcación de salida) [50].

Las siguientes tareas muestran cómo activar el equipo de marcación de salida para iniciar comunicaciones con éxito con el servidor de marcación de entrada. Las comunicaciones se inician como se definió en las opciones de los archivos de configuración de PPP. Necesita crear los siguientes archivos:

- `/etc/ppp/options`

- `/etc/ppp/options.`*nombre de tty*
- Secuencia de comandos de chat
- `/etc/ppp/peers/`*nombre de par*

Solaris PPP 4.0 proporciona plantillas para los archivos de configuración de PPP, que puede personalizar según sus necesidades. Consulte “Archivos de plantilla de PPP de marcación telefónica” [48] para obtener información detallada acerca de esos archivos.

▼ Cómo definir comunicaciones a través de la línea de serie

1. **Conviértase en administrador en el equipo de marcación de salida.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Cree un archivo denominado `/etc/ppp/options` con la siguiente entrada:**

   ```
   lock
   ```

   El archivo `/etc/ppp/options` se utiliza para definir parámetros globales que se aplican a todas las comunicaciones por el equipo local. La opción `lock` activa el bloqueo de estilo UUCP del formato `/var/spool/locks/LK.xxx.yyy.zzz`.

   Nota - Si la máquina de marcación de salida no tiene el archivo `/etc/ppp/options`, sólo el superusuario puede ejecutar el comando `pppd`. Sin embargo, `/etc/ppp/options` puede estar vacío.

   Para obtener una descripción completa de `/etc/ppp/options`, consulte “Archivo de configuración `/etc/ppp/options`” [117].

3. **(Opcional) Cree un archivo denominado `/etc/ppp/options.`*ttyname* para definir cómo se deben iniciar las comunicaciones desde un puerto de serie específico.**

   En el siguiente ejemplo, se muestra un archivo `/etc/ppp/options.`*ttyname* para el puerto con el nombre del dispositivo `/dev/cua/a`.

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

   La opción PPP `crtscts` indica al daemon `pppd` que active el control de flujo de hardware para el puerto de serie a.

   Para obtener más información sobre el archivo `/etc/ppp/options.ttyname`, vaya a “Archivo de configuración `/etc/ppp/options.`*ttyname*” [119].

4. **Establezca la velocidad del módem, como se describe en Cómo establecer la velocidad del módem [56].**

▼ Cómo crear las instrucciones para llamar a un par

Antes de que el equipo de marcación de salida pueda iniciar un enlace de PPP, debe recopilar información sobre el servidor de marcación de entrada que se convertirá en el par. A continuación, podrá utilizar esta información para crear la secuencia de comandos de chat que describe la conversación real entre el equipo de marcación de salida y el par.

1. **Determine la velocidad a la que el módem del equipo de marcación de salida necesita ejecutarse.**

   Para obtener más información, consulte “Configuración de velocidad del módem para un enlace por marcación telefónica” [125].

2. **Obtenga la siguiente información a partir del sitio del servidor de marcación de entrada.**

   - Número de teléfono del servidor
   - Protocolo de autenticación que se utiliza, si corresponde
   - Secuencia de inicio de sesión que requiere el par para la secuencia de comandos de chat

3. **Obtenga los nombres y las direcciones IP de los servidores de nombre en el sitio del servidor de marcación de entrada.**

4. **En una secuencia de comandos de chat, proporcione instrucciones para iniciar llamadas al par particular.**

   Por ejemplo, podría crear la siguiente secuencia de comandos de chat, `/etc/ppp/mychat` para llamar al servidor de marcación de entrada `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
```

La secuencia de comandos contiene instrucciones para llamar a un servidor de marcación de entrada de Oracle Solaris que requiere una secuencia de inicio de sesión. Para obtener una descripción de cada instrucción, consulte “Secuencia de comandos de chat básica mejorada para un inicio de sesión de estilo UNIX” [130]. Para obtener detalles completos sobre la creación de una secuencia de comandos de chat, lea la sección “Definición de la conversación en el enlace por marcación telefónica” [126].

Nota - No invoque la secuencia de comandos de chat directamente. En su lugar, utilice el nombre de archivo de la secuencia de comandos de chat como un argumento para el comando `chat` que invoca la secuencia de comandos.

Si un par ejecuta Oracle Solaris o un sistema operativo similar, considere utilizar la secuencia de comandos de chat anterior como una plantilla para los equipos de marcación de salida.

▼ Cómo definir la conexión con un par individual

1. **Conviértase en administrador en el equipo de marcación de salida.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Actualice la información del repositorio para los servicios DNS y de cambio de nombre.**

```
# 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. **Cree un archivo para el par.**

Por ejemplo, se crearía el siguiente archivo para definir el servidor de marcación de entrada `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	Especifica que el dispositivo `/dev/cua/a` se debe utilizar como la interfaz en serie para llamadas a `myserver`.
57600	Define la velocidad del enlace.
noipdefault	Especifica que para las transacciones con el par `myserver`, la máquina de marcación de salida tiene inicialmente una dirección IP 0.0.0.0. `myserver` asigna una dirección IP a la máquina de marcación de salida para cada sesión de acceso telefónico.
idle 120	Indica que el enlace debe entrar en tiempo de espera tras un período de inactividad de 120 segundos.
noauth	Especifica que el par `myserver` no necesita proporcionar credenciales de autenticación al negociar la conexión con la máquina de marcación de salida.
connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"	Especifica la opción `connect` y sus argumentos, que incluyen el número de teléfono del par, y la secuencia de comandos de chat `/etc/ppp/mychat` con instrucciones de llamada.

Véase también La siguiente lista proporciona referencias a la información relacionada.

- Para configurar otro equipo de marcación de salida, consulte Cómo configurar el módem y el puerto de serie (equipo de marcación de salida) [50].
- Para probar la conectividad del módem llamando a otro equipo, consulte las páginas del comando man `cu`(1C) y `tip`(1). Estas utilidades pueden ayudarlo a probar si el módem está configurado correctamente. Asimismo, emplee estas utilidades para probar si puede establecer una conexión con otro equipo.
- Para obtener más información sobre opciones y archivos de configuración, consulte “Uso de opciones de PPP en archivos y en la línea de comandos” [113].
- Para configurar un servidor de marcación de entrada, consulte “Configuración de dispositivos en el servidor de marcación de entrada” [55].

Configuración del servidor de marcación de entrada

Las tareas de esta sección son para configurar el servidor de marcación de entrada. El servidor de marcación de entrada es un equipo de par que recibe la llamada a través del enlace de PPP desde el equipo de marcación de salida. Las tareas muestran cómo configurar el servidor de marcación de entrada `myserver` que se presentó en la Figura 2-1, “Enlace de acceso telefónico de ejemplo”.

Tareas para la configuración de un servidor de marcación de entrada (mapa de tareas)

TABLA 3-3 Mapa de tareas para configuración de servidor de marcación de entrada

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los datos que se necesitan antes de configurar el enlace, como los nombres de host de pares, los números de teléfono de destino y la velocidad del módem.	“Planificación de un enlace de PPP por marcación telefónica” [30]
2. Configurar el módem y el puerto de serie	Configurar el módem y el puerto de serie.	Cómo configurar el módem y el puerto de serie (servidor de marcación de entrada) [56]
3. Configurar información de par de llamada	Configurar los entornos de usuario y las opciones de PPP para cada equipo de marcación de salida al que se le permite llamar al servidor de marcación de entrada.	Cómo configurar usuarios del servidor de marcación de entrada [57]
4. Configurar la comunicación de línea de serie	Configurar las características de la transmisión a través de la línea de serie.	Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada) [58]

Configuración de dispositivos en el servidor de marcación de entrada

El siguiente procedimiento explica cómo configurar el módem y el puerto de serie en el servidor de marcación de entrada.

Antes de realizar el siguiente procedimiento, debe haber completado las siguientes actividades en el servidor de marcación de entrada de par:

- Instalado la versión de Oracle Solaris
- Determinado la velocidad de módem óptima

- Decidido qué puerto de serie utilizar

▼ Cómo configurar el módem y el puerto de serie (servidor de marcación de entrada)

1. **Programe el módem como se indica en la documentación del fabricante del módem.**

   Para obtener otras sugerencias, consulte Cómo configurar el módem y el puerto de serie (equipo de marcación de salida) [50].

2. **Conecte el módem al puerto de serie del servidor de marcación de entrada.**

3. **Conviértase en administrador en el servidor de marcación de entrada.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

4. **Especifique la dirección del módem como sólo marcación de entrada.**

▼ Cómo establecer la velocidad del módem

El siguiente procedimiento explica cómo establecer la velocidad del módem para un servidor de marcación de entrada. Para obtener sugerencias sobre velocidades a utilizar con equipos de Sun Microsystems, consulte “Configuración de velocidad del módem para un enlace por marcación telefónica” [125].

1. **Inicie sesión en el servidor de marcación de entrada.**

2. **Utilice el comando `tip` para acceder al módem.**

   Las instrucciones para usar `tip` para establecer la velocidad del módem están en la página del comando man `tip`(1).

3. **Configure el módem para una velocidad DTE fija.**

4. **Bloquee el puerto de serie a esa velocidad mediante `ttymon`.**

Véase también La siguiente lista proporciona referencias a la información relacionada.

- Cómo configurar el módem y el puerto de serie (servidor de marcación de entrada) [56]

Configuración de usuarios del servidor de marcación de entrada

Parte del proceso de configuración de un servidor de marcación de entrada incluye información de configuración acerca de cada emisor de llamada remoto conocido.

Antes de iniciar los procedimientos de esta sección, debe haber hecho lo siguiente:

- Obtenido los nombres de usuarios de UNIX para todos los usuarios autorizados a iniciar sesión desde equipos de marcación de salida remotos.
- Configurado el módem y la línea de serie, como se describe en Cómo configurar el módem y el puerto de serie (servidor de marcación de entrada) [56].
- Dedicado una dirección IP para asignar a las llamadas entrantes procedentes de usuarios remotos. Considere la posibilidad de crear una dirección IP entrante dedicada si el número de posibles emisores de llamadas supera el número de módems y puertos de serie del servidor de marcación de entrada. Para obtener información completa sobre la creación de direcciones IP dedicadas, vaya a "Creación de un esquema de direccionamiento IP para emisores de llamadas" [142].

▼ Cómo configurar usuarios del servidor de marcación de entrada

1. **Conviértase en administrador en el servidor de marcación de entrada.**

   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Cree una cuenta nueva en el servidor de marcación de entrada para cada usuario de PPP remoto.**

   Para obtener instrucciones sobre cómo crear un usuario nuevo, consulte "Mapa de tareas para la configuración y gestión de cuentas de usuario mediante el uso de la interfaz de línea de comandos" de "Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.2 ".

3. **Cree para cada emisor de llamada un archivo `$HOME/.ppprc` que contenga varias opciones específicas de la sesión de PPP del usuario.**

   Por ejemplo, puede crear el siguiente archivo `.ppprc` para `pppuser`.

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

`noccp` desactiva el control de compresión del enlace.

Véase también La siguiente lista proporciona referencias a la información relacionada.

- Cómo configurar usuarios del servidor de marcación de entrada [57].
- Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada) [58].

Configuración de comunicaciones a través del servidor de marcación de entrada

La siguiente tarea muestra cómo activar el servidor de marcación de entrada para abrir comunicaciones con cualquier equipo de marcación de salida. Las opciones definidas en los siguientes archivos de configuración de PPP determinan cómo están establecidas las comunicaciones.

- `/etc/ppp/options`
- `/etc/ppp/options.`*nombre de tty*

Para obtener información detallada acerca de estos archivos, consulte "Uso de opciones de PPP en archivos y en la línea de comandos" [113].

Antes de continuar, debe haber hecho lo siguiente:

- Configurado el puerto de serie y el módem en el servidor de marcación de entrada, como se describe en Cómo configurar el módem y el puerto de serie (servidor de marcación de entrada) [56].
- Configurado información sobre los posibles usuarios del servidor de marcación de entrada, como se describe en Cómo configurar usuarios del servidor de marcación de entrada [57].

▼ Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada)

1. **Conviértase en administrador en el servidor de marcación de entrada.**

   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Cree el archivo `/etc/ppp/options` con la siguiente entrada.**

   ```
   nodefaultroute
   ```

`nodefaultroute` indica que ninguna sesión `pppd` en el sistema local puede establecer una ruta predeterminada sin privilegios `root`.

Nota - i el servidor de marcación de entrada no tiene un archivo `/etc/ppp/options`, sólo el superusuario puede ejecutar el comando `pppd` command. Sin embargo, el archivo `/etc/ppp/options` puede estar vacío.

---

3. **Cree el archivo `/etc/options.`*ttyname* para definir cómo las llamadas que se reciben a través del puerto de serie *ttyname* se deben gestionar.**

   El siguiente archivo `/etc/options.ttya` define cómo el puerto de serie del servidor de marcación de entrada `/dev/ttya` debe manejar llamadas entrantes.

   ```
   :10.0.0.80
   xonxoff
   ```

`:10.0.0.80`	Asigna la dirección IP 10.0.0.80 a todos los pares que llaman a través del puerto de serie `ttya`
`xonxoff`	Permite que la línea de serie gestione las comunicaciones de módems con control de flujo de software activado

Véase también

Si ha seguido todos los procedimientos de este capítulo, ha completado la configuración del enlace por marcación telefónica. La siguiente lista proporciona referencias a la información relacionada.

- Para probar la conectividad del módem llamando a otro equipo, consulte las páginas del comando man `cu`(1C) y `tip`(1). Estas utilidades pueden ayudarlo a probar si el módem está configurado correctamente. Asimismo, emplee estas utilidades para probar si puede establecer una conexión con otro equipo.
- Para configurar más opciones del servidor de marcación de entrada, consulte “Configuración del servidor de marcación de entrada” [55].
- Para configurar más equipos de marcación de salida, consulte “Configuración del equipo de marcación de salida” [48].
- Para que el equipo remoto llame al servidor de marcación de entrada, consulte “Llamada al servidor de marcación de entrada” [59].

Llamada al servidor de marcación de entrada

Establece un enlace de PPP por marcación telefónica haciendo que el equipo de marcación de salida llame al servidor de marcación de entrada. Puede indicar al equipo de marcación de salida que llame al servidor especificando la opción `demand` en los archivos de configuración

de PPP locales. Sin embargo, el método más común para establecer el enlace es que el usuario ejecute el comando `pppd` en el equipo de marcación de salida.

Antes de continuar con la tarea siguiente, debe haber hecho una o ambas de las siguientes acciones:

- Configurado el equipo de marcación de salida, como se describe en "Configuración del equipo de marcación de salida" [48]
- Configurado el servidor de marcación de entrada, como se describe en "Configuración del servidor de marcación de entrada" [55]

▼ Cómo llamar al servidor de marcación de entrada

1. **Inicie sesión en la máquina de marcación de salida utilizando la cuenta de usuario común, no `root`.**

2. **Llame al servidor de marcación de entrada ejecutando el comando `pppd`.**

   Por ejemplo, el siguiente comando inicia un enlace entre el equipo de marcación de salida y el servidor de marcación de entrada `myserver`:

   ```
   % pppd 57600 call myserver
   ```

`pppd`	Inicia la llamada invocando el daemon `pppd`
`57600`	Ajusta la velocidad de la línea entre el host y el módem
`call myserver`	Invoca la opción `call` de `pppd`. `pppd` y, a continuación, lee las opciones del archivo `/etc/ppp/peers/myserver`, que se ha creado en Cómo definir la conexión con un par individual [53]

3. **Póngase en contacto con un host en la red del servidor, por ejemplo, el host `lindyhop` que se muestra en la Figura 2-1, "Enlace de acceso telefónico de ejemplo":**

   ```
   ping lindyhop
   ```

   Si el enlace no funciona correctamente, consulte el Capítulo 7, Resolución de problemas comunes del protocolo punto a punto.

4. **Termine la sesión de PPP:**

   ```
   % pkill -x pppd
   ```

Véase también Si ha seguido todos los procedimientos de este capítulo, ha completado la configuración del enlace por marcación telefónica. La siguiente lista proporciona referencias a la información relacionada.

- Para que los usuarios empiecen a trabajar en sus equipos de marcación de salida, consulte Cómo llamar al servidor de marcación de entrada [60].
- Para solucionar problemas en el enlace, consulte Capítulo 7, Resolución de problemas comunes del protocolo punto a punto.
- Para obtener más información sobre los archivos y las opciones que se utilizan en este capítulo, consulte "Uso de opciones de PPP en archivos y en la línea de comandos" [113].

♦ ♦ ♦ CAPÍTULO 4

Configuración de un enlace de protocolo de punto a punto de línea arrendada

En este capítulo se explica cómo configurar un enlace de PPP que utiliza una línea arrendada entre pares. Las secciones principales incluyen lo siguiente:

Configuración de una línea arrendada (mapa de tareas)

Los enlaces de líneas arrendadas son relativamente fáciles de configurar en comparación con los enlaces por marcación telefónica. En la mayoría de los casos, no tiene que configurar la CSU/DSU, los servicios de marcación ni la autenticación. Si necesita configurar la CSU/DSU, consulte la documentación del fabricante para obtener ayuda para esta tarea compleja.

El mapa de tareas en la siguiente tabla describe todas las tareas relacionadas con la configuración de un enlace de línea arrendada básico.

Nota - Algunos tipos de líneas arrendadas exigen CSU/DSU para "marcar" la dirección del par opuesto Por ejemplo, Frame Relay utiliza Circuitos virtuales conmutados (SVCs) o servicio conmutado 56.

TABLA 4-1 Mapa de tareas para configuración del enlace de línea arrendada

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de configuración previa.	Recopilar los datos que se necesitan antes de configurar el enlace.	"Información que se recopilará para el enlace de línea arrendada" [35]
2. Configurar el hardware de la línea arrendada	Integrar CSU/DSU con la tarjeta de interfaz síncrona.	Cómo configurar dispositivos síncronos [64]
3. Configurar la tarjeta de interfaz, si es necesario	Configurar la secuencia de comandos de interfaz que se debe utilizar cuando se inicia la línea arrendada.	Cómo configurar dispositivos síncronos [64]

Tarea	Descripción	Para obtener instrucciones
4. Configurar la información sobre el par remoto	Definir cómo deben funcionar las comunicaciones entre el equipo local y el par remoto.	Cómo configurar un equipo en una línea arrendada [66]
5. Iniciar la línea arrendada	Configurar el equipo para iniciar PPP a través de la línea arrendada como parte del proceso de inicio.	Cómo configurar un equipo en una línea arrendada [66]

Configuración de dispositivos síncronos en la línea arrendada

La tarea en esta sección implica la configuración del equipo requerido por la topología de la línea arrendada que se presenta en “Ejemplo de una configuración para un enlace de línea arrendada” [35]. Los dispositivos síncronos necesarios para conectarse a la línea arrendada incluyen la interfaz y el módem.

Requisitos previos para configuración de dispositivos síncronos

Antes de poder realizar el siguiente procedimiento, debe tener los siguientes elementos:

- Una línea arrendada activa instalada en su sitio por el proveedor
- Una unidad síncrona (CSU/DSU)
- Versión de Oracle Solaris instalada en el sistema
- Una tarjeta de interfaz síncrona del tipo requerido por el sistema

▼ Cómo configurar dispositivos síncronos

1. **Instale físicamente la tarjeta de interfaz en el local, si es necesario.**

   Siga las instrucciones de la documentación del fabricante.

2. **Conecte los cables de la CSU/DSU a la interfaz.**

   Si es necesario, conecte cables de la CSU/DSU al conector de la línea arrendada o a un conector similar.

3. **Configure la CSU/DSU como se indica en la documentación del fabricante o del proveedor de red.**

Nota - Es posible que el proveedor de quien obtuvo la línea arrendada le proporcione y configure la CSU/DSU para su enlace.

4. **Configure la tarjeta de interfaz, si es necesario, como se indica en la documentación de la interfaz.**

   La configuración de la tarjeta de interfaz implica la creación de una secuencia de comandos de inicio para la interfaz. El enrutador en LocalCorp en la configuración de línea arrendada que se muestra en la Figura 2-2, “Ejemplo de una configuración de línea arrendada” utiliza una tarjeta de interfaz HSI/P.

   La siguiente secuencia de comandos, `hsi-conf`, inicia la interfaz 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`	Indica que HSI/P es el puerto síncrono utilizado
`speed=1536000`	Indica la velocidad de la CSU/DSU

Véase también Para configurar el equipo local en la línea arrendada, consulte Cómo configurar un equipo en una línea arrendada [66].

Configuración de un equipo en la línea arrendada

La tarea en esta sección explica cómo configurar un enrutador para que funcione como el par local en el extremo de una línea arrendada. La tarea utiliza la línea arrendada que se presentó en “Ejemplo de una configuración para un enlace de línea arrendada” [35] como ejemplo.

Requisitos previos para la configuración del equipo local en una línea arrendada

Antes de poder realizar el siguiente procedimiento, debe haber realizado lo siguiente:

- Instalado y configurado el dispositivos síncrono para el enlace, como se describe en “Configuración de dispositivos síncronos en la línea arrendada” [64].
- Obtenido la contraseña root para el equipo local en la línea arrendada.
- Configurado el equipo local para que se ejecute como enrutador en la red o redes para utilizar los servicios del proveedor de la línea arrendada.

▼ Cómo configurar un equipo en una línea arrendada

1. **Conviértase en administrador en el equipo local (enrutador).**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Agregue una entrada para el par remoto en el archivo `/etc/hosts` del enrutador.**

```
# 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
```

   El archivo `/etc/hosts` de ejemplo es para el enrutador local en LocalCorp ficticio. Tenga en cuenta la dirección IP y el nombre de host para el par remoto `farisp` en el proveedor de servicios.

3. **Cree el archivo `/etc/ppp/peers/`*peer-name* para mantener información sobre el par del proveedor.**

   Para este ejemplo de enlace de línea arrendada, puede crear el archivo `/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
```

   La siguiente tabla explica las opciones y los parámetros que se utilizan en `/etc/ppp/peers/farISP`.

Opción	Definición
`init '/etc/ppp/conf_hsi'`	Inicia el enlace. `init` luego configura la interfaz HSI utilizando los parámetros en la secuencia de comandos `/etc/ppp/conf_hsi`.

Opción	Definición
`local`	Indica al daemon `pppd` que no cambie el estado de la señal de Terminal de datos listo (DTR, Data Terminal Ready). También le indica a `pppd` que ignore la señal de entrada de Detección de portadora de datos (DCD, Data Carrier Detect).
`/dev/hihp1`	Proporciona el nombre de dispositivo de interfaz síncrona.
`sync`	Establece la codificación síncrona para el enlace.
`noauth`	Establece que el sistema local no necesita solicitar autenticación del par. Sin embargo, el par aún puede solicitar autenticación.
`192.168.130.10:10.0.0.25`	Define las direcciones IP del par local y el par remoto, separado por dos puntos.
`passive`	Indica al daemon `pppd` en la máquina local que pase a modo silencioso después de emitir un número máximo de solicitudes de configuración de LCP y espere a que el par inicie actividad.
`persist`	Indica al daemon `pppd` que intente reiniciar el enlace después de que finaliza una conexión.
`noccp, nopcomp, novj, noaccomp`	Desactiva el Protocolo de control de compresión (CCP), la compresión de campo de protocolo, la compresión de Van Jacobson y la compresión de direcciones y de campo de control respectivamente. Estas formas de compresión aceleran las transmisiones en un enlace por marcación telefónica, pero podrían disminuir la velocidad de la línea arrendada.

4. Cree una secuencia de comandos de inicialización denominada `demand`, que crea el enlace de PPP como parte del proceso de arranque.

```
# 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
```

La secuencia de comandos `demand` contiene los comandos `pppd` para establecer un enlace de línea arrendada. La siguiente tabla explica el contenido de `$PPPDIR/demand`.

Ejemplo de código	Explicación
`if [ -f /system/volatile/ppp-demand.pid ] && /usr/bin/kill -s 0 `/bin/cat /system/volatile/ppp-demand.pid``	Estas líneas comprueban si `pppd` se está ejecutando. Si `pppd` se está ejecutando, no es necesario iniciarlo.
`/usr/bin/pppd call farISP`	Esta línea inicia `pppd`. `pppd` lee las opciones de `/etc/ppp/options`. La opción `call farISP` en la línea de comandos hace que también se lea `/etc/ppp/peers/farISP`.

La secuencia de comandos de inicio de Solaris PPP 4.0 `/etc/rc2.d/S47pppd` invoca la secuencia de comandos `demand` como parte del proceso de arranque. Las siguientes líneas en `/etc/rc2.ds47pppd` buscan la presencia de un archivo que se denomina `$PPPDIR/demand`.

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

Si se encuentra, `$PPPDIR/demand` se ejecuta. Durante el curso de la ejecución de `$PPPDIR/demand`, se establece el enlace.

Nota - Para llegar a equipos que se encuentran fuera de la red local, debe hacer que los usuarios ejecuten `telnet`, `ftp`, `rsh` o comandos similares.

Véase también

Si ha seguido todos los procedimientos de este capítulo, ha completado la configuración del enlace de línea arrendada. La siguiente lista proporciona referencias a la información relacionada.

- Para encontrar información sobre la resolución de problemas, consulte “Resolución de problemas de línea arrendada” [110].
- Para obtener más información sobre los archivos y las opciones que se utilizan en este capítulo, consulte “Uso de opciones de PPP en archivos y en la línea de comandos” [113].

♦ ♦ ♦ CAPÍTULO 5

Configuración de autenticación de protocolo punto a punto

Este capítulo contiene tareas para configuración de autenticación PPP. En los temas que se tratan se incluye lo siguiente:

- “Configurar autenticación PAP” [70]
- “Configuración de autenticación CHAP” [78]

Los procedimientos muestran cómo implementar la autenticación a través de un enlace por marcación telefónica, porque es más probable que los enlaces por marcación telefónica estén configurados para la autenticación que los enlaces de líneas arrendadas. Puede configurar la autenticación a través de líneas arrendadas si la autenticación es requerida por la política de seguridad corporativa. Para la autenticación de líneas arrendadas, use las tareas de este capítulo como directrices.

Si desea utilizar la autenticación PPP, pero no está seguro de qué protocolo debe utilizar, consulte la sección “¿Por qué utilizar autenticación PPP?” [24]. Para obtener más información sobre la autenticación PPP, consulte la página del comando man `pppd`(1M) y “Autenticación de emisores de llamadas en un enlace” [135].

Configuración de autenticación PPP (mapa de tareas)

Esta sección contiene mapas de tareas para ayudarlo a acceder rápidamente a los procedimientos para la autenticación PPP.

TABLA 5-1 Mapa de tareas para autenticación general de PPP

Tarea	Descripción	Para obtener instrucciones
Configurar autenticación PAP	Utilizar estos procedimientos para activar la autenticación PAP en un servidor de marcación de entrada y un equipo de marcación de salida.	“Configuración de autenticación PAP (mapas de tareas)” [70]
Configurar autenticación CHAP	Utilizar estos procedimientos para activar la autenticación CHAP en un servidor	“Configuración de autenticación CHAP (mapas de tareas)” [79]

Tarea	Descripción	Para obtener instrucciones
	de marcación de entrada y un equipo de marcación de salida.	

Configurar autenticación PAP

Las tareas de esta sección explican cómo implementar la autenticación en un enlace de PPP mediante el Protocolo de autenticación de contraseña (PAP). Las tareas utilizan el ejemplo que se muestra en “Ejemplos de configuraciones de autenticación PPP” [38] para ilustrar un escenario de trabajo de PAP para un enlace por marcación telefónica. Utilice las instrucciones como base para la implementación de la autenticación PAP en el sitio.

Antes de poder realizar los siguientes procedimientos debe haber hecho lo siguiente:

- Configurado y probado el enlace por marcación telefónica entre un servidor de marcación de entrada y equipos de marcación de salida que pertenecen a emisores de llamadas de confianza.
- En condiciones ideales, para la autenticación del servidor de marcación de entrada, haber obtenido permiso de superusuario para el equipo donde la base de datos de contraseñas de red se administra, por ejemplo, en LDAP, NIS o archivos locales.
- Obtenido autoridad de superusuario para el equipo local, ya sea servidor de marcación de entrada o equipo de marcación de salida.

Configuración de autenticación PAP (mapas de tareas)

Utilice los mapas de tareas siguientes para acceder rápidamente a tareas relacionadas de PAP con el servidor de marcación de entrada y los emisores de llamadas de confianza en equipos de marcación de salida.

TABLA 5-2 Mapa de tareas para autenticación PAP (servidor de marcación de entrada)

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los nombres de usuario y otros datos necesarios para la autenticación.	“Planificación para autenticación en un enlace” [37]
2. Actualizar la base de datos de contraseñas, si es necesario	Asegurarse de que todos los posibles emisores de llamadas estén en la base de datos de contraseñas del servidor.	Cómo crear una base de datos de credenciales de PAP (servidor de marcación de entrada) [71]
3. Crear la base de datos de PAP	Crear credenciales de seguridad para todos los posibles emisores de llamadas en `/etc/ppp/pap-secrets`.	Cómo crear una base de datos de credenciales de PAP (servidor de marcación de entrada) [71]

Tarea	Descripción	Para obtener instrucciones
4. Modificar los archivos de configuración de PPP	Agregar opciones específicas para PAP a los archivos `/etc/ppp/options` y `/etc/ppp/peers/`*peer-name*.	Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (servidor de marcación de entrada) [73]

TABLA 5-3 Mapa de tareas para autenticación PAP (equipo de marcación de salida)

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los nombres de usuario y otros datos necesarios para la autenticación.	"Planificación para autenticación en un enlace" [37]
2. Crear la base de datos de PAP para el equipo del emisor de llamada de confianza	Crear credenciales de seguridad para un emisor de llamada de confianza y, si es necesario, credenciales de seguridad para otros usuarios que llaman al equipo de marcación de salida, en `/etc/ppp/pap-secrets`.	Cómo configurar credenciales de autenticación PAP para los emisores de llamadas de confianza [75]
3. Modificar los archivos de configuración de PPP	Agregar opciones específicas para PAP a los archivos `/etc/ppp/options` y `/etc/ppp/peers/`*peer-name*.	Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (equipo de marcación de salida) [77]

Configuración de autenticación PAP en el servidor de marcación de entrada

Para configurar la autenticación PAP, debe realizar lo siguiente:

- Crear una base de datos de credenciales de PAP
- Modificar archivos de configuración de PPP para compatibilidad de PAP

▼ Cómo crear una base de datos de credenciales de PAP (servidor de marcación de entrada)

Este procedimiento modifica el archivo `/etc/ppp/pap-secrets`, que contiene las credenciales de seguridad de PAP que se utilizan para autenticar los emisores de llamadas en el enlace. `/etc/ppp/pap-secrets` debe existir en ambos equipos en un enlace de PPP.

El ejemplo de configuración de PAP que se presentó en la Figura 2-3, "Ejemplo de un escenario de autenticación PAP (al trabajar desde casa)" utiliza la opción `login` de PAP. Si planea utilizar esta opción, puede que también necesite actualizar la base de datos de contraseñas de red. Para

obtener más información sobre la opción `login`, consulte “Uso de la opción `login` con `/etc/ppp/pap-secrets`” [139].

1. **Arme una lista de todos los posibles emisores de llamadas de confianza. Los emisores de llamadas de confianza son personas a las que se debe otorgar el permiso de llamar al servidor de marcación de entrada desde sus equipos remotos.**

2. **Verifique que cada emisor de confianza ya tenga un nombre de usuario y una contraseña de UNIX en la base de datos de contraseñas del servidor de marcación de entrada.**

   Nota - La verificación es importante para el ejemplo de configuración de PAP, que utiliza la opción `login` de PAP para autenticar a los emisores de llamadas. Si decide no implementar `login` para PAP, los nombres de usuario de PAP de los emisores de llamadas no tienen que corresponderse con sus nombres de usuario de UNIX. Para obtener más información sobre `/etc/ppp/pap-secrets` estándar, consulte “Archivo `/etc/ppp/pap-secrets`” [136].

   Realice las siguientes acciones si un posible emisor de llamada no tiene un nombre de usuario y una contraseña de UNIX:

   a. **Confirme con sus gestores que emisores de llamadas que no conoce personalmente tienen permiso de acceso al servidor de marcación de entrada.**

   b. **Cree nombres de usuario y contraseñas de UNIX para estos emisores de llamadas de manera que se guíen por la política de seguridad corporativa.**

3. **Conviértase en administrador en el servidor de marcación de entrada.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

4. **Edite el archivo `/etc/ppp/pap-secrets`.**

   Esta versión proporciona un archivo `pap-secrets` en `/etc/ppp` que contiene comentarios sobre cómo utilizar la autenticación PAP, pero no contiene opciones. Puede agregar las siguientes opciones al final de los comentarios.

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

   Para utilizar la opción `login` de `/etc/ppp/pap-secrets` , debe escribir el nombre de usuario de UNIX de cada emisor de llamada de confianza. Siempre que un juego de comillas dobles (““) aparece en el tercer campo, la contraseña para el emisor de llamada se consulta en la base de datos de contraseñas del servidor.

La entrada `myserver * serverpass *` contiene el nombre de usuario y la contraseña de PAP para el servidor de marcación de entrada. En la Figura 2-3, “Ejemplo de un escenario de autenticación PAP (al trabajar desde casa)”, el emisor de llamada de confianza `user2` necesita autenticación de pares remotos. Por lo tanto, el archivo `/etc/ppp/pap-secrets` de `myserver` contiene credenciales de PAP para utilizarlas cuando haya un enlace establecido con `user2`.

Véase también La siguiente lista proporciona referencias a la información relacionada.

- “Modificación de archivos de configuración de PPP para PAP (servidor de marcación de entrada)” [73]
- “Configuración de autenticación PAP para emisores de llamadas de confianza (equipos de marcación de salida)” [75]

Modificación de archivos de configuración de PPP para PAP (servidor de marcación de entrada)

Las tareas de esta sección explican cómo actualizar cualquier archivo de configuración de PPP existente para admitir la autenticación PAP en el servidor de marcación de entrada.

▼ Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (servidor de marcación de entrada)

El procedimiento usa como ejemplos los archivos de configuración de PPP que se presentaron en Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada) [58].

1. **Conviértase en administrador en el servidor de marcación de entrada.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Agregue opciones de autenticación al archivo `/etc/ppp/options`.**

   Por ejemplo, debe agregar las opciones en negrita para un archivo `/etc/ppp/options` existente para implementar la autenticación PAP:

   ```
   lock
   auth
   login
   ```

```
nodefaultroute
proxyarp
ms-dns 10.0.0.1
idle 120
```

`auth`	Especifica que el servidor debe autenticar a los emisores de llamadas antes de establecer el enlace.
`login`	Especifica que el emisor de llamada remoto se debe autenticar mediante el uso de servicios de autenticación de usuarios de UNIX.
`nodefaultroute`	Indica que ninguna sesión de `pppd` en el sistema local puede establecer una ruta predeterminada sin privilegios `root`.
`proxyarp`	Agrega una entrada a la tabla de Protocolo de resolución de direcciones (ARP) del sistema que especifica la dirección IP del par y la dirección Ethernet del sistema. Con esta opción, el par parece estar en el Ethernet local para otros sistemas.
`ms-dns 10.0.0.1`	Activa `pppd` para proporcionar una dirección de Servidor de nombres de dominio (DNS), `10.0.0.1`, para el cliente.
`idle 120`	Especifica que los usuarios inactivos se desconectan después de dos minutos.

3. **En el archivo `/etc/ppp/options.cua.a`, agregue la siguiente dirección para el usuario `cua/a`.**

```
:10.0.0.2
```

4. **En el archivo `/etc/ppp/options.cua.b`, agregue la siguiente dirección para el usuario `cua/b`.**

```
:10.0.0.3
```

5. **En el archivo `/etc/ppp/pap-secrets`, agregue la siguiente entrada.**

```
*     *       ""      *
```

Nota - La opción `login`, como se ha descrito anteriormente, proporciona la autenticación de usuario necesaria. Esta entrada en el archivo `/etc/ppp/pap-secrets` es la forma estándar de activar PAP con la opción `login`.

Véase también Para configurar credenciales de autenticación PAP para los emisores de llamadas de confianza del servidor de marcación de entrada, consulte “Configuración de autenticación PAP para emisores de llamadas de confianza (equipos de marcación de salida)” [75].

Configuración de autenticación PAP para emisores de llamadas de confianza (equipos de marcación de salida)

Esta sección contiene tareas para configuración de autenticación PAP en los equipos de marcación de salida de emisores de llamadas de confianza. Como administrador del sistema, puede configurar la autenticación PAP en los sistemas antes de la distribución a los posibles emisores de llamadas. O bien, si los emisores de llamadas remotos ya tienen sus equipos, puede asignarles a estos las tareas de esta sección.

La configuración de PAP para emisores de llamadas de confianza incluye dos tareas:

- Configuración de las credenciales de seguridad de PAP de los emisores de llamadas.
- Configuración de los equipos de marcación de salida de los emisores de llamadas para admitir autenticación PAP.

▼ Cómo configurar credenciales de autenticación PAP para los emisores de llamadas de confianza

Este procedimiento muestra cómo configurar credenciales de PAP para dos emisores de llamadas de confianza, uno de los cuales necesita credenciales de autenticación de iguales remotos. Los pasos del procedimiento dan por sentado que usted, el administrador del sistema, crea las credenciales de PAP en los equipos de marcación de salida de emisores de llamadas de confianza.

1. **Conviértase en administrador en el equipo de marcación de salida.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

   Con el ejemplo de configuración de PAP que se presentó en la Figura 2-3, “Ejemplo de un escenario de autenticación PAP (al trabajar desde casa)”, asuma que el equipo de marcación de salida pertenece a `user1`.

2. **Modifique la base de datos pap-secrets para el emisor de llamada.**

   Esta versión proporciona un archivo `/etc/ppp/pap-secrets` que contiene comentarios útiles, pero no contiene opciones. Puede agregar las siguientes opciones a este archivo `/etc/ppp/pap-secrets`.

   ```
   user1    myserver  pass1    *
   ```

   Tenga en cuenta que la contraseña de `user1` `pass1` se transmite en formato ASCII legible a través del enlace. `myserver` es el nombre del emisor de llamada `user1` para el par.

3. **Conviértase en administrador en el equipo de marcación de salida.**

   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

   Con el ejemplo de autenticación PAP, asuma que este equipo de marcación de salida pertenece al emisor de llamada `user2`.

4. **Modifique la base de datos pap-secrets para el emisor de llamada.**

   Puede agregar las siguientes opciones al final del archivo `/etc/ppp/pap-secrets` existente.

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

   En este ejemplo, `/etc/ppp/pap-secrets` tiene dos entradas. La primera entrada contiene las credenciales de seguridad de PAP que `user2` pasa al servidor de marcación de entrada `myserver` para la autenticación.

   `user2` requiere credenciales de PAP del servidor de marcación de entrada como de la negociación de enlace. Por lo tanto, `/etc/ppp/pap-secrets` también contiene credenciales de PAP que se esperan de `myserver` en la segunda línea.

Nota - Dado que la mayoría de los ISP no proporcionan credenciales de autenticación, es posible que el escenario anterior no sea realista para comunicaciones con un ISP.

Véase también La siguiente lista proporciona referencias a la información relacionada.

- Cómo crear una base de datos de credenciales de PAP (servidor de marcación de entrada) [71]
- Cómo configurar credenciales de autenticación PAP para los emisores de llamadas de confianza [75]

Modificación de archivos de configuración de PPP para PAP (equipo de marcación de salida)

Las siguientes tareas explican cómo actualizar los archivos de configuración de PPP existentes para admitir la autenticación PAP en los equipos de marcación de salida de emisores de llamadas de confianza.

El procedimiento utiliza los siguientes parámetros para configurar la autenticación PAP en el equipo de marcación de salida que pertenece a `user2`, que se presentó en la Figura 2-3, "Ejemplo de un escenario de autenticación PAP (al trabajar desde casa)". `user2` requiere emisores de llamadas entrantes para autenticar, incluidas las llamadas de `myserver` de marcación de entrada.

▼ Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (equipo de marcación de salida)

Este procedimiento usa como ejemplos los archivos de configuración de PPP que se presentaron en Cómo definir comunicaciones a través de la línea de serie [51]. El procedimiento configura el equipo de marcación de salida que pertenece a `user2`, como se muestra en la Figura 2-3, “Ejemplo de un escenario de autenticación PAP (al trabajar desde casa)”.

1. **Inicie sesión en el equipo de marcación de salida como superusuario.**

2. **Modifique el archivo `/etc/ppp/options`.**

   El siguiente archivo `/etc/ppp/options` contiene opciones para compatibilidad de PAP, que se muestran en negrita.

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

name user2	Establece `user2` como nombre de PAP del usuario en la máquina local. Si se utiliza la opción `login`, el nombre de PAP debe ser el mismo que el nombre de usuario de UNIX del usuario en la base de datos de contraseñas.
auth	Indica que el equipo de marcación de salida debe autenticar a los emisores de llamadas antes de establecer el enlace.

   Nota - Este equipo de marcación de salida demanda autenticación de sus pares, aunque la mayoría de los equipos de marcación de salida no realizan esta demanda. Cualquiera de los casos es aceptable.

require-pap	Solicita credenciales PAP del par.

3. **Cree un archivo `/etc/ppp/peers/`*peer-name* para la máquina remota `myserver`.**

   En el siguiente ejemplo, se muestra cómo agregar compatibilidad de PAP al archivo `/etc/ppp/peers/myserver` existente que se creó en Cómo definir la conexión con un par individual [53].

```
# 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"
```

Las nuevas opciones en negrita agregan requisitos de PAP para pares `myserver`.

user user2	Define `user2` como el nombre de usuario del equipo local.
remotename myserver	Define `myserver` como un par que requiere credenciales de autenticación del equipo local.

Véase también La siguiente lista proporciona referencias a la información relacionada.

- Para probar la configuración de autenticación PAP mediante una llamada al servidor de marcación de entrada, consulte Cómo llamar al servidor de marcación de entrada [60].
- Para obtener más información acerca de la autenticación PAP, consulte “Protocolo de autenticación de contraseña (PAP)” [135].

Configuración de autenticación CHAP

Las tareas de esta sección explican cómo implementar la autenticación en un enlace de PPP mediante el Protocolo de autenticación por desafío mutuo (CHAP). Las tareas utilizan el ejemplo que se muestra en la Figura 2-4, “Ejemplo de un escenario de autenticación CHAP (llamada a una red privada)” para ilustrar un escenario de trabajo de CHAP para acceso telefónico a una red privada. Utilice las instrucciones como base para la implementación de la autenticación CHAP en el sitio.

Antes de poder realizar los siguientes procedimientos, debe haber hecho lo siguiente:

- Configurado y probado el enlace por marcación telefónica entre un servidor de marcación de entrada y equipos de marcación de salida que pertenecen a emisores de llamadas de confianza.
- Obtenido permiso de superusuario para el equipo local, ya sea servidor de marcación de entrada o equipo de marcación de salida.

Configuración de autenticación CHAP (mapas de tareas)

TABLA 5-4 Mapa de tareas para autenticación CHAP (servidor de marcación de entrada)

Tarea	Descripción	Para obtener instrucciones
1. Asignar secretos de CHAP a todos los emisores de llamadas de confianza	Crear o hacer que los emisores de llamadas creen sus secretos de CHAP.	Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada) [80]
2. Crear la base de datos chap-secrets	Agregar las credenciales de seguridad para todos los emisores de llamadas de confianza al archivo `/etc/ppp/chap-secrets`.	Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada) [80]
3. Modificar los archivos de configuración de PPP	Agregar opciones específicas para CHAP a los archivos `/etc/ppp/options` y `/etc/ppp/peers/`*peer-name*.	Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (servidor de marcación de entrada) [81]

TABLA 5-5 Mapa de tareas para autenticación CHAP (equipo de marcación de salida)

Tarea	Descripción	Para obtener instrucciones
1. Crear la base de datos de CHAP para el equipo del emisor de llamada de confianza	Crear credenciales de seguridad para un emisor de llamada de confianza y, si es necesario, credenciales de seguridad para otros usuarios que llaman al equipo de marcación de salida, en `/etc/ppp/chap-secrets`.	Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada) [80]
2. Modificar los archivos de configuración de PPP	Agregar opciones específicas para CHAP al archivo `/etc/ppp/options`.	Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (equipo de marcación de salida) [83]

Configuración de autenticación CHAP en el servidor de marcación de entrada

La primera tarea en la configuración de la autenticación CHAP es modificar el archivo `/etc/ppp/chap-secrets`. Este archivo contiene las credenciales de seguridad de CHAP, incluido el secreto de CHAP, que se utilizan para autenticar a los emisores de llamadas en el enlace.

Nota - Los mecanismos de autenticación UNIX o PAM no funcionan con CHAP. Por ejemplo, no puede utilizar la opción `login` de PPP, como se describe en Cómo crear una base de datos de credenciales de PAP (servidor de marcación de entrada) [71]. Si el escenario de autenticación requiere autenticación PAM o de estilo UNIX, seleccione PAP en su lugar.

El siguiente procedimiento implementa la autenticación CHAP para un servidor de marcación de entrada en una red privada. El enlace de PPP es la única conexión con el mundo exterior. Los únicos emisores de llamadas que tienen acceso a la red son aquellos a los que los gestores de red les han otorgado permiso, incluido, posiblemente, el administrador del sistema.

▼ Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada)

1. **Arme una lista que contenga los nombres de usuario de todos los emisores de llamadas de confianza.**

   Los emisores de llamadas de confianza incluyen a todas las personas a las que se les otorgó permiso para llamar a la red privada.

2. **Asigne a cada usuario un secreto de CHAP.**

   Nota - Asegúrese de elegir un buen secreto de CHAP que no sea fácil de adivinar. No hay ninguna otra restricción en el contenido del secreto de CHAP.

   El método para asignar secretos de CHAP depende de la política de seguridad del sitio. O bien, se tiene la responsabilidad de crear los secretos o los emisores de llamadas deben crear sus propios secretos. Si no es responsable de la asignación de secretos de CHAP, asegúrese de obtener los secretos de CHAP creados por o para emisores de llamadas de confianza.

3. **Conviértase en administrador en el servidor de marcación de entrada.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

4. **Modifique el archivo `/etc/ppp/chap-secrets`.**

   Esta versión incluye un archivo `/etc/ppp/chap-secrets` que contiene comentarios útiles, pero no contiene opciones. Puede agregar las siguientes opciones para el servidor `CallServe` al final del archivo `/etc/ppp/chap-secrets` existente.

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

   `key123` es el secreto de CHAP para emisores de llamadas de confianza `account1`.

   `key456` es el secreto de CHAP para emisores de llamadas de confianza `account2`.

Véase también La siguiente lista proporciona referencias a la información relacionada.

- Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada) [80]

Modificación de archivos de configuración de PPP para CHAP (servidor de marcación de entrada)

La tarea de esta sección explica cómo actualizar archivos de configuración de PPP existentes para admitir la autenticación CHAP en el servidor de marcación de entrada.

▼ Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (servidor de marcación de entrada)

1. **Inicie sesión en el servidor de marcación de entrada como superusuario.**

2. **Modifique el archivo `/etc/ppp/options`.**

   Agregue las opciones que se muestran en negrita para compatibilidad de CHAP.

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

`name` *CallServe*	Define *CallServe* como nombre de usuario de CHAP en la máquina local, en esta instancia, el servidor de marcación de entrada.
`auth`	Hace que el equipo local autentique a los emisores de llamadas antes de establecer el enlace.

3. **Cree el resto de los archivos de configuración de PPP para admitir a los emisores de llamadas de confianza.**

   Consulte Cómo configurar usuarios del servidor de marcación de entrada [57] y Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada) [58].

Véase también Para configurar las credenciales de autenticación CHAP para emisores de llamadas de confianza, consulte Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada) [80].

Configuración de autenticación CHAP para emisores de llamadas de confianza (equipos de marcación de salida)

Esta sección contiene tareas para configuración de la autenticación CHAP en las máquinas de marcación de salida de emisores de llamadas de confianza. En función de la política de seguridad del sitio, tanto usted como los emisores de llamadas de confianza pueden ser responsables de la configuración de autenticación CHAP.

Para que los emisores de llamadas remotos configuren CHAP, asegúrese de que los secretos de CHAP locales de los emisores coincidan con los secretos de CHAP equivalentes de los emisores de llamadas en el archivo `/etc/ppp/chap-secrets` del servidor de marcación de entrada. A continuación, proporcione a los emisores de llamadas las tareas de esta sección para la configuración de CHAP.

La configuración de CHAP para emisores de llamadas de confianza incluye dos tareas:

- Creación de credenciales de seguridad de CHAP de emisores de llamadas.
- Configuración de los equipos de marcación de salida de los emisores de llamadas para admitir autenticación CHAP.

▼ Cómo configurar credenciales de autenticación CHAP para los emisores de llamadas de confianza

Este procedimiento muestra cómo configurar credenciales de CHAP para dos emisores de llamadas de confianza. Los pasos del procedimiento dan por sentado que usted, el administrador del sistema, crea las credenciales de CHAP en los equipos de marcación de salida de emisores de llamadas de confianza.

1. **Conviértase en administrador en el equipo de marcación de salida.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.
   Con el ejemplo de configuración de CHAP en “Ejemplo de una configuración mediante autenticación CHAP” [40], asuma que el equipo de marcación de salida pertenece a un emisor de llamada de confianza `account1`.

2. **Modifique la base de datos chap-secrets para el emisor de llamada `account1`.**
   Esta versión incluye un archivo `/etc/ppp/chap-secrets` que contiene comentarios útiles, pero no contiene opciones. Puede agregar las siguientes opciones al archivo `/etc/ppp/chap-secrets` existente.

   ```
   account1  CallServe   key123   *
   ```

`CallServe` es el nombre del par que `account1` está intentando alcanzar. `key123` es el secreto de CHAP que se utilizará para enlaces entre `account1` y `CallServer`.

3. **Conviértase en administrador en el equipo de marcación de salida.**
   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

   Asuma que este equipo pertenece al emisor de llamada `account2`.

4. **Modifique la base de datos `/etc/ppp/chap-secrets` para el emisor de llamada account2.**

   ```
   account2  CallServe   key456   *
   ```

   Ahora, `account2` tiene el secreto `key456` como sus credenciales de CHAP para utilizar a través de enlaces con el par `CallServe`.

Véase también La siguiente lista proporciona referencias a la información relacionada.

- Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada) [80]
- Cómo configurar credenciales de autenticación CHAP para los emisores de llamadas de confianza [82]

Agregación de CHAP para los archivos de configuración (equipo de marcación de salida)

Para obtener más información sobre la autenticación CHAP, consulte "Protocolo de autenticación por desafío mutuo (CHAP)" [139]. La siguiente tarea configura el equipo de marcación de salida que pertenece al emisor de llamada `account1`, que se presenta en "Ejemplo de una configuración mediante autenticación CHAP" [40].

▼ Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (equipo de marcación de salida)

1. **Inicie sesión en el equipo de marcación de salida como superusuario.**

2. **Asegúrese de que el archivo `/etc/ppp/options` tenga las siguientes opciones.**

   ```
   # cat /etc/ppp/options
   ```

```
lock
nodefaultroute
```

3. **Cree un archivo `/etc/ppp/peers/`*peer-name* para la máquina remota `CallServe`.**

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

La opción `user account1` establece `account1` como nombre de usuario de CHAP que se otorgará a `CallServe`. Para obtener una descripción de las otras opciones en el archivo anterior, consulte el archivo similar `/etc/ppp/peers/myserver` en Cómo definir la conexión con un par individual [53].

Véase también Para probar la autenticación CHAP mediante una llamada al servidor de marcación de entrada, consulte Cómo llamar al servidor de marcación de entrada [60].

♦ ♦ ♦ CAPÍTULO 6

Configuración de un túnel de PPP a través de Ethernet

Este capítulo contiene tareas para configurar los participantes en cualquiera de los extremos del túnel PPPoE: el cliente PPPoE y el servidor de acceso PPPoE. Los temas específicos incluyen lo siguiente:

- “Tareas principales para la configuración de un túnel PPPoE (mapas de tareas)” [85]
- “Configuración del cliente PPPoE” [86]
- “Configuración de un servidor de acceso PPPoE” [89]

Las tareas utilizan el escenario que se presentó en “Planificación de compatibilidad de DSL a través de un túnel PPPoE” [42] como un ejemplo. Para obtener una descripción general de PPPoE, consulte “Compatibilidad para usuarios de DSL a través de PPPoE” [24].

Tareas principales para la configuración de un túnel PPPoE (mapas de tareas)

En las siguientes tablas, se enumeran las tareas principales para la configuración de clientes PPPoE y el servidor de acceso PPPoE. Para implementar PPPoE en su sitio, necesita configurar sólo el extremo de su túnel PPPoE, ya sea el lado del cliente o del servidor de acceso.

TABLA 6-1 Mapa de tareas para configuración de un cliente PPPoE

Tarea	Descripción	Para obtener instrucciones
1. Configurar una interfaz para PPPoE	Definir la interfaz Ethernet que se utilizará para el túnel PPPoE.	Cómo configurar una interfaz para un cliente PPPoE [87]
2. Configurar la información sobre el servidor de acceso PPPoE	Definir los parámetros para el servidor de acceso en el extremo del proveedor de servicios del túnel PPPoE.	Cómo definir un par de servidor de acceso PPPoE [87]
3. Configurar los archivos de configuración de PPP	Definir los archivos de configuración de PPP para el cliente, si no lo ha hecho aún.	Cómo definir comunicaciones a través de la línea de serie [51]

Tarea	Descripción	Para obtener instrucciones
4. Crear el túnel	Llamar al servidor de acceso.	Cómo definir un par de servidor de acceso PPPoE [87]

TABLA 6-2 Mapa de tareas para configuración de un servidor de acceso PPPoE

Tarea	Descripción	Para obtener instrucciones
1. Configurar un servidor de acceso PPPoE	Definir la interfaz Ethernet que se utilizará para el túnel PPPoE y definir los servicios que ofrece el servidor de acceso.	Cómo configurar un servidor de acceso PPPoE [89]
2. Configurar los archivos de configuración de PPP	Definir los archivos de configuración de PPP para el cliente, si no lo ha hecho aún.	"Configuración de comunicaciones a través del servidor de marcación de entrada" [58]
3. (Opcional) Limitar el uso de una interfaz	Usar las opciones de PPPoE y autenticación PAP para restringir el uso de una interfaz Ethernet en particular para determinados clientes.	Cómo restringir el uso de una interfaz a clientes específicos [91]

Configuración del cliente PPPoE

Para proporcionar PPP a sistemas cliente a través de DSL, primero debe configurar PPPoE en la interfaz que está conectada al módem o concentrador. Luego necesita cambiar los archivos de configuración de PPP para definir el servidor de acceso en el extremo opuesto de PPPoE.

Requisitos previos para la configuración del cliente PPPoE

Antes de poder configurar el cliente PPPoE, debe haber hecho lo siguiente:

- Instalado la versión de Oracle Solaris en los equipos cliente para utilizar el túnel PPPoEl.
- Contactado al proveedor de servicios para obtener información acerca de su servidor de acceso PPPoE.
- Logrado que la compañía telefónica o el proveedor de servicios conecten los dispositivos que utilizan los equipos cliente. Esos dispositivos incluyen, por ejemplo, el módem DSL y el separador, que es posible que de eso se encargue la compañía telefónica.

▼ Cómo configurar una interfaz para un cliente PPPoE

Utilice este procedimiento para definir la interfaz Ethernet que se utilizará para el túnel PPPoE.

1. **Conviértase en administrador en el cliente PPPoE.**
   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Agregue el nombre de la interfaz Ethernet con la conexión DSL para el archivo `/etc/ppp/pppoe.if`.**
   Por ejemplo, agregue la siguiente entrada a `/etc/ppp/pppoe.if` para un cliente PPPoE que utiliza `hme0` como la interfaz de red que está conectada al módem DSL.

   ```
   hme0
   ```

   Para obtener más información sobre `/etc/ppp/pppoe.if`, vaya a "Archivo `/etc/ppp/pppoe.if`" [146].

3. **Configure la interfaz para utilizar PPPoE.**

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

4. **(Opcional) Verifique que la interfaz esté conectada para PPPoE.**

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

   También puede utilizar el comando `/usr/sbin/sppptun` para conectar manualmente interfaces para PPPoE. Para obtener instrucciones, consulte "Comando `/usr/sbin/sppptun`" [146].

▼ Cómo definir un par de servidor de acceso PPPoE

Define el servidor de acceso en el archivo `/etc/ppp/peers/`*peer-name*. Muchas de las opciones que se utilizan para el servidor de acceso también se utilizan para definir el servidor de marcación de entrada en un escenario de marcación telefónica. Para obtener una explicación detallada de `/etc/ppp/peers.`*peer-name*, consulte "Archivo `/etc/ppp/peers/`*peer-name*" [123].

1. **Conviértase en administrador en el cliente PPPoE.**
   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Defina el servidor de acceso PPPoE del proveedor de servicios en el archivo `/etc/ppp/peers/`*peer-name*.**

   Por ejemplo, el siguiente archivo, `/etc/ppp/peers/dslserve`, define el servidor de acceso `dslserve` en Far ISP que se presenta en "Ejemplo de una configuración para un túnel PPPoE" [44].

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

   Para obtener una definición de las opciones de este archivo, vaya a "Archivo para definir un igual de servidor de acceso `/etc/ppp/peers/`*peer-name*" [153].

3. **Modifique los archivos de configuración de PPP en el cliente PPPoE.**

   a. **Configure `/etc/ppp/options` como se describe en las instrucciones para la configuración de un equipo de marcación de salida en "Configuración del equipo de marcación de salida" [48].**

   b. **Cree un archivo `/etc/ppp/options.sppptun`. `/etc/ppp/options.sppptun` define opciones de PPP para el puerto de serie al cual está conectada la interfaz (la cual está conectada para PPPoE).**

      Puede utilizar cualquiera de las opciones que están disponibles para el archivo `/etc/ppp/options.`*ttyname* según lo descrito en "Archivo de configuración `/etc/ppp/options.`*ttyname*" [119]. Debe dar al archivo el nombre `/etc/ppp/options.sppptun` porque `sppptun` es el nombre de dispositivo especificado en la configuración de `pppd`.

4. **Asegúrese de que todos los usuarios puedan iniciar PPP en el cliente.**

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

5. **Pruebe si PPP puede ejecutar la línea DSL.**

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

   `dslserve` es el nombre que se asigna al servidor de acceso de ISP que se muestra en "Ejemplo de una configuración para un túnel PPPoE" [44]. La opción `debug updetach` provoca que la información de depuración se muestre en una ventana de terminal.

Si PPP se ejecuta correctamente, la salida de terminal muestra cuando el enlace se vuelve activo. Si PPP todavía no se ejecuta, intente el siguiente comando para ver si los servidores se ejecutan correctamente:

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

Nota - Los usuarios de clientes PPPoE configurados pueden iniciar la ejecución de PPP a través de una línea DSL al escribir lo siguiente:

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

Entonces los usuarios pueden ejecutar una aplicación o un servicio.

Véase también La siguiente lista proporciona referencias a la información relacionada.

- Consulte “Configuración del cliente PPPoE” [86].
- Consulte “Creación de túneles PPPoE para compatibilidad de DSL” [145].
- Consulte el Capítulo 7, Resolución de problemas comunes del protocolo punto a punto.
- Consulte “Configuración de un servidor de acceso PPPoE” [89].

Configuración de un servidor de acceso PPPoE

Si su compañía es un proveedor de servicios, puede ofrecer Internet y otros servicios a los clientes que lleguen a su sitio mediante conexiones DSL. El procedimiento implica determinar qué interfaces en el servidor deben formar parte del túnel PPPoE y definir qué servicios estarán disponibles para los usuarios.

▼ Cómo configurar un servidor de acceso PPPoE

Utilice este procedimiento para definir la interfaz Ethernet que se utilizará para el túnel PPPoE y para configurar los servicios que ofrece el servidor de acceso.

1. **Conviértase en administrador en el servidor de acceso.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Agregue el nombre de las interfaces Ethernet dedicadas a los túneles PPPoE para el archivo `/etc/ppp/pppoe.if`.**
   Por ejemplo, debe utilizar el siguiente archivo `/etc/ppp/pppoe.if` para el servidor de acceso `dslserve` que se muestra en “Ejemplo de una configuración para un túnel PPPoE” [44].

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

```
hme1
hme2
```

3. **Defina los servicios globales que proporciona el servidor de acceso en el archivo `/etc/ppp/pppoe`.**

   El siguiente archivo `/etc/ppp/pppoe` enumera los servicios que proporciona el servidor de acceso `dslserve`, que se mostró en la Figura 2-5, “Ejemplo de un túnel PPPoE”.

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

   En el ejemplo de archivo, el servicio de Internet se anuncia para las interfaces Ethernet de `dslserve` `hme1` y `hme2`. La depuración está activada para enlaces de PPP en las interfaces Ethernet.

4. **Configure los archivos de configuración de PPP de la misma manera que lo haría para un servidor de marcación de entrada.**

   Para obtener más información, consulte “Creación de un esquema de direccionamiento IP para emisores de llamadas” [142].

5. **Inicie el daemon `pppoed`.**

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

   `pppd` también conecta las interfaces que se enumeran en `/etc/ppp/pppoe.if`.

6. **(Opcional) Verifique que las interfaces en el servidor estén conectadas para PPPoE.**

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

   El ejemplo anterior muestra que las interfaces `hme1` y `hme2` están conectadas para PPPoE. También puede utilizar el comando `/usr/sbin/sppptun` para conectar manualmente interfaces para PPPoE. Para obtener instrucciones, consulte “Comando `/usr/sbin/sppptun`” [146].

▼ Cómo modificar un archivo `/etc/ppp/pppoe` existente

1. **Conviértase en administrador en el servidor de acceso.**

Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Modifique `/etc/ppp/pppoe`, según sea necesario.**

3. **Haga que el daemon `pppoed` reconozca los nuevos servicios.**

```
# pkill -HUP pppoed
```

Cómo restringir el uso de una interfaz a clientes específicos

El siguiente procedimiento muestra cómo restringir una interfaz a un grupo de clientes PPPoE. Antes de realizar esta tarea, debe obtener las direcciones MAC Ethernet reales de los clientes a los que les asigna la interfaz.

Nota - Algunos sistemas le permiten cambiar la dirección MAC de la interfaz Ethernet. Debe considerar esta capacidad como una comodidad, no como una medida de seguridad.

En el ejemplo que se muestra en “Ejemplo de una configuración para un túnel PPPoE” [44], se muestran los pasos sobre cómo reservar una de las interfaces `dslserve`, `hme1`, para clientes en MiddleCo.

1. **Configure la interfaz del servidor de acceso y defina los servicios, como se muestra en Cómo configurar un servidor de acceso PPPoE [89].**

2. **Cree entradas para los clientes en la base de datos `/etc/ethers` del servidor.**

   A continuación, se muestra una entrada para clientes Rojo, Azul, Amarillo.

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

   El ejemplo asigna los nombres simbólicos `redether`, `yellowether` y `blueether` para las direcciones Ethernet de clientes Rojo, Amarillo y Azul. La asignación de nombres simbólicos para las direcciones MAC es opcional.

3. **Restrinja los servicios que se proporcionan en una interfaz específica definiendo la siguiente información en el archivo `/etc/ppp/pppoe.`*device*.**

   En este archivo, *dispositivo* es el nombre del dispositivo que se va a definir.

```
# cat /etc/ppp/pppoe.hme1
service internet
     pppd "name dslserve-hme1"
```

```
clients redether,yellowether,blueether
```

`dslserve-hme1` es el nombre del servidor de acceso, que se utiliza para hacer coincidir entradas en el archivo `pap-secrets`. La opción `clients` restringe el uso de la interfaz `hme1` a los clientes con los nombres Ethernet simbólicos `redether`, `yellowether` y `blueether`.

Si no definió nombres simbólicos para las direcciones MAC del cliente en `/etc/ethers`, puede utilizar las direcciones numéricas como argumentos para la opción `clients`. Se permiten comodines.

Por ejemplo, puede especificar la dirección numérica `clients 8:0:20:*:*:*`. Mediante el uso de comodines, todas las direcciones que coinciden en `/etc/ethers` son aceptadas.

4. **Cree el archivo `/etc/ppp/pap-secrets` para el servidor de acceso:**

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

Las entradas son los nombres y las contraseñas de PAP de clientes autorizados a ejecutar PPP a través de la interfaz `hme1` de `dslserve`.

Para obtener más información sobre la autenticación PAP, consulte “Configurar autenticación PAP” [70].

Véase también La siguiente lista proporciona referencias a la información relacionada.

- Para obtener más información sobre PPPoE, consulte “Creación de túneles PPPoE para compatibilidad de DSL” [145].
- Para solucionar problemas de PPPoE y PPP, consulte “Resolución de problemas relacionados con PPP y PPPoE” [97].
- Para configurar un cliente PPPoE, consulte “Configuración del cliente PPPoE” [86].
- Para configurar la autenticación PAP para un cliente, consulte “Configuración de autenticación PAP para emisores de llamadas de confianza (equipos de marcación de salida)” [75].
- Para configurar la autenticación PAP en un servidor, consulte “Configuración de autenticación PAP en el servidor de marcación de entrada” [71].

♦ ♦ ♦ CAPÍTULO 7

Resolución de problemas comunes del protocolo punto a punto

Este capítulo contiene información para solucionar problemas comunes que se producen con Solaris PPP 4.0. Se tratan los temas siguientes:

- “Herramientas para resolución de problemas de PPP” [94]
- “Resolución de problemas relacionados con PPP y PPPoE” [97]
- “Resolución de problemas de línea arrendada” [110]
- “Diagnóstico y resolución de problemas de autenticación” [110]

Las fuentes *PPP Design, Implementation, and Debugging* por James Carlson y el sitio web de la Universidad Nacional de Australia (ANU, Australian National University) también detallan sugerencias para la resolución de problemas de PPP. Para obtener más información, consulte “Manuales de referencia profesional sobre PPP” [15].

Resolución de problemas de PPP (mapa de tareas)

Utilice el siguiente mapa de tareas para acceder rápidamente a sugerencias y resolución de problemas de PPP comunes.

TABLA 7-1 Mapa de tareas para resolución de problemas de PPP

Tarea	Definición	Para obtener instrucciones
Obtener información de diagnóstico sobre el enlace de PPP	Utilizar herramientas de diagnóstico de PPP para obtener resultados para la resolución de problemas.	Cómo obtener información de diagnóstico desde `pppd` [95]
Obtener información de depuración para el enlace de PPP	Utilizar el comando `pppd debug` con el fin de generar un resultado para la resolución de problemas.	Cómo activar la depuración de PPP [96]
Solucionar problemas generales con la capa de red	Identificar y solucionar problemas de PPP relacionados con la red mediante una serie de comprobaciones.	Cómo diagnosticar problemas de red [98]

Tarea	Definición	Para obtener instrucciones
Solucionar problemas de comunicaciones generales	Identificar y solucionar problemas de comunicaciones que afectan al enlace de PPP.	Cómo diagnosticar y solucionar problemas de comunicaciones [100]
Solucionar problemas de configuración	Identificar y solucionar problemas en los archivos de configuración de PPP.	Cómo diagnosticar problemas con la configuración de PPP [102]
Solucionar problemas relacionados con el módem	Identificar y corregir problemas del módem.	Cómo diagnosticar problemas del módem [103]
Solucionar problemas relacionados con la secuencia de comandos de chat	Identificar y solucionar problemas de la secuencia de comandos de chat en un equipo de marcación de salida.	Cómo obtener información de depuración para secuencias de comandos de chat [104]
Solucionar problemas de velocidad de la línea de serie	Identificar y solucionar problemas de velocidad de la línea en un servidor de marcación de entrada.	Cómo diagnosticar y solucionar problemas de velocidad de línea de serie [106]
Solucionar problemas comunes de las líneas arrendadas	Identificar y solucionar los problemas de rendimiento de una línea arrendada.	“Resolución de problemas de línea arrendada” [110]
Solucionar problemas relacionados con la autenticación	Identificar y solucionar problemas relacionados con las bases de datos de autenticación.	“Diagnóstico y resolución de problemas de autenticación” [110]
Solucionar problemas de áreas para PPPoE	Utilizar herramientas de diagnóstico de PPP para obtener una solución para identificar y solucionar problemas de PPPoE.	Cómo obtener información de diagnóstico para PPPoE [107]

Herramientas para resolución de problemas de PPP

Los enlaces de PPP generalmente tienen tres áreas principales de fallo:

- Fallo del enlace que se establecerá
- Bajo rendimiento del enlace durante el uso regular
- Problemas que pueden rastrearse en las redes en cualquier lado del enlace

La manera más sencilla de averiguar si PPP funciona es ejecutar un comando a través del enlace. Ejecute un comando como `ping` o `traceroute` para un host en la red del par. A continuación, observe los resultados. Sin embargo, debe utilizar herramientas de depuración de PPP y UNIX para supervisar el rendimiento de un enlace establecido o para solucionar un enlace problemático.

Esta sección explica cómo obtener información de diagnóstico de `pppd` y sus archivos log asociados. El resto de las secciones de este capítulo describen problemas habituales con PPP

que puede detectar y solucionar con la ayuda de las herramientas de resolución de problemas de PPP.

▼ Cómo obtener información de diagnóstico desde pppd

El siguiente procedimiento muestra cómo visualizar la operación actual de un enlace en el equipo local.

1. **Conviértase en administrador en el equipo local.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Ejecute `pppd` con el dispositivo serie configurado para PPP como el argumento:**

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

   Los siguientes ejemplos muestran las pantallas que se obtienen como resultado de un enlace por marcación telefónica y un enlace de línea arrendada cuando `pppd` se ejecuta en primer plano. Si ejecuta `pppd debug` en segundo plano, el resultado que se obtiene se envía al archivo `/etc/ppp/connect-errors`.

ejemplo 7-1 Resultado de un enlace por marcación telefónica que funciona correctamente

```
# 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
```

ejemplo 7-2 Resultado de un enlace de línea arrendada que funciona correctamente

```
# 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
```

▼ Cómo activar la depuración de PPP

La siguiente tarea muestra cómo utilizar el comando `pppd` para obtener información de depuración.

Nota - Sólo necesita realizar del paso 1 al paso 3 una vez para cada host. A partir de ese momento, puede continuar con el paso 4 para activar la depuración para el host.

1. **Conviértase en administrador.**

Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Cree un archivo log para mantener las salidas de `pppd`.**

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

3. **Agregue las siguientes utilidades `syslog` para `pppd` en `/etc/syslog.conf`.**

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

4. **Reinicie `syslogd`.**

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

5. **Active la depuración para llamadas a un igual específico mediante la siguiente sintaxis de `pppd`.**

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

peer-name debe ser el nombre de un archivo en el directorio`/etc/ppp/peers`.

6. **Visualice los contenidos del archivo log.**

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

Para obtener un ejemplo de un archivo log, consulte el Paso 3.

Resolución de problemas relacionados con PPP y PPPoE

Consulte las siguientes secciones para obtener información sobre cómo resolver problemas relacionados con PPP y PPPoE.

▼ Cómo diagnosticar problemas de red

Si el enlace de PPP pasa a ser activo pero sólo se puede establecer contacto con pocos hosts remotos, se puede tratar de un problema de red. El siguiente procedimiento le muestra cómo aislar y solucionar problemas de red que afectan a un enlace de PPP.

1. **Conviértase en administrador en el equipo local.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Cierre el enlace problemático.**

3. **Desactive cualquier protocolo opcional en los archivos de configuración agregando las siguientes opciones para la configuración de PPP:**

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

   Estas opciones proporcionan el PPP no comprimido más simple que está disponible. Intente invocar estas opciones como argumentos para `pppd` en la línea de comandos. Si puede acceder a hosts que antes eran inaccesibles, agregue las opciones en cualquiera de las siguientes ubicaciones.

   - `/etc/ppp/peers/`*nombre de par*, después de la opción `call`
   - `/etc/ppp/options` y asegúrese de que las opciones se apliquen globalmente

4. **Llame al par remoto. A continuación, active las funciones de depuración.**

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

5. **Obtenga logs detallados del programa de chat mediante la opción `-v` de `chat`.**

   Por ejemplo, utilice el siguiente formato en cualquier archivo de configuración de PPP:

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

   /etc/ppp/chatfile representa el nombre del archivo de chat.

6. **Intente recrear el problema mediante Telnet u otras aplicaciones para llegar a los hosts remotos.**

   Observe los logs de depuración. Si aún no puede alcanzar los hosts remotos, es posible que el problema de PPP esté relacionado con la red.

7. **Verifique que las direcciones IP de los hosts remotos sean direcciones de Internet registradas.**

   Algunas organizaciones asignan direcciones IP internas que son conocidas en la red local, pero que no se pueden enrutar a Internet. Si los hosts remotos se encuentran dentro de la compañía,

debe configurar un servidor de traducción de dirección de red (NAT) o servidor proxy para acceder a Internet. Si los hosts remotos no están en la compañía, debe informar el problema a la organización remota.

8. **Examine las tablas de enrutamiento.**

   a. **Compruebe las tablas de enrutamiento en el equipo local y en el par.**

   b. **Compruebe las tablas de enrutamiento de cualquier enrutador que se encuentre en la ruta desde el par hasta el servidor remoto. Compruebe también las tablas de enrutamiento de cualquier enrutador que se encuentre en la ruta de retorno al par.**

      Asegúrese de que los enrutadores intermedios no se hayan configurado incorrectamente. Con frecuencia el problema se encuentra en la ruta de retorno al par.

9. **(Opcional) Si el equipo es un enrutador, compruebe las características opcionales.**

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

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

   En la versión Solaris 10, puede usar `routeadm`(1M), en lugar de `ndd`(1M).

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

   Nota - El comando `ndd` no es persistente. Los valores establecidos con este comando se pierden cuando el sistema se reinicia. El comando `routeadm` es persistente. Los valores establecidos con este comando se mantienen después de que se reinicia el sistema.

10. **Compruebe las estadísticas que se obtienen de `netstat -s` y herramientas similares.**

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

    a. **Ejecute estadísticas en el equipo local.**

    b. **Llame al par.**

    c. **Observe las nuevas estadísticas generadas por `netstat -s`.**

       Para obtener más información, consulte “Problemas de red comunes que afectan el PPP” [100].

11. **Compruebe la configuración de DNS.**

Una configuración de servicio de nombres defectuosa hace que las aplicaciones fallen porque no se pueden resolver direcciones IP.

Problemas de red comunes que afectan el PPP

Puede utilizar los mensajes que genera `netstat -s` para solucionar los problemas de red que se muestran en la siguiente tabla. Para obtener información de procedimiento relacionada, consulte Cómo diagnosticar problemas de red [98].

TABLA 7-2 Problemas de red comunes que afectan el PPP

Mensaje	Problema	Solución
`Paquetes IP no reenviables`	Falta una ruta en el host local.	Agregue la ruta faltante a las tablas de enrutamiento del host local.
`Destino de entrada de ICMP inaccesible`	Falta una ruta en el host local.	Agregue la ruta faltante a las tablas de enrutamiento del host local.
`Tiempo de ICMP superado`	Dos enrutadores se envían la misma dirección de destino a cada uno, lo que provoca que el paquete vaya y vuelva hasta que el valor de tiempo de actividad (TTL) se excede.	Utilice `traceroute` para averiguar el origen del bucle de enrutamiento y, a continuación, póngase en contacto con el administrador del enrutador que presenta el error. Para obtener información sobre `traceroute`, consulte la página del comando man `traceroute`(1M).
`Paquetes IP no reenviables`	Falta una ruta en el host local.	Agregue la ruta faltante a la tabla de enrutamiento del host local.
`Destino de entrada de ICMP inaccesible`	Falta una ruta en el host local.	Agregue la ruta faltante a las tablas de enrutamiento del host local.

▼ Cómo diagnosticar y solucionar problemas de comunicaciones

Los problemas de comunicaciones se producen cuando los dos pares no pueden establecer un enlace correctamente. Algunas veces, estos problemas son, en realidad, problemas de negociación causados por secuencias de comandos de chat configuradas incorrectamente. El siguiente procedimiento muestra cómo solucionar problemas de comunicación. Para solucionar problemas de negociación causados por una secuencia de comandos de chat defectuosa, consulte la Tabla 7-5, “Problemas de secuencia de comandos de chat comunes”.

1. **Conviértase en administrador en el equipo local.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Llame al par.**

3. **Llame al par remoto. A continuación, active las funciones de depuración.**

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

Es posible que necesite obtener información de depuración del par para solucionar determinados problemas de comunicaciones.

4. **Compruebe los logs resultantes para problemas de comunicación. Para obtener más información, consulte "Problemas de comunicaciones generales que afectan PPP" [101].**

Problemas de comunicaciones generales que afectan PPP

La siguiente tabla describe síntomas que están relacionados con la salida del log del procedimiento, Cómo diagnosticar y solucionar problemas de comunicaciones [100].

TABLA 7-3 Problemas de comunicaciones generales que afectan PPP

Síntoma	Problema	Solución
`demasiadas Configure-Requests`	Un par no puede escuchar a otro par.	Compruebe si se presentan los siguientes problemas: ■ El equipo o el módem pueden tener un cableado defectuoso. ■ Es posible que la configuración del módem tenga valores de bit incorrectos. O bien, es posible que la configuración haya afectado al control de flujo. ■ Es posible que se haya producido un fallo en la secuencia de comandos de chat. En esta situación, consulte la Tabla 7-5, "Problemas de secuencia de comandos de chat comunes".
El resultado `pppd debug` muestra que LCP se inicia, pero hay fallas en protocolos de alto nivel o se muestran errores de CRC.	El mapa de caracteres de control asíncrono (ACCM) se estableció de manera incorrecta.	Utilice la opción `default-async` para establecer ACCM según los valores predeterminados estándar de FFFFFFFF. Primero, intente usar `default-async` como una opción para `pppd` en la línea de comandos. Si el problema se soluciona, agregue `default-async` a `/etc/ppp/options` o a `/etc/ppp/peers/`*nombre de par* después de la opción de llamada.
El resultado `pppd debug` muestra que IPCP se inicia, pero finaliza inmediatamente.	Las direcciones IP pueden estar configuradas de forma incorrecta.	1. Compruebe la secuencia de comandos de chat para verificar si la secuencia de comandos tiene direcciones IP incorrectas. 2. Si la secuencia de comandos de chat es correcta, solicite logs de depuración para el par y compruebe las direcciones IP en los logs del par.
El enlace muestra un rendimiento muy bajo.	El módem podría estar configurado de manera	Compruebe la configuración del módem. Ajuste la configuración si es necesario.

Síntoma	Problema	Solución
	incorrecta, con errores de configuración de control de flujo, errores de configuración de módem y tasas DTE configuradas de manera incorrecta.	

▼ Cómo diagnosticar problemas con la configuración de PPP

Algunos problemas de PPP se pueden rastrear en problemas de archivos de configuración de PPP. El siguiente procedimiento muestra cómo aislar y solucionar problemas de configuración generales.

1. **Conviértase en administrador en el equipo local.**

   Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

2. **Llame al par remoto. A continuación, active las funciones de depuración.**

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

3. **Compruebe el log resultante para problemas de comunicación. Para obtener más información, consulte "Problemas de configuración de PPP comunes" [102].**

Problemas de configuración de PPP comunes

La siguiente tabla describe síntomas que están relacionados con la salida del log del procedimiento, Cómo diagnosticar problemas con la configuración de PPP [102].

TABLA 7-4 Problemas de configuración de PPP comunes

Síntoma	Problema	Solución
El resultado `pppd debug` contiene el mensaje de error `Could not determine remote IP address`.	El archivo `/etc/ppp/peers/`*peer-name* no tiene una dirección IP para el par. El par no proporciona una dirección IP durante la negociación del enlace.	Proporcione una dirección IP para el par en la línea de comando pppd o en `/etc/ppp/peers/`*peer-name* con el siguiente formato: :10.0.0.10
El resultado `pppd debug` muestra que falló la compresión de datos de CCP.	Es posible que las configuraciones de compresión de PPP de los pares estén en conflicto.	Desactive la compresión de CCP agregando la opción `noccp` a `/etc/ppp/options` en uno de los pares.

Síntoma	Problema	Solución
El resultado también indica que el enlace está caído.		

▼ Cómo diagnosticar problemas del módem

Los módems pueden ser áreas de problemas principales para un enlace de acceso telefónico. El indicador más común de problemas con la configuración del módem es cuando no hay respuesta del par. Sin embargo, es posible que tenga dificultades para determinar si un problema de enlace es en realidad el resultado de problemas de configuración del módem.

La documentación y los sitios web de los fabricantes de módems contienen soluciones para problemas de sus respectivos equipos. El siguiente procedimiento ayuda a determinar si una configuración de módem defectuosa causa problemas de enlace.

1. **Llame al par con la depuración activada, como se explica en Cómo activar la depuración de PPP [96].**

2. **Muestre el registro `/var/log/pppdebug` resultante para la configuración defectuosa de un módem.**

3. **Utilice `ping` para enviar paquetes de distintos tamaños a través del enlace.**

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

   Si se reciben paquetes pequeños, pero se descartan paquetes más grandes, se indican problemas del módem.

4. **Compruebe la existencia de errores en la interfaz `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 los errores de interfaz se incrementan con el tiempo, es posible que haya problemas en la configuración del módem.

Errores más frecuentes

Cuando se muestra el registro `/var/log/pppdebug` resultante, los siguientes síntomas en el resultado pueden indicar una configuración de módem defectuosa. El equipo local puede escuchar al par, pero el par no puede escuchar al equipo local.

- No se recibió ningún mensaje "`recvd`" del par.
- El resultado contiene mensajes de LCP del par, pero el enlace falla con mensajes `too many LCP Configure Requests` que se envían mediante el equipo local.

- El enlace finaliza con una señal SIGHUP.

▼ Cómo obtener información de depuración para secuencias de comandos de chat

Utilice el siguiente procedimiento para obtener información de depuración de `chat` y sugerencias para solucionar problemas comunes. Para obtener más información, consulte “Problemas de secuencia de comandos de chat comunes” [104].

1. **Conviértase en administrador en el equipo de marcación de salida.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Edite el archivo `/etc/ppp/peers/`*peer-name* para el par al que se debe llamar.**

3. **Agregue `-v` como un argumento para el comando `chat` que se especifica en `connect`.**

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

4. **Visualice errores de secuencia de comandos de chat en el archivo `/etc/ppp/connect-errors`.**

   A continuación, se muestra el principal error que se produce con `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
   ```

   En el ejemplo se muestra el tiempo de espera mientras se aguarda una cadena `(CONNECT)`. Cuando `chat` falla, obtendrá el siguiente mensaje de `pppd`:

   ```
   Connect script failed
   ```

Problemas de secuencia de comandos de chat comunes

Las secuencias de comandos de chat son áreas propensas a errores para enlaces por marcación telefónica. La siguiente tabla muestra errores de secuencia de comandos de chat comunes y proporciona sugerencias para solucionar los errores. Para obtener información de procedimiento, consulte Cómo obtener información de depuración para secuencias de comandos de chat [104].

TABLA 7-5 Problemas de secuencia de comandos de chat comunes

Síntoma	Problema	Solución
El resultado `pppd debug` contiene `Connect script failed`	La secuencia de comandos de chat proporciona un nombre de usuario y una contraseña. `ogin:` *user-name* `ssword:` *password* Sin embargo, el par al que intentó conectarse no muestra esta información.	1. Elimine el inicio de sesión y la contraseña de la secuencia de comandos de chat. 2. Intente llamar al par nuevamente. 3. Si sigue recibiendo el mensaje, llame al ISP. Pida al ISP la secuencia de inicio de sesión correcta.

El registro `/usr/bin/chat -v` contiene `"expect (login:)" alarm read timed out`	La secuencia de comandos de chat proporciona un nombre de usuario y una contraseña.
	
	`ogin: pppuser`
	`ssword: \q\U`
	
	Sin embargo, el par al que intenta conectarse no muestra esta información.
		1. Elimine el inicio de sesión y la contraseña de la secuencia de comandos de chat.
		2. Intente llamar al par nuevamente.
		3. Si sigue recibiendo el mensaje, llame al ISP. Pida al ISP la secuencia de inicio de sesión correcta.

La salida de `pppd debug` contiene `possibly looped-back`	El equipo local o su par está bloqueado en la línea de comandos y no ejecuta PPP. Un nombre de inicio de sesión y una contraseña están configurados incorrectamente en la secuencia de comandos de chat.	1. Elimine el inicio de sesión y la contraseña de la secuencia de comandos de chat. 2. Intente llamar al par nuevamente. 3. Si sigue recibiendo el mensaje, llame al ISP. Solicite la secuencia de inicio de sesión correcta.
El resultado `pppd debug` muestra que se activa LCP, pero finaliza al poco tiempo de su activación.	Es posible que la contraseña en la secuencia de comandos de chat sea incorrecta.	1. Asegúrese de que tiene la contraseña correcta para el equipo local. 2. Compruebe la contraseña en la secuencia de comandos de chat. Corrija la contraseña si es incorrecta. 3. Intente llamar al par nuevamente. 4. Si sigue recibiendo el mensaje, llame al ISP. Pida al ISP la secuencia de inicio de sesión correcta.

El texto del par comienza con una tilde (~).	La secuencia de comandos de chat proporciona un nombre de usuario y una contraseña.
	
	`ogin: pppuser`
	`ssword: \q\U`
	
	Sin embargo, el par al que intenta conectarse no muestra esta información.
		1. Elimine el inicio de sesión y la contraseña de la secuencia de comandos de chat.
		2. Intente llamar al par nuevamente.
		3. Si sigue recibiendo el mensaje, llame al ISP. Solicite la secuencia de inicio de sesión correcta.

El módem se bloquea.	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje `CONNECT` del par:	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del par:

Síntoma	Problema	Solución
	`CONNECT ”`	`CONNECT \c` Finalice la secuencia de comandos de chat con `~ \c`.
El resultado `pppd debug` contiene `LCP: timeout sending Config-Requests`	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje `CONNECT` del par: `CONNECT ”`	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del par: `CONNECT \c` Finalice la secuencia de comandos de chat con `~ \c`.
El resultado `pppd debug` contiene `El enlace de serie no es de 8 bits`	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje `CONNECT` del par: `CONNECT ”`	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del par: `CONNECT \c` Finalice la secuencia de comandos de chat con `~ \c`.
El resultado `pppd debug` contiene `Loopback detected`	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje `CONNECT` del par: `CONNECT ”`	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del par: `CONNECT \c` Finalice la secuencia de comandos de chat con `~ \c`.
El resultado `pppd debug` contiene `SIGHUP`	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje `CONNECT` del par: `CONNECT ”`	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del par: `CONNECT \c` Finalice la secuencia de comandos de chat con `~ \c`.

▼ Cómo diagnosticar y solucionar problemas de velocidad de línea de serie

Es posible que los servidores de marcación de entrada tengan problemas debido a una configuración de velocidad conflictiva. El siguiente procedimiento lo ayuda a aislar la causa del problema de enlace para velocidades de línea de serie conflictivas.

Los siguientes comportamientos provocan problemas de velocidad:

- Invocó PPP a través de un programa, como `/bin/login`, y especificó la velocidad de la línea.
- Inició PPP desde `mgetty` y accidentalmente proporcionó la tasa de bits.

pppd cambia la velocidad que se estableció originalmente para la línea por la velocidad establecida por `/bin/login` o `mgetty`. Como resultado, la línea falla.

1. **Inicie sesión en el servidor de marcación de entrada. Llame al par con la depuración activada.**
   Si necesita instrucciones, consulte Cómo activar la depuración de PPP [96].

2. **Visualice el registro `/var/log/pppdebug` resultante.**
   Compruebe el resultado del siguiente mensaje:

   ```
   LCP too many configure requests
   ```

   Este mensaje indica que las velocidades de las líneas de serie que se configuraron para PPP podrían estar en conflicto.

3. **Compruebe si PPP se invoca a través de un programa, como `/bin/login`, y la velocidad de línea que se estableció.**
   En esta situación, `pppd` cambia la velocidad de línea que se configuró originalmente por la velocidad especificada en `/bin/login`.

4. **Compruebe si un usuario inició PPP desde el comando `mgetty` y especificó accidentalmente una tasa de bits.**
   Esta acción también hace que las velocidades de línea de serie entren en conflicto.

5. **Solucione el problema de velocidad de línea de serie conflictiva como se indica a continuación:**

   a. **Bloquee la velocidad DTE del módem.**

   b. **No utilice velocidades automáticas.**

   c. **No cambie la velocidad de línea después de la configuración.**

▼ Cómo obtener información de diagnóstico para PPPoE

Puede utilizar PPP y utilidades UNIX estándar para identificar problemas de PPPoE. Cuando sospecha que PPPoE es la causa de los problemas de un enlace, utilice las siguientes herramientas de diagnóstico para obtener información de resolución de problemas.

1. **Conviértase en superusuario en el equipo que ejecuta el túnel PPPoE, ya sea cliente PPPoE o servidor de acceso PPPoE.**

2. **Active la depuración, como se explica en el procedimiento Cómo activar la depuración de PPP [96].**

3. **Visualice el contenido del archivo log `/var/log/pppdebug`.**

   En el siguiente ejemplo, se muestra parte de un archivo log que se generó para un enlace con un túnel 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 salida de la depuración no lo ayuda a aislar el problema, continúe con este procedimiento.

4. **Obtenga mensajes de diagnóstico de PPPoE.**

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

   `pppoec` envía información de diagnóstico a `stderr` . Si ejecuta `pppd` en primer plano, se muestra un resultado en la pantalla. Si `pppd` se ejecuta en segundo plano, el resultado se envía a `/etc/ppp/connect-errors`.

   En el siguiente ejemplo, se muestran los mensajes que se generan al negociar el túnel 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 los mensajes de diagnóstico no lo ayudan a aislar el problema, continúe con este procedimiento.

5. Ejecute `snoop`. A continuación, guarde el rastreo en un archivo.

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

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

6. Visualice el archivo de rastreo `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
```

Resolución de problemas de línea arrendada

El problema más común con las líneas arrendadas es el bajo rendimiento. En la mayoría de los casos, necesita trabajar con la compañía telefónica para solucionar el problema.

TABLA 7-6 Problemas comunes de línea arrendada

Síntoma	Problema	Solución
El enlace no se inicia.	Esto se puede deber a violaciones bipolares de CSU (CSU BPV). Uno de los extremos del enlace está configurado para líneas AMI. El otro extremo está configurado para sustitución bipolar de 8 ceros (B8Zs) ESF.	Si reside en los Estados Unidos o en Canadá, puede solucionar directamente este problema desde el menú de CSU/DSU. Consulte la documentación del fabricante de CSU/DSU para obtener detalles. En otras configuraciones regionales, es posible que el proveedor sea el responsable de solucionar CSU BPVs.
El enlace tiene un bajo rendimiento.	El resultado `pppd debug` muestra errores de CRC cuando el tráfico sostenido está en el enlace. Es posible que la línea tenga problemas de sincronización a causa de configuraciones incorrectas entre la compañía telefónica y la red.	Póngase en contacto con la compañía telefónica para asegurarse de que la "sincronización de bucle" esté en uso. En algunas líneas arrendadas no estructuradas, es posible que tenga que proporcionar la sincronización. Los usuarios de Estados Unidos deben utilizar la sincronización de bucle.

Diagnóstico y resolución de problemas de autenticación

La siguiente tabla describe soluciones para problemas de autenticación generales.

TABLA 7-7 Problemas de autenticación generales

Síntoma	Problema	Solución
El resultado `pppd debug` muestra el mensaje `Peer is not authorized to use remote address` *dirección*.	Utiliza autenticación PAP y la dirección IP para el par remoto no está en el archivo `/etc/ppp/pap-secrets`.	Agregue un asterisco (*) después de la entrada para el par en el archivo `/etc/ppp/pap-secrets`.
El resultado `pppd debug` muestra que LCP se inicia, pero finaliza su actividad al poco tiempo de su inicio.	Es posible que la contraseña no sea correcta en la base de datos para un protocolo de seguridad específico.	Compruebe la contraseña para el par en el archivo `/etc/ppp/pap-secrets` o `/etc/ppp/chap-secrets`.

♦ ♦ ♦ CAPÍTULO 8

Solaris PPP 4.0 (Referencia)

Este capítulo proporciona información conceptual detallada sobre Solaris PPP 4.0. Los temas incluyen lo siguiente:

Uso de opciones de PPP en archivos y en la línea de comandos

Solaris PPP 4.0 contiene una gran cantidad de opciones, que se utilizan para definir la configuración de PPP. Estas opciones se utilizan en los archivos de configuración de PPP o en la línea de comandos, o mediante el uso de una combinación de archivos y opciones de línea de comandos. Esta sección contiene información detallada sobre el uso de opciones de PPP en archivos de configuración y como argumentos para comandos de PPP.

Dónde definir opciones de PPP

La configuración de Solaris PPP 4.0 es muy flexible. Puede definir opciones de PPP en las siguientes ubicaciones:

- Archivos de configuración de PPP

- Comandos de PPP que se emiten en la línea de comandos
- Una combinación de ambos

La siguiente tabla enumera comandos y archivos de configuración de PPP.

TABLA 8-1 Resumen de comandos y archivos de configuración de PPP

Archivo o comando	Descripción	Para obtener información
`/etc/ppp/options`	Un archivo que contiene características que se aplican de manera predeterminada a todos los enlaces de PPP del sistema, por ejemplo, si la máquina requiere que los pares se autentiquen ellos mismos. Si este archivo está ausente, no se les permite a los usuarios que no son root utilizar PPP.	"Archivo de configuración `/etc/ppp/options`" [117]
`/etc/ppp/options.`*nombre de tty*	Un archivo que describe las características de todas las comunicaciones a través del puerto de serie *ttyname*.	"Archivo de configuración `/etc/ppp/options.`*ttyname*" [119]
`/etc/ppp/peers`	Directorio que contiene, por lo general, información sobre pares con los que se conecta un equipo de marcación de salida. Los archivos de este directorio se utilizan con la opción `call` del comando `pppd`.	"Especificación de información para comunicación con el servidor de marcación de entrada" [122]
`/etc/ppp/peers/`*peer-name*	Un archivo que contiene características del par remoto *peer-name*. Las características típicas incluyen el número de teléfono del par y una secuencia de comandos de chat para la negociación del enlace con el par.	"Archivo `/etc/ppp/peers/`*peer-name*" [123]
`/etc/ppp/pap-secrets`	Un archivo que contiene las credenciales de seguridad necesarias para la autenticación Protocolo de autenticación de contraseña (PAP).	"Archivo `/etc/ppp/pap-secrets`" [136]
`/etc/ppp/chap-secrets`	Un archivo que contiene las credenciales de seguridad necesarias para la autenticación de protocolo de autenticación por desafío mutuo (CHAP).	"Archivo `/etc/ppp/chap-secrets`" [140]
`~/.ppprc`	Archivo en el directorio principal de un usuario de PPP. Se utiliza generalmente con servidores de marcación de entrada. Este archivo contiene información específica sobre la configuración de cada usuario.	"Configuración de `$HOME/.ppprc` en un servidor de marcación de entrada" [121]
`pppd` *options*	Comando y opciones para iniciar un enlace de PPP y describir sus características.	"Cómo se procesan las opciones de PPP" [115]

Consulte la página del comando man pppd(1M) para obtener detalles sobre los archivos de PPP. `pppd` (1M) también incluye descripciones completas de todas las opciones que están disponibles para el comando `pppd`. Las plantillas de ejemplo para todos los archivos de configuración de PPP están disponibles en `/etc/ppp`.

Cómo se procesan las opciones de PPP

1. El daemon `pppd` analiza lo siguiente:

   Todas las operaciones de Solaris PPP 4.0 son gestionadas por el daemon `pppd`, que se inicia cuando el usuario ejecuta el comando `pppd`. Cuando un usuario llama a un par remoto, se produce lo siguiente:

   - `/etc/ppp/options`
   - `$HOME/.ppprc`
   - Los archivos que se abren mediante la opción `file` o `call` en `/etc/ppp/options` y `$HOME/.ppprc`
2. `pppd` analiza la línea de comandos para determinar el dispositivo en uso. El daemon aún no interpreta ninguna de las opciones que se encuentran.
3. `pppd` intenta detectar el dispositivo serie que se utilizará mediante el uso de estos criterios:
   - Si un dispositivo serie se especifica en la línea de comandos o un archivo de configuración procesado anteriormente, `pppd` utiliza el nombre de ese dispositivo.
   - Si no hay ningún dispositivo serie con nombre, `pppd` busca la opción `notty`, `pty` o `socket` en la línea de comandos. Si se especifica una de estas opciones, `pppd` asume que no existe ningún nombre de dispositivo.
   - De lo contrario, si `pppd` descubre que la entrada estándar está conectada a tty, se utiliza el nombre de tty.
   - Si `pppd` no puede encontrar un dispositivo serie, `pppd` finaliza la conexión y emite un error.
4. `pppd` después comprueba la existencia del archivo `/etc/ppp/options.`*ttyname*. Si se encuentra el archivo, `pppd` analiza el archivo.
5. `pppd` procesa cualquier opción de la línea de comandos.
6. `pppd` negocia el Protocolo de control de enlace (LCP) para configurar el enlace.
7. (Opcional) Si se necesita autenticación, `pppd` lee `/etc/ppp/pap-secrets` o `/etc/ppp/chap-secrets` para autenticar al par opuesto.

El archivo `/etc/ppp/peers/`*peer-name* se lee cuando el daemon `pppd` encuentra la opción `call` *peer-name* en la línea de comandos o en otros archivos de configuración.

Cómo funcionan los privilegios de archivos de configuración de PPP

La configuración de Solaris PPP 4.0 incluye el concepto de *privileges*. Los privilegios determinan la precedencia de las opciones de configuración, especialmente cuando la misma opción se invoca en más de una ubicación. Una opción que se invoca desde un origen privilegiado tiene más prioridad que la misma opción invocada desde un origen no privilegiado.

Privilegios del usuario

El único usuario con privilegios es el superusuario (`root`), con el UID de cero. Todos los demás usuarios no tienen privilegios.

Privilegios de archivos

Los siguientes archivos de configuración tienen privilegios, independientemente de sus propietarios:

- `/etc/ppp/options`
- `/etc/ppp/options.`*nombre de tty*
- `/etc/ppp/peers/`*nombre de par*

El archivo `$HOME/.ppprc` es propiedad del usuario. Las opciones que se leen desde `$HOME/.ppprc` y desde la línea de comandos tienen privilegios sólo si el usuario que invoca `pppd` es `root`.

Los argumentos que siguen a la opción `file` tienen privilegios.

Efectos de privilegios de opciones

Algunas opciones necesitan que el usuario que invoca o el origen tengan privilegios para poder funcionar. A las opciones que se invocan en la línea de comandos se les asignan los privilegios del usuario que ejecuta el comando `pppd`. Estas opciones no tienen privilegios, a menos que el usuario que invoca `pppd` esté en `root`.

Opción	Estado	Explicación
`domain`	Con privilegios	Requiere privilegios para su uso.
`linkname`	Con privilegios	Requiere privilegios para su uso.
`noauth`	Con privilegios	Requiere privilegios para su uso.
`nopam`	Con privilegios	Requiere privilegios para su uso.
`pam`	Con privilegios	Requiere privilegios para su uso.
`plugin`	Con privilegios	Requiere privilegios para su uso.
`privgroup`	Con privilegios	Requiere privilegios para su uso.
`allow-ip` *addresses*	Con privilegios	Requiere privilegios para su uso.
`name` *hostname*	Con privilegios	Requiere privilegios para su uso.
`plink`	Con privilegios	Requiere privilegios para su uso.
`noplink`	Con privilegios	Requiere privilegios para su uso.
`plumbed`	Con privilegios	Requiere privilegios para su uso.

Opción	Estado	Explicación
`proxyarp`	Tiene privilegios si `noproxyarp` se ha especificado	No se puede sustituir por un usuario sin privilegios.
`defaultroute`	Con privilegios si `nodefaultroute` está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
`disconnect`	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
`bsdcomp`	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	El usuario sin privilegios no puede especificar un tamaño de código mayor al que el usuario con privilegios ha especificado.
`deflate`	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	El usuario sin privilegios no puede especificar un tamaño de código mayor al que el usuario con privilegios ha especificado.
`connect`	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
`init`	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
`pty`	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
`welcome`	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
ttyname	Con privilegios si se estableció en un archivo con privilegios	Abierto con permisos root, independientemente de quién invoca `pppd`.
	Sin privilegios si se estableció en un archivo sin privilegios	Abierto con los privilegios del usuario que invoca `pppd`.

Archivo de configuración `/etc/ppp/options`

Utiliza el archivo `/etc/ppp/options` para definir opciones globales para todas las comunicaciones de PPP en la máquina local. `/etc/ppp/options` es un archivo con privilegios. `/etc/ppp/options` debe pertenecer a root aunque `pppd` no aplica esta regla. Las opciones que define en `/etc/ppp/options` tienen precedencia sobre las definiciones de las mismas opciones en todos los demás archivos y la línea de comandos.

Entre las opciones típicas que puede usar en `/etc/ppp/options`, se incluyen las siguientes:

- **`lock`** – Activa el bloqueo de archivos de estilo UUCP
- **`noauth`** – Indica que el equipo no autentica a los emisores de llamadas

---

Nota - El software de Solaris PPP 4.0 no incluye un archivo `/etc/ppp/options` predeterminado. `pppd` no requiere el archivo `/etc/ppp/options` para funcionar. Si un equipo no tiene un archivo `/etc/ppp/options`, sólo `root` puede ejecutar `pppd` en ese equipo.

Debe crear `/etc/ppp/options` mediante un editor de texto, como se muestra en Cómo definir comunicaciones a través de la línea de serie [51]. Si un máquina no requiere opciones globales, puede crear un archivo `/etc/ppp/options` vacío. Entonces, `root` y los usuarios comunes pueden ejecutar `pppd` en el equipo local.

Plantilla `/etc/ppp/options.tmpl`

`/etc/ppp/options.tmpl` contiene comentarios útiles sobre el archivo `/etc/ppp/options` y tres opciones comunes para el archivo global `/etc/ppp/options`.

```
lock
nodefaultroute
noproxyarp
```

Opción	Definición
`lock`	Activa el bloqueo de archivos de estilo UUCP
`nodefaultroute`	Especifica que no se definió ninguna ruta predeterminada
`noproxyarp`	No permite `proxyarp`

Para usar `/etc/ppp/options.tmpl` como el archivo de opciones globales, cambie el nombre de `/etc/ppp/options.tmpl` a `/etc/ppp/options`. A continuación, modifique los contenidos del archivo según sea necesario en función del sitio.

¿Dónde encontrar ejemplos de los archivos `/etc/ppp/options`?

Para encontrar ejemplos del archivo `/etc/ppp/options`, consulte lo siguiente:

- Para un equipo de marcación de salida, consulte Cómo definir comunicaciones a través de la línea de serie [51].
- Para un servidor de marcación de entrada, consulte Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada) [58].

- Para compatibilidad de PAP en un servidor de marcación de entrada, consulte Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (servidor de marcación de entrada) [73].
- Para compatibilidad de PAP en un equipo de marcación de salida, consulte Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (equipo de marcación de salida) [77].
- Para compatibilidad de CHAP en un servidor de marcación de entrada, consulte Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (servidor de marcación de entrada) [81].

Archivo de configuración `/etc/ppp/options.`*ttyname*

Puede configurar las características de comunicaciones en la línea de serie en el archivo `/etc/ppp/options.`*ttyname*. `/etc/ppp/options.`*ttyname* es un archivo con privilegios que lee `pppd` después de analizar cualquier archivo existente `/etc/ppp/options` y `$HOME/.ppprc`. De lo contrario, `pppd` lee `/etc/ppp/options.`*ttyname* después de analizar `/etc/ppp/options`.

ttyname se utiliza tanto para enlaces de acceso telefónico como también para enlaces de líneas arrendadas. *ttyname* representa un determinado puerto de serie en una máquina, como `cua/a` o `cua/b`, donde es posible que un módem o un adaptador de terminal RDSI estén conectados.

Al asignar un nombre al archivo `/etc/ppp/options.`*ttyname*, sustituya la barra diagonal (/) en el nombre del dispositivo con un punto (.). Por ejemplo, el archivo `options` para el dispositivo `cua/b` debe llamarse `/etc/ppp/options.cua.b`.

Nota - Solaris PPP 4.0 no requiere un archivo `/etc/ppp/options.`*ttyname* para funcionar correctamente. Es posible que el servidor tenga sólo una línea de serie para PPP. Además, el servidor requiere algunas opciones. En esta instancia, puede especificar cualquier opción requerida en otro archivo de configuración o en la línea de comandos.

Uso de `/etc/ppp/options.`*ttyname* en un servidor de marcación de entrada

Para un enlace de acceso telefónico, es posible que elija crear archivos `/etc/ppp/options.`*ttyname* individuales para cada puerto de serie en un servidor de marcación de entrada con un módem conectado. Entre las opciones típicas, se incluyen las siguientes:

- Dirección IP requerida por el servidor de marcación de entrada

  Establezca esta opción si requiere que los emisores de llamadas en el puerto de serie *ttyname* utilicen una dirección IP específica. Su espacio de dirección puede tener un número limitado de direcciones IP disponibles para PPP en comparación con el número de posibles emisores de llamadas. En esta situación, considere la posibilidad de asignar una dirección IP

a cada interfaz en serie que se utiliza para PPP en el servidor de marcación de entrada. Esta asignación implementa un direccionamiento dinámico para PPP.

- `asyncmap` *map-value*

  La opción `asyncmap` asigna caracteres de control que no se pueden recibir a través de la línea de serie mediante el módem específico o el adaptador de terminal RDSI. Cuando se utiliza la opción `xonxoff`, `pppd` establece automáticamente un asyncmap de 0xa0000.

  valor de mapa, en formato hexadecimal, indica los caracteres de control que son problemáticos.

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

  La opción `init` indica al módem que inicie comunicaciones a través de la línea de serie utilizando la información del comando `chat -U`. El módem utiliza la cadena de chat en el archivo `/etc/ppp/mychat`.

- Parámetros de seguridad que se muestran en la página del comando man `pppd`(1m)

Uso de `/etc/ppp/options.`*ttyname* en una máquina de marcación de salida

Para un sistema de marcación de salida, puede crear un archivo `/etc/ppp/options.`*ttyname* para el puerto de serie que está conectado al módem u optar por no utilizar `/etc/ppp/options.`*ttyname*.

Nota - Solaris PPP 4.0 no requiere un archivo `/etc/ppp/options.`*ttyname* para funcionar correctamente. Es posible que el equipo de marcación de salida tenga sólo una línea de serie para PPP. Además, es posible que el equipo de marcación de salida requiera algunas opciones. Puede especificar cualquier opción requerida en otro archivo de configuración o en la línea de comandos.

Archivo de plantilla `options.ttya.tmpl`

El archivo `/etc/ppp/options.ttya.tmpl` contiene comentarios útiles sobre el archivo `/etc/ppp/options.`*tty-name*. La plantilla contiene tres opciones comunes para el archivo `/etc/ppp/options.`*nombre de tty*.

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

Opción	Definición
`38400`	Utilice esta velocidad de transferencia para el puerto de tty.

Opción	Definición
`asyncmap 0xa0000`	Asigne el valor asyncmap de 0xa0000 para que el equipo local pueda comunicarse con iguales con problemas.
`:192.168.1.1`	Asigne la dirección IP 192.168.1.1 a todos los pares que llaman a través de un enlace.

Para usar `/etc/ppp/options.ttya.tmpl` en el sitio, cambie el nombre de `/etc/ppp/options.tmpl` a `/etc/ppp/options.`*ttya-name*. Reemplace *ttya-name* por el nombre del puerto de serie con el módem. A continuación, modifique los contenidos del archivo según sea necesario en función del sitio.

¿Dónde encontrar ejemplos de los archivos `/etc/ppp/options.`*ttyname*?

Para encontrar ejemplos de los archivos `/etc/ppp/options.`*ttyname*, consulte lo siguiente:

- Para un equipo de marcación de salida, consulte Cómo definir comunicaciones a través de la línea de serie [51].
- Para un servidor de marcación de entrada, consulte Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada) [58].

Configuración de opciones específicas de usuarios

Esta sección contiene información detallada sobre la configuración de usuarios en el servidor de marcación de entrada.

Configuración de `$HOME/.ppprc` en un servidor de marcación de entrada

El archivo `$HOME/.ppprc` es para usuarios que configuran opciones de PPP preferidas. Como administrador, también puede configurar `$HOME/.ppprc` para los usuarios.

Las opciones en `$HOME/.ppprc` tienen privilegios sólo cuando el usuario que invoca el archivo tiene privilegios.

Cuando un emisor utiliza el comando `pppd` para iniciar una llamada, el archivo `.ppprc` es el segundo archivo que el daemon `pppd` comprueba.

Consulte “Configuración de usuarios del servidor de marcación de entrada” [57] para obtener instrucciones acerca de la configuración de `$HOME/.ppprc` en el servidor de marcación de entrada.

Configuración de `$HOME/.ppprc` en un equipo de marcación de salida

No se necesita el archivo `$HOME/.ppprc` en la máquina de marcación de salida para que Solaris PPP 4.0 funcione correctamente. Además, no necesita tener un archivo `$HOME/.ppprc` en la máquina de marcación de salida (excepto en circunstancias especiales). Cree uno o más archivos `.ppprc` si realiza lo siguiente:

- Permite que varios usuarios con diferentes necesidades de comunicación llamen a pares remotos desde el mismo equipo. En tal caso, cree archivos `.ppprc` individuales en los directorios principales de cada usuario que debe realizar una llamada.
- Necesita especificar opciones que controlan problemas específicos de su enlace, como la desactivación de la compresión de Van Jacobson. Consulte *PPP Design, Implementation, and Debugging* de James Carlson y la página del comando man pppd(1M) para recibir asistencia de resolución de problemas de enlace.

Debido a que el archivo `.ppprc` se utiliza la mayoría de las veces al configurar un servidor de marcación de entrada, consulte Cómo configurar usuarios del servidor de marcación de entrada [57] para obtener instrucciones de configuración para `.ppprc`.

Especificación de información para comunicación con el servidor de marcación de entrada

Para comunicarse con un servidor de marcación de entrada, necesita recopilar información sobre el servidor. Y, a continuación, editar algunos archivos. Lo más importante es que debe configurar los requisitos de comunicación de todos los servidores de marcación de entrada a los que el equipo de marcación de salida necesita llamar. Puede especificar opciones acerca de un servidor de marcación de entrada, como un número de teléfono de ISP, en el archivo `/etc/ppp/options.`*ttyname*. Sin embargo, el lugar óptimo para configurar información del par se encuentra en los archivos `/etc/ppp/peers/`*peer-name*.

Archivo `/etc/ppp/peers/`*peer-name*

Nota - No se necesita el archivo `/etc/ppp/peers/`*peer-name* en la máquina de marcación de salida para que Solaris PPP 4.0 funcione correctamente.

Utilice el archivo `/etc/ppp/peers/`*peer-name* para proporcionar información para comunicarse con un igual determinado. `/etc/ppp/peers/`*peer-name* permite a los usuarios comunes invocar opciones con privilegios preseleccionadas que a los usuarios no se les permite establecer.

Por ejemplo, un usuario sin privilegios no puede sustituir la opción `noauth` si `noauth` se especifica en el archivo `/etc/ppp/peers/`*peer-name*. Supongamos que el usuario desea configurar un enlace para `peerB`, que no proporciona credenciales de autenticación. Como superusuario, puede crear un archivo `/etc/ppp/peers/peerB` que incluye la opción `noauth`. `noauth` indica que el equipo local no autentica llamadas de `peerB`.

El daemon `pppd` lee `/etc/ppp/peers/`*peer-name* cuando `pppd` encuentra la siguiente opción:

`call` *peer-name*

Puede crear un archivo `/etc/ppp/peers/`*peer-name* para cada igual de destino con el que la máquina de marcación de salida necesita comunicarse. Esta práctica es particularmente útil para permitir que los usuarios comunes puedan invocar enlaces de marcación de salida sin la necesidad de privilegios root.

Las opciones típicas que especifica en `/etc/ppp/peers/`*peer-name* incluyen lo siguiente:

- `user` *user-name*

  Proporcione *nombre de usuario* al servidor de marcación de entrada, como el nombre de inicio de sesión del equipo de marcación de salida, cuando realice autenticación con PAP o CHAP.

- `remotename` *peer-name*

  Utilice *peer-name* como el nombre de la máquina de marcación de entrada. `remotename` se utiliza junto con la autenticación PAP o CHAP al explorar los archivos `/etc/ppp/pap-secrets` o `/etc/ppp/chap-secrets`.

- `connect "chat` *chat_script*`..."`

  Establezca comunicación con el servidor de marcación de entrada mediante el uso de instrucciones de la secuencia de comandos de chat.

- `noauth`

  No autentique al par *peer-name* al iniciar comunicaciones.

- `noipdefault`

  Defina en 0.0.0.0 la dirección IP inicial que se utiliza en la negociación con el par. Utilice `noipdefault` cuando configure un enlace para la mayoría de los ISP a fin de facilitar la negociación de IPCP entre los iguales.

- `defaultroute`

  Instale una ruta IPv4 predeterminada cuando se establece IP en el enlace.

Consulte la página del comando man pppd(1M) para obtener más opciones que se pueden aplicar a un igual de destino específico.

Archivo de plantilla `/etc/ppp/peers/myisp.tmpl`

El archivo `/etc/ppp/peers/myisp.tmpl` contiene comentarios útiles sobre el archivo `/etc/ppp/peers/`*peer-name*. La plantilla concluye con opciones comunes que puede utilizar para un archivo `/etc/ppp/peers/`*peer-name*:

```
connect "/usr/bin/chat -f /etc/ppp/myisp-chat"
user myname
remotename myisp
noauth
noipdefault
defaultroute
updetach
noccp
```

Opción	Definición
`connect "/usr/bin/chat -f /etc/ppp/myisp-chat"`	Llame al par mediante la secuencia de comandos de chat `/etc/ppp/myisp-chat`.
`user myname`	Utilice este nombre de cuenta para el equipo local. `myname` es el nombre de este equipo en el archivo `/etc/ppp/pap-secrets` del par.
`remotename myisp`	Reconozca `myisp` como el nombre del par en el equipo local del archivo `/etc/ppp/pap-secrets`.
`noauth`	No necesita que los pares que llaman proporcionen credenciales de autenticación.
`noipdefault`	No utilice una dirección IP predeterminada para el equipo local.
`defaultroute`	Utilice la ruta predeterminada que se asignó al equipo local.
`updetach`	Errores de registro en los archivos log de PPP, en lugar de en la salida estándar.
`noccp`	No utilice la compresión de CCP.

Para usar `/etc/ppp/peers/myisp.tmpl` en su sitio, cambie el nombre de `/etc/ppp/peers/myisp.tmpl` a `/etc/ppp/peers/.`*peer-name*. Reemplace *peer-name* por el nombre del par que se llamará. A continuación, modifique los contenidos del archivo según sea necesario en función del sitio.

Dónde encontrar ejemplos de los archivos `/etc/ppp/peers/`*peer-name*

Para encontrar ejemplos de los archivos `/etc/ppp/peers/`*peer-name*, consulte lo siguiente:

- Para un equipo de marcación de salida, consulte Cómo definir la conexión con un par individual [53].
- Para un equipo local en una línea arrendada, consulte Cómo configurar un equipo en una línea arrendada [66].
- Para compatibilidad de autenticación PAP en un equipo de marcación de salida, consulte Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (equipo de marcación de salida) [77].
- Para compatibilidad de autenticación CHAP en un equipo de marcación de salida, consulte Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (equipo de marcación de salida) [83].
- Para compatibilidad de PPPoE en un sistema cliente, consulte “Configuración del cliente PPPoE” [86].

Configuración de velocidad del módem para un enlace por marcación telefónica

Un problema grave en la configuración del módem es la determinación de la velocidad a la que el módem debería funcionar. Las siguientes directrices se aplican a los módems que se utilizan con equipos de Sun Microsystems:

- Sistemas SPARC anteriores: Consulte la documentación del hardware que acompaña al sistema. Muchas máquinas SPARCstation™ requieren que la velocidad del módem no exceda 38.400 bps.
- Máquinas UltraSPARC®: establezca la velocidad del módem en 115.200 bps, que es útil con los módems modernos y lo suficientemente rápida para un enlace de acceso telefónico. Si tiene previsto utilizar un adaptador de terminal RDSI de doble canal con compresión, deberá aumentar la velocidad del módem. El límite en un sistema UltraSPARC es 460.800 bps para un enlace asíncrono.

Para una *máquina de marcación de salida*, establezca la velocidad del módem en los archivos de configuración de PPP, como `/etc/ppp/peers/`*peer-name*, o mediante la especificación de la velocidad como una opción para `pppd`.

Para un *servidor de marcación de entrada*, necesita establecer la velocidad mediante el uso de la utilidad `ttymon`, como se describe en “Configuración de dispositivos en el servidor de marcación de entrada” [55].

Definición de la conversación en el enlace por marcación telefónica

La máquina de marcación de salida y sus pares remotos se comunican a través del enlace de PPP mediante la negociación y el intercambio de diversas instrucciones. Al configurar un equipo de marcación de salida, debe determinar qué instrucciones necesitan los módems locales y remotos. A continuación, cree un archivo denominado secuencia de comandos de chat que contenga estas instrucciones. En esta sección se trata información sobre la configuración de módems y la creación de secuencias de comandos de chat.

Contenidos de la secuencia de comandos de chat

Cada par remoto al que el equipo de marcación de salida necesita conectarse probablemente necesite su propia secuencia de comandos de chat.

Nota - Las secuencias de comandos de chat se utilizan, por lo general, sólo en enlaces por marcación telefónica. Los enlaces de líneas arrendadas no utilizan secuencias de comandos de chat, a menos que el enlace incluya una interfaz asíncrona que requiera configuración de inicio.

Los contenidos de la secuencia de comandos de chat están determinados por los requisitos del modelo del módem o adaptador de terminal RDSI, y el par remoto. Estos contenidos aparecen como un conjunto de cadenas expect-send. El equipo de marcación de salida y sus iguales remotos intercambian las cadenas como parte del proceso de iniciación de comunicaciones.

Una cadena *expect* contiene caracteres que el equipo host de marcación de salida espera recibir del par remoto para iniciar una conversación. Una cadena *send* contiene caracteres que el equipo de marcación de salida envía al par remoto después de recibir la cadena "expect".

La información en la secuencia de comandos de chat, normalmente, incluye lo siguiente:

- Comandos del módem, conocidos, generalmente, como *comandos AT*, que permiten que el módem transmita datos por teléfono
- Número de teléfono del par de destino

  Este número de teléfono podría ser el número que requiere el ISP o un servidor de marcación de entrada en un sitio corporativo, o un equipo individual.
- Valor de tiempo de espera, si es necesario
- Secuencia de inicio de sesión que se espera del par remoto
- Secuencia de inicio de sesión que se envía mediante el equipo de marcación de salida

Ejemplos de secuencias de comandos de chat

Esta sección contiene secuencias de comandos de chat que puede utilizar como una referencia para crear sus propias secuencias de comandos. La guía del fabricante del módem e información sobre el ISP y otros hosts de destino contienen requisitos de chat para el módem y los iguales de destino. Además, numerosos sitios web de PPP tienen secuencias de comandos de chat de ejemplo.

Secuencia de comandos de chat de módem básica

A continuación se muestra una secuencia de comandos de chat básica que puede utilizar como una plantilla para crear sus propias secuencias de comandos de chat.

```
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
```

La siguiente tabla describe los contenidos de la secuencia de comandos de chat.

Contenidos de la secuencia de comandos	Explicación
`ABORT BUSY`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`ABORT 'NO CARRIER'`	Aborta la transmisión si el módem informa `ABORT 'NO CARRIER'` durante la marcación. Este mensaje se debe, normalmente, a fallos en el marcado o en la negociación del módem.
`REPORT CONNECT`	Recopila la cadena `CONNECT` desde el módem. Imprime la cadena.
`TIMEOUT 10`	Establece el tiempo de espera inicial en 10 segundos. La respuesta del módem debería ser inmediata.
`"" AT&F1M0&M5S2=255`	`M0`: desactiva el altavoz durante la conexión. `&M5`: hace que el módem requiera control de errores. `S2=255`: desactiva la secuencia de bloqueo TIES "+++".
`SAY "Calling myserver\n"`	Muestra el mensaje `Calling myserver` en el equipo local.
`TIMEOUT 60`	Restablece el tiempo de espera en 60 segundos para permitir más tiempo para la negociación del enlace.
`OK "ATDT1-123-555-1212"`	Llama al par remoto mediante el número de teléfono 123-555-1212.
`ogin: pppuser`	Inicia sesión con el par mediante el inicio de sesión de estilo UNIX. Proporciona el nombre de usuario `pppuser`.

Contenidos de la secuencia de comandos	Explicación
`ssword: \q\U`	`\q`: no inicia sesión si se depura con la opción `-v`. `\U`: inserta en esta ubicación los contenidos de la cadena que se indica a continuación de `-U`, que se especifica en la línea de comandos. Normalmente, la cadena contiene la contraseña.
`% pppd`	Espera el indicador de shell % y ejecuta el comando `pppd`.

Plantilla de secuencia de comandos de chat `/etc/ppp/myisp-chat.tmpl`

Esta versión incluye `/etc/ppp/myisp-chat.tmpl`, que puede modificar para su uso en el sitio. `/etc/ppp/myisp-chat.tmpl` es similar a la secuencia de comandos de chat de módem básica, excepto que la plantilla no incluye una secuencia de inicio de sesión.

```
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
```

Contenidos de la secuencia de comandos	Explicación
`ABORT BUSY`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`ABORT 'NO CARRIER`	Aborta la transmisión si el módem informa `ABORT 'NO CARRIER'` durante la marcación. Este mensaje se debe, normalmente, a fallos en el marcado o en la negociación del módem.
`REPORT CONNECT`	Recopila la cadena `CONNECT` desde el módem. Imprime la cadena.
`TIMEOUT 10`	Establece el tiempo de espera inicial en 10 segundos. La respuesta del módem debería ser inmediata.
`"" "AT&F1"`	Restablece el módem a los valores predeterminados de fábrica.
`OK "AT&C1&D2"`	Restablece el módem de manera que, para &C1, DCD desde el módem sigue al proveedor. Si el lado remoto cuelga el teléfono por alguna razón, entonces DCD se pierde. Para &D2, la transición alta a baja de DTR hace que el módem esté listo para establecer una comunicación o finalice una llamada.
`SAY "Calling myisp\n"`	Muestra el mensaje “Calling myisp” en el equipo local.
`TIMEOUT 60`	Restablece el tiempo de espera en 60 segundos para permitir más tiempo para la negociación del enlace.
`OK "ATDT1-123-555-1212"`	Llama al par remoto mediante el número de teléfono 123-555-1212.

Contenidos de la secuencia de comandos	Explicación
`CONNECT \c`	Espera el mensaje `CONNECT` del módem del par opuesto.

Secuencia de comandos de chat de módem para llamar a un ISP

Utilice la siguiente secuencia de comandos de chat como una plantilla para llamar a un ISP desde un equipo de marcación de salida con un módem 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"
```

La siguiente tabla describe los contenidos de la secuencia de comandos de chat.

Contenidos de la secuencia de comandos	Explicación
`ABORT BUSY`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`ABORT 'NO CARRIER'`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`REPORT CONNECT`	Recopila la cadena `CONNECT` desde el módem. Imprime la cadena.
`TIMEOUT 10`	Establece el tiempo de espera inicial en 10 segundos. La respuesta del módem debería ser inmediata.
`"" AT&F1M0M0M0M0&M5S2=255`	`M0`: desactiva el altavoz durante la conexión. `&M5`: hace que el módem requiera control de errores. `S2=255`: desactiva la secuencia de bloqueo TIES "+++".
`SAY "Calling myisp\n"`	Muestra el mensaje `Calling myisp` en el equipo local.
`TIMEOUT 60`	Restablece el tiempo de espera en 60 segundos para permitir más tiempo para la negociación del enlace.
`OK "ATDT1-123-555-1212"`	Llama al par remoto mediante el número de teléfono 123-555-1212.
`CONNECT \c`	Espera el mensaje `CONNECT` del módem del par opuesto.
`\r \d\c`	Espera hasta el final del mensaje `CONNECT`.
SAY “Connected; running PPP\n”	Muestra el mensaje informativo `Connected; running PPP` en el equipo local.

Secuencia de comandos de chat básica mejorada para un inicio de sesión de estilo UNIX

La siguiente secuencia de comandos de chat es una secuencia de comandos básica que se ha mejorado para llamar a un igual Oracle Solaris remoto u otro igual de tipo UNIX. Esta secuencia de comandos de chat se usa en Cómo crear las instrucciones para llamar a un par [52].

```
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
```

La siguiente tabla explica los parámetros de la secuencia de comandos de chat.

Contenidos de la secuencia de comandos	Explicación
`TIMEOUT 10`	Establece el tiempo de espera inicial en 10 segundos. La respuesta del módem debería ser inmediata.
`ABORT BUSY`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`ABORT 'NO CARRIER'`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`ABORT ERROR`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`REPORT CONNECT`	Recopila la cadena `CONNECT` desde el módem. Imprime la cadena.
`"" AT&F1&M5S2=255`	`&M5`: hace que el módem requiera control de errores. `S2=255`: desactiva la secuencia de bloqueo TIES "+++".
`TIMEOUT 60`	Restablece el tiempo de espera en 60 segundos para permitir más tiempo para la negociación del enlace.

Contenidos de la secuencia de comandos	Explicación
`OK ATDT1-123-555-1234`	Llama al par remoto mediante el número de teléfono 123-555-1212.
`CONNECT \c`	Espera el mensaje `CONNECT` del módem del par opuesto.
`SAY "Connected; logging in.\n"`	Muestra el mensaje informativo `Connected; logging in` para proporcionar el estado de usuario.
`TIMEOUT 5`	Cambia el tiempo de espera para permitir una visualización rápida del indicador de inicio de sesión.
`ogin:--ogin: pppuser`	Espera el indicador de inicio de sesión. Si no se recibe el indicador, se envía una DEVOLUCIÓN y se espera. A continuación, se envía el nombre de usuario `pppuser` al par. La mayoría de los ISP hacen referencia a la secuencia que se indica a continuación como inicio de sesión de PAP. Sin embargo, el inicio de sesión de PAP no tiene ninguna relación con la autenticación PAP.
`TIMEOUT 20`	Cambia el tiempo de espera a 20 segundos para permitir una verificación de contraseña lenta.
`ssword: \qmysecrethere`	Espera el indicador de contraseña del par. Cuando se recibe el indicador, se envía la contraseña `\qmysecrethere`. `\q` impide que la contraseña se escriba para los archivos log del sistema.
`"% " \c`	Espera un indicador de shell del par. La secuencia de comandos de chat utiliza el shell C. Cambia este valor si el usuario prefiere iniciar sesión con un shell diferente.
`SAY "Logged in. Starting PPP on peer system. \n"`	Muestra el mensaje informativo `Logged in. Starting PPP on peer system` para brindar el estado del usuario.
`ABORT 'not found'`	Aborta la transmisión si el shell encuentra errores.
`"" "exec pppd"`	Inicia `pppd` en el par.
`~ \c`	Espera que PPP se inicie en el par.

El inicio de PPP inmediatamente después de `CONNECT \c` se denomina con frecuencia *inicio de sesión de PAP* por los ISP, aunque el inicio de sesión de PAP, en realidad, no forma parte de la autenticación PAP.

La frase `ogin:--ogin: pppuser` indica al módem que envíe el nombre de usuario `pppuser` en respuesta al indicador de inicio de sesión del servidor de marcación de entrada. `pppuser` es un nombre de cuenta de usuario de PPP especial que se creó para `user1` remoto en el servidor de marcación de entrada. Para obtener instrucciones sobre cómo crear cuentas de usuarios de PPP en un servidor de marcación de entrada, consulte Cómo configurar usuarios del servidor de marcación de entrada [57].

Secuencia de comandos de chat para adaptador de terminal RDSI externo

La siguiente secuencia de comandos de chat se utiliza para llamar desde un equipo de marcación de salida con un adaptador de terminal `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"
```

La siguiente tabla explica los parámetros de la secuencia de comandos de chat.

Contenidos de la secuencia de comandos	Explicación
`SAY "Calling the peer"`	Muestra este mensaje en la pantalla del equipo de marcación de salida.
`TIMEOUT 10`	Establece el tiempo de espera inicial en 10 segundos.
`ABORT BUSY`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`ABORT 'NO CARRIER'`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`ABORT ERROR`	Aborta la transmisión si el módem recibe este mensaje del par opuesto.
`REPORT CONNECT`	Recopila la cadena `CONNECT` desde el módem. Imprime la cadena.
`"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255`	Las letras en esta línea tienen el siguiente significado: ■ `&F`: usa los valores predeterminados de fábrica ■ `B40`: realiza la conversión de PPP asíncrono ■ `S83.7=1`: utiliza los datos a través del portador de voz ■ `&K44`: activa la compresión de CCP ■ `&J3`: activa MP ■ `X7`: informa las velocidades de DCE ■ `S61.3=1`: utiliza la fragmentación de paquetes ■ `S0=0`: no hay respuesta automática ■ `S2=255`: desactiva el escape de TIES
`OK ATDI18882638234`	Realiza una llamada RDSI. Para multivínculo, la segunda llamada se ubica en el mismo número de teléfono, que, generalmente, es lo que requieren

Contenidos de la secuencia de comandos	Explicación
	la mayoría de los ISP. Si el par remoto requiere un segundo número de teléfono diferente, se anexa "+*nnnn*.". *nnnn* representa el segundo número de teléfono.
`CONNECT \c`	Espera el mensaje `CONNECT` del módem del par opuesto.
`\r \d\c`	Espera hasta el final del mensaje `CONNECT`.
`SAY "Connected; running PPP\n"`	Muestra este mensaje en la pantalla del equipo de marcación de salida.

Consulte la página del comando man `chat`(1M) para obtener descripciones de opciones y otra información detallada sobre la secuencia de comandos de chat. Para obtener una explicación de la cadena expect-send, consulte “Campo Chat-Script en el archivo `/etc/uucp/Systems`” [185].

Para obtener más ejemplos de secuencias de comandos de chat

Un número de sitios web ofrece secuencias de comandos de chat de ejemplo y asistencia para la creación de secuencias de comandos de chat. Por ejemplo, consulte http://ppp.samba.org/ppp/index.html.

Invocación de la secuencia de comandos de chat

Llama secuencias de comandos de chat mediante el uso de la opción `connect`. Puede utilizar `connect "chat ..."` en cualquier archivo de configuración de PPP o en la línea de comandos.

Las secuencias de comandos de chat no son ejecutables, pero el programa invocado por `connect` debe ser ejecutable. Es posible que utilice la utilidad de chat como el programa que será invocado por `connect`. En esta instancia, si almacena la secuencia de comandos de chat en un archivo externo mediante la opción `-f`, el archivo de secuencia de comandos de chat no es ejecutable.

El programa `chat` que se describe en `chat`(1m) ejecuta la secuencia de comandos real. El daemon `pppd` invoca el programa `chat` siempre que `pppd` encuentra la opción `connect "chat ..."`.

Nota - Puede utilizar cualquier programa externo, como `Perl` `oTcl`, para crear secuencias de comandos de chat avanzadas. La utilidad `chat` se proporciona como una comodidad.

▼ Cómo invocar una secuencia de comandos de chat (tarea)

1. **Cree la secuencia de comandos de chat como un archivo ASCII.**

2. **Invoque la secuencia de comandos de chat en cualquier archivo de configuración de PPP mediante la siguiente sintaxis:**

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

El indicador `-f` indica que sigue un nombre de archivo. */etc/ppp/chatfile* representa el nombre del archivo de chat.

3. **Otorgue permiso de lectura para el archivo de chat externo para el usuario que ejecuta el comando `pppd`.**

Atención - El programa de chat siempre se ejecuta con los privilegios del usuario, incluso si la opción `connect 'chat ...'` se invoca desde una fuente con privilegios. Por lo tanto, un archivo de chat independiente que se lee con la opción `-f` podrá ser leído por el usuario que invoca. Este privilegio puede ser un problema de seguridad si la secuencia de comandos de chat contiene contraseñas u otra información confidencial.

ejemplo 8-1 Secuencia de comandos de chat en línea

Puede ubicar toda la conversación de secuencia de comandos de chat en una única línea, similar a lo siguiente:

```
connect 'chat "" "AT&F1" OK ATDT5551212 CONNECT "\c"'
```

La secuencia de comandos de chat completa sigue la palabra clave `chat`. La secuencia de comandos finaliza con `"\c"'`. Utiliza esta forma en cualquier archivo de configuración de PPP o en la línea de comandos como un argumento para `pppd`.

Secuencia de comandos de chat en un archivo externo

Si la secuencia de comandos de chat necesaria para un igual determinado es extensa o complicada, considere la posibilidad de crear la secuencia de comandos como un archivo independiente. Los archivos de chat externos son fáciles de mantener y documentar. Puede agregar comentarios al archivo de chat si antepone el signo de almohadilla (#) a los comentarios.

El procedimiento Cómo crear las instrucciones para llamar a un par [52] muestra el uso de una secuencia de comandos de chat contenida en un archivo externo.

Creación de un archivo de chat que es ejecutable

Puede crear un archivo de chat que sea una secuencia de comandos ejecutable para que se ejecute automáticamente cuando se inicie el enlace por marcación telefónica. Por lo tanto, puede ejecutar comandos adicionales durante el inicio del enlace, como `stty`, para valores de paridad, además de los comandos que se incluyen en una secuencia de comandos de chat tradicional.

Esta secuencia de comandos de chat ejecutable se registra en un sistema de estilo UNIX antiguo que requiere 7 bits con paridad par. A continuación, el sistema cambia a 8 bits sin paridad al ejecutar PPP.

```
#!/bin/sh
chat "" "AT&F1" OK "ATDT555-1212" CONNECT "\c"
stty evenp
chat ogin: pppuser ssword: "\q\U" % "exec pppd"
stty -evenp
```

▼ Cómo crear un programa de chat ejecutable

1. **Utilice su editor de texto para crear un programa de chat ejecutable, como el ejemplo anterior.**
2. **Convierta el programa de chat en ejecutable.**

   ```
   # chmod +x /etc/ppp/chatprogram
   ```

3. **Invoque el programa de chat.**

   ```
   connect /etc/ppp/chatprogram
   ```

   Los programas de chat no tienen que estar ubicados dentro del sistema de archivos `/etc/ppp`. Puede almacenar los programas de chat en cualquier ubicación.

Autenticación de emisores de llamadas en un enlace

En esta sección se explica cómo funcionan los protocolos de autenticación PPP y se explican las bases de datos que están asociadas a los protocolos de autenticación.

Protocolo de autenticación de contraseña (PAP)

La autenticación PAP es parecida en operación al programa `login` de UNIX, aunque PAP no concede acceso shell al usuario. PAP utiliza los archivos de configuración de PPP y la base de

datos de PAP en forma del archivo `/etc/ppp/pap-secrets` para configurar la autenticación. PAP también utiliza `/etc/ppp/pap-secrets` para definir credenciales de seguridad de PAP. Estas credenciales incluyen un nombre de par, un "nombre de usuario" en lenguaje de PAP y una contraseña. Las credenciales de PAP también contienen información relacionada para cada emisor de llamada al que se le permite establecer un enlace con el equipo local. Los nombres de usuario y las contraseñas de PAP pueden ser idénticos o diferentes de los nombres de usuario y las contraseñas de UNIX en la base de datos de contraseñas.

Archivo `/etc/ppp/pap-secrets`

La base de datos de PAP se implementa en el archivo `/etc/ppp/pap-secrets`. Las máquinas en ambos lados del enlace de PPP deben haber configurado correctamente las credenciales de PAP en sus archivos `/etc/ppp/pap-secrets` para una autenticación correcta. El emisor de llamada (autenticado) proporciona credenciales en las columnas `user` y `password` del archivo `/etc/ppp/pap-secrets` o en el archivo `+ua` obsoleto. El servidor (autenticador) valida estas credenciales comparando la información en `/etc/ppp/pap-secrets`, a través de la base de datos `passwd` de UNIX o en la utilidad de PAM.

El archivo `/etc/ppp/pap-secrets` tiene la siguiente sintaxis.

```
myclient ISP-server mypassword *
```

Los parámetros tienen el siguiente significado.

`myclient`	Nombre de usuario de PAP del emisor de llamada. Con frecuencia, este nombre es idéntico al nombre de usuario de UNIX del emisor, especialmente si el servidor de marcación de entrada utiliza la opción `login` de PAP.
`ISP-server`	Nombre del equipo remoto, generalmente un servidor de marcación de entrada.
`mypassword`	Contraseña de PAP del emisor de llamada.
`*`	Dirección IP que está asociada con el emisor. Utilice un asterisco (*) para indicar cualquier dirección IP.

Creación de contraseñas de PAP

Las contraseñas de PAP se envían a través del enlace *sin cifrar*, es decir, en formato ASCII legible. Para el emisor de llamada (autenticado), la contraseña de PAP se debe almacenar sin cifrar en cualquiera de las siguientes ubicaciones:

- En `/etc/ppp/pap-secrets`
- En otro archivo externo
- En una conducción con nombre a través de la función `pap-secrets` @
- Como una opción para `pppd`, en la línea de comandos o en un archivo de configuración de PPP
- A través del archivo `+ua`

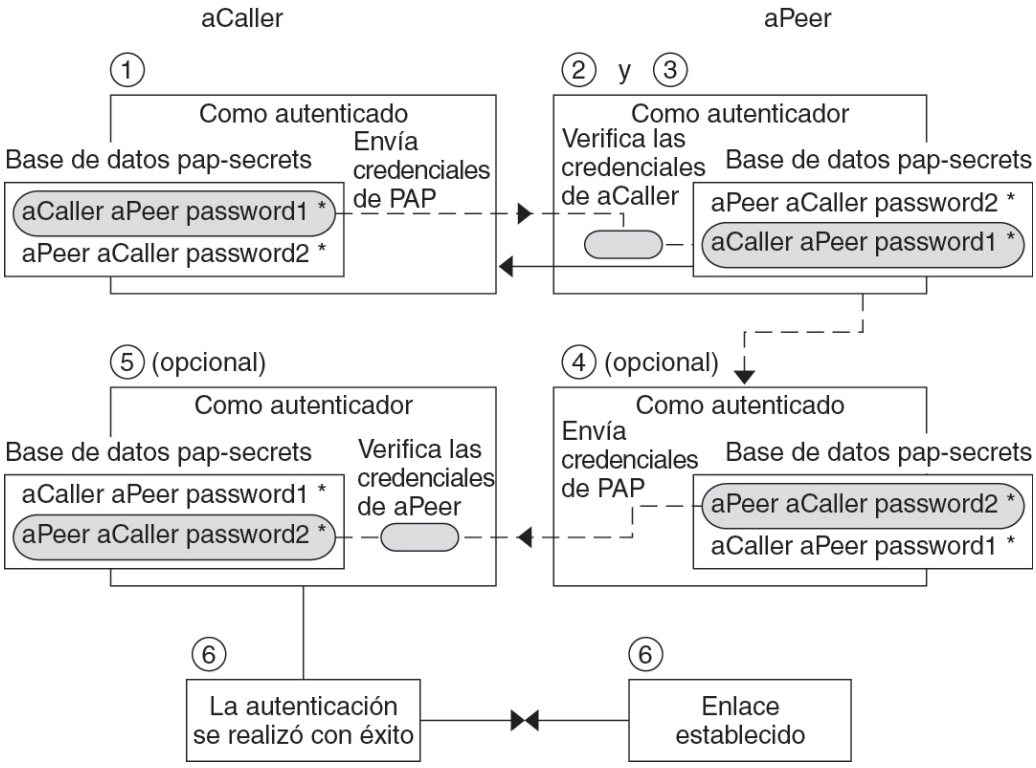
En el servidor (autenticador), la contraseña de PAP se puede ocultar al realizar una de las siguientes acciones:

- Especificar `papcrypt` y utilizar contraseñas a las que se les ha aplicado un algoritmo hash mediante el comando `encrypt` en el archivo `pap-secrets`.
- Especificar la opción `login` para `pppd` y omitir la contraseña del archivo `pap-secrets` colocando comillas dobles (`""`) en la columna de contraseña. En esta instancia, la autenticación se realiza a través de la base de datos "passwd" de UNIX o el mecanismo PAM.

Qué sucede durante la autenticación PAP

La autenticación PAP se produce en la siguiente secuencia.

FIGURA 8-1 Proceso de autenticación PAP



1. El emisor de llamada (autenticado) llama al par remoto (autenticador) y proporciona su nombre de usuario y contraseña de PAP como parte de la negociación del enlace.
2. El par verifica la identidad del emisor de llamada en su archivo `/etc/ppp/pap-secrets`. Si el par utiliza la opción `login` de PAP, el par verifica el nombre de usuario y la contraseña del emisor de llamada en su base de datos de contraseñas.
3. Si la autenticación es correcta, el par continúa la negociación del enlace con el emisor. Si la autenticación falla, el enlace se pierde.
4. (Opcional) Si el emisor de llamada autentica respuestas de iguales remotos, el par remoto debe enviar sus propias credenciales de PAP al emisor. Por lo tanto, el par remoto se convierte en el autenticado y el emisor en el autenticador.
5. (Opcional) El emisor de llamada original lee su propio `/etc/ppp/pap-secrets` para verificar la identidad del par remoto.

Nota - Si el emisor de llamada original requiere credenciales de autenticación del par remoto, el paso 1 y el paso 4 suceden en paralelo.

Si se autentica al par, la negociación continúa. De lo contrario, el enlace se pierde.

6. La negociación entre el emisor de llamada y el par continúa hasta que el enlace se establece correctamente.

Uso de la opción `login` con `/etc/ppp/pap-secrets`

Puede agregar la opción `login` para autenticar credenciales de PAP en cualquier archivo de configuración de PPP. Cuando se especifica `login`, por ejemplo, en `/etc/ppp/options`, `pppd` verifica que las credenciales de PAP del emisor de llamada existen en la base de datos de contraseñas. En el siguiente ejemplo, se muestra el formato de un archivo `/etc/ppp/pap-secrets` con la opción `login`.

```
joe    *  ""  *
sally  *  ""  *
sue    *  ""  *
```

Los parámetros tienen los siguientes significados.

Emisor de llamada	`joe`, `sally` y `sue` son los nombres de los emisores de llamadas autorizados.
Servidor	Asterisco (*), que indica que cualquier nombre de servidor es válido. La opción `name` no es necesaria en los archivos de configuración de PPP.
Contraseña	Comillas dobles, que indican que cualquier contraseña es válida. Si una contraseña está en esta columna, la contraseña del par debe coincidir con la contraseña de PAP y la base de datos `passwd` de UNIX.
Direcciones IP	Asterisco (*), que indica que se permite cualquier dirección IP.

Protocolo de autenticación por desafío mutuo (CHAP)

La autenticación CHAP utiliza la noción de *desafío* y *respuesta*, que significa que el par (autenticador) exige al emisor de llamada (autenticado) que demuestre su identidad. El desafío

incluye un número aleatorio y un ID único que genera el autenticador. El emisor de llamada debe utilizar el ID, el número aleatorio y sus credenciales de seguridad de CHAP para generar la respuesta adecuada (reconocimiento) para enviar al par.

Las credenciales de seguridad de CHAP incluyen un nombre de usuario de CHAP y un "secreto" de CHAP. El secreto de CHAP es una cadena arbitraria conocida por el emisor de llamada y por el par antes de negociar un enlace de PPP. Configure credenciales de seguridad de CHAP en la base de datos de CHAP, `/etc/ppp/chap-secrets`.

Archivo `/etc/ppp/chap-secrets`

La base de datos de CHAP se implementa en el archivo `/etc/ppp/chap-secrets`. Los equipos en ambos lados del enlace de PPP deben tener sus respectivas credenciales de PAP en sus archivos `/etc/ppp/chap-secrets` para una autenticación correcta.

Nota - A diferencia de PAP, el secreto compartido debe estar sin cifrar en ambos iguales. No puede utilizar crypt, PAM ni la opción login de PPP con CHAP.

El archivo `/etc/ppp/chap-secrets` tiene la siguiente sintaxis.

```
myclient myserver secret5748 *
```

Los parámetros tienen los siguientes significados:

`myclient` Nombre de usuario de CHAP del emisor de llamada. Este nombre puede ser diferente o igual al nombre de usuario de UNIX del emisor de llamada.

`myserver` Nombre del equipo remoto, generalmente un servidor de marcación de entrada.

`secret5748` Secreto de CHAP del emisor de llamada.

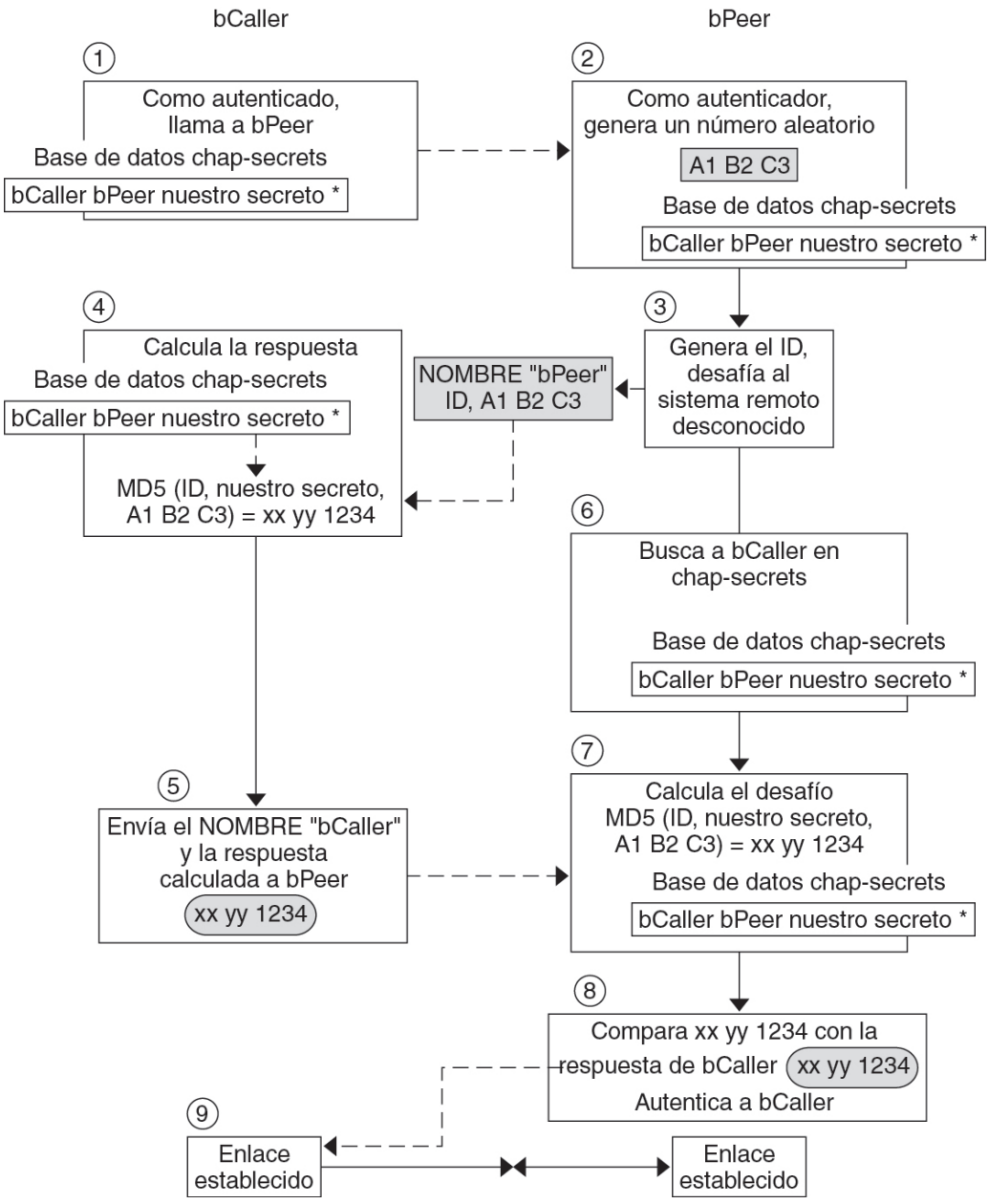
Nota - A diferencia de las contraseñas de PAP, los secretos de CHAP nunca se envían a través del enlace. En su lugar, los secretos de CHAP se utilizan cuando los equipos locales procesan la respuesta.

`*` Dirección IP que está asociada con el emisor. Utilice un asterisco (*) para indicar cualquier dirección IP.

Qué sucede durante la autenticación CHAP

La autenticación CHAP se produce en la siguiente secuencia.

FIGURA 8-2 Secuencia de autenticación CHAP



1. Dos iguales que están por iniciar comunicaciones se ponen de acuerdo sobre un secreto que se utilizará para la autenticación durante la negociación del enlace de PPP.
2. Los administradores de ambas máquinas agregan el secreto, los nombres de usuario de CHAP y otras credenciales de CHAP a la base de datos `/etc/ppp/chap-secrets` de sus respectivas máquinas.
3. El emisor de llamada (autenticado) llama al par remoto (autenticador).
4. El autenticador genera un número aleatorio y un ID, y envía esos datos al autenticado como una desafío.
5. El autenticado busca el nombre y secreto del par en su base de datos `/etc/ppp/chap-secrets`.
6. El autenticado calcula una respuesta aplicando el algoritmo computacional MD5 al secreto y al desafío de número aleatorio del par. A continuación, el autenticado envía los resultados como su respuesta al autenticador.
7. El autenticador busca el nombre y secreto del autenticado en su base de datos `/etc/ppp/chap-secrets`.
8. El autenticador calcula su propia figura aplicando MD5 al número que se generó como el desafío y el secreto para el autenticado en `/etc/ppp/chap-secrets`.
9. El autenticador compara sus resultados con la respuesta del emisor de llamada. Si los dos números son los mismos, el par ha autenticado correctamente al emisor de llamada y la negociación del enlace continúa. De lo contrario, el enlace se pierde.

Creación de un esquema de direccionamiento IP para emisores de llamadas

Considere la posibilidad de crear una o más direcciones IP para todas las llamadas entrantes en lugar de asignar una dirección IP única para cada usuario remoto. Las direcciones IP dedicadas son especialmente importantes si el número de posibles emisores de llamadas supera el número de puertos de serie y módems en el servidor de marcación de entrada. Puede implementar un número de diferentes escenarios, según las necesidades del sitio. Además, los escenarios no son mutuamente excluyentes.

Asignación de direcciones IP dinámicas a emisores de llamadas

El direccionamiento dinámico implica la asignación a cada emisor de llamada de la dirección IP que está definida en `/etc/ppp/options.`*ttyname*. El direccionamiento dinámico se produce por puerto de serie. Cuando llega una llamada a través de una línea de serie, el emisor de llamada recibe la dirección IP del archivo `/etc/ppp/options.`*ttyname* para la interfaz en serie del emisor de llamada.

Por ejemplo, suponga que un servidor de marcación de entrada tiene cuatro interfaces de serie que proporcionan servicio por marcación telefónica para llamadas entrantes:

- Para el puerto de serie `term/a`, cree el archivo `/etc/ppp/options.term.a` con el siguiente registro:

  ```
  :10.1.1.1
  ```

- Para el puerto de serie `term/b`, cree el archivo `/etc/ppp/options.term.b` con la siguiente entrada:

  ```
  :10.1.1.2
  ```

- Para el puerto de serie `term/c`, cree el archivo `/etc/ppp/options.term.c` con la siguiente entrada:

  ```
  :10.1.1.3
  ```

- Para el puerto de serie `term/d`, cree el archivo `/etc/ppp/options.term.d` con la siguiente entrada:

  ```
  :10.1.1.4
  ```

Con el esquema de direccionamiento anterior, a una llamada entrante en la interfaz de serie `/dev/term/c` se le proporciona la dirección IP 10.1.1.3 durante la duración de la llamada. Después de que el primer emisor de llamada cuelga, a la llamada que llega después a través de una interfaz en serie `/dev/term/c` también se le proporciona la dirección IP 10.1.1.3.

Entre las ventajas del direccionamiento dinámico, se incluye lo siguiente:

- Puede realizar un seguimiento del uso de red de PPP en el puerto de serie.
- Puede asignar un número mínimo de direcciones IP para uso de PPP.
- Puede administrar el filtrado IP de una manera más simple.

Asignación de direcciones IP estáticas a emisores de llamadas

Si su sitio implementa autenticación PPP, puede asignar direcciones IP *estáticas* específicas a emisores de llamadas individuales. En este escenario, cada vez que un equipo de marcación de salida llama al servidor de marcación de entrada, el emisor de llamada recibe la misma dirección IP.

Implementa direcciones estáticas en la base de datos pap-secrets o chap-secrets. Aquí se muestra un ejemplo de un archivo `/etc/ppp/pap-secrets` que define direcciones IP estáticas.

```
joe    myserver  joepasswd   10.10.111.240
sally  myserver  sallypasswd 10.10.111.241
sue    myserver  suepasswd   10.10.111.242
```

Emisor de llamada	`joe`, `sally` y `sue` son los nombres de los emisores de llamadas autorizados.
Servidor	`myserver` indica el nombre del servidor.
Contraseña	`joepasswd`, `sallypasswd` y `suepasswd` indican las contraseñas para cada emisor de llamada.
Direcciones IP	`10.10.111.240`, `10.10.111.241` y `10.10.111.242` son las direcciones IP asignadas a cada emisor de llamada.

Aquí se muestra un ejemplo de un archivo `/etc/ppp/chap-secrets` que define direcciones IP estáticas.

```
account1 myserver secret5748  10.10.111.244
account2 myserver secret91011 10.10.111.245
```

Emisor de llamada	`account1` y `account2` indican los nombres de los emisores de llamadas.
Servidor	`myserver` indica el nombre del servidor para cada emisor de llamada.
Contraseña	`secret5748` y `secret91011` indican el secreto de CHAP para cada emisor de llamada.
Direcciones IP	`10.10.111.244` y `10.10.111.245` son las direcciones IP para cada emisor de llamada.

Asignación de direcciones IP por número de unidad sppp

Si utiliza autenticación PAP o CHAP, puede asignar direcciones IP a los emisores de llamadas por número de unidad `sppp`. A continuación se muestra un ejemplo de este uso.

```
myclient ISP-server mypassword 10.10.111.240/28+
```

El signo más (+) indica que el número de unidad se agrega a la dirección IP. Tenga en cuenta los siguientes puntos:

- Las direcciones `10.10.111.240` a través de `10.10.111.255` se asignan a usuarios remotos.
- `sppp0` obtiene la dirección IP `10.10.111.240`.
- `sppp1` obtiene la dirección IP `10.10.111.241` y así sucesivamente.

Creación de túneles PPPoE para compatibilidad de DSL

Al utilizar PPPoE, puede proporcionar PPP a través de servicios digitales de alta velocidad a varios clientes que utilizan uno o más módems DSL. PPPoE implementa estos servicios mediante la creación de un túnel Ethernet a través de tres participantes: la empresa, la compañía telefónica y el proveedor de servicios.

- Para obtener una descripción general y una descripción sobre cómo funciona PPPoE, consulte “Descripción general de PPPoE” [25].
- Para tareas de configuración de túneles PPPoE, consulte el Capítulo 6, Configuración de un túnel de PPP a través de Ethernet.

Esta sección contiene información detallada acerca de comandos y archivos de PPPoE, que se resume en la siguiente tabla.

TABLA 8-2 Comandos y archivos de configuración de PPPoE

Archivo o comando	Descripción	Para obtener instrucciones
`/etc/ppp/pppoe`	Un archivo que contiene características que se aplican de manera predeterminada a todos los túneles configurados por PPPoE en el sistema	“Archivo `/etc/ppp/pppoe`” [148]
`/etc/ppp/pppoe.`*dispositivo*	Un archivo que contiene características de una interfaz determinada utilizada por PPPoE para un túnel	“Archivo `/etc/ppp/pppoe.`*device*” [150]
`/etc/ppp/pppoe.if`	Archivo que muestra la interfaz Ethernet a través de la que se ejecuta el túnel configurado por PPPoE	“Archivo `/etc/ppp/pppoe.if`” [146]
`/usr/sbin/sppptun`	Comando para configurar interfaces Ethernet implicadas en un túnel PPPoE	“Comando `/usr/sbin/sppptun`” [146]
`/usr/lib/inet/pppoed`	Comando y opciones para utilizar PPPoE para configurar un túnel	“Daemon `/usr/lib/inet/pppoed`” [148]

Archivos para configuración de interfaces para PPPoE

Las interfaces que se utilizan en cualquier extremo del túnel PPPoE deben estar configuradas antes de que el túnel pueda admitir comunicaciones de PPP. Utilice los archivos `/usr/sbin/sppptun` y `/etc/ppp/pppoe.if` para este propósito. Debe utilizar estas herramientas para configurar interfaces Ethernet en todos los servidores de acceso PPPoE y clientes PPPoE de Oracle Solaris.

Archivo `/etc/ppp/pppoe.if`

El archivo `/etc/ppp/pppoe.if` enumera los nombres de todas las interfaces Ethernet en un host que se utilizarán para los túneles PPPoE. Este archivo se procesa durante el inicio del sistema cuando las interfaces que se enumeran están conectadas para su uso en túneles PPPoE.

Necesita crear explícitamente `/etc/ppp/pppoe.if`. Escriba el nombre de una interfaz que se debe configurar para PPPoE en cada línea.

En el siguiente ejemplo se muestra un archivo `/etc/ppp/pppoe.if` para un servidor que ofrece tres interfaces para túneles PPPoE.

```
# cat /etc/ppp/pppoe.if
hme1
hme2
hme3
```

Los clientes PPPoE normalmente sólo tienen una interfaz mencionada en `/etc/ppp/pppoe.if`.

Comando `/usr/sbin/sppptun`

Puede utilizar el comando `/usr/sbin/sppptun` para asociar y desasociar manualmente las interfaces Ethernet que se utilizarán para túneles PPPoE. Por el contrario, `/etc/ppp/pppoe.if` sólo se lee cuando se inicia el sistema. Estas interfaces deben corresponderse con las interfaces enumeradas en `/etc/ppp/pppoe.if`.

`sppptun` conecta las interfaces Ethernet que se utilizan en túneles PPPoE de una manera similar al comando `ipadm`. A diferencia de `ipadm`, debe conectar las interfaces dos veces para admitir PPPoE debido a que participan dos números de protocolo Ethernet.

La sintaxis básica para `sppptun` es la siguiente:

```
# /usr/sbin/sppptun plumb pppoed device-name
      device-name:pppoed
# /usr/sbin/sppptun plumb pppoe device-name
      device-name:pppoe
```

En esta sintaxis, *nombre de dispositivo* es el nombre del dispositivo que se conectará para PPPoE.

La primera vez que emite el comando `sppptun`, el protocolo de detección `pppoed` se conecta en la interfaz. La segunda vez que ejecuta `sppptun`, el protocolo de sesión `pppoe` está conectado. `sppptun` imprime el nombre de la interfaz que se acaba de conectar. Este nombre se utiliza para desconectar la interfaz, cuando es necesario.

Para obtener más información, consulte la página del comando man `sppptun`(1M).

Ejemplos de comandos `sppptun` para administración de interfaces

En el siguiente ejemplo se muestra cómo conectar manualmente una interfaz para PPPoE mediante `/usr/sbin/sppptun`.

```
# /usr/sbin/sppptun plumb pppoed hme0
hme0:pppoed
# /dev/sppptun plumb pppoe hme0
 hme0:pppoe
```

En este ejemplo se muestra cómo enumerar las interfaces en un servidor de acceso conectado para PPPoE.

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
hme1:pppoe
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

En este ejemplo se muestra cómo desconectar una interfaz.

```
# sppptun unplumb hme0:pppoed
# sppptun unplumb hme0:pppoe
```

Comandos y archivos de servidor de acceso PPPoE

Un proveedor de servicios que ofrece servicios DSL o admite que los clientes puedan utilizar un servidor de acceso que ejecuta PPPoE. El cliente y el servidor de acceso PPPoE funcionan en la relación cliente-servidor tradicional. Esta relación es similar a la relación del equipo de marcación de salida y el servidor de marcación de entrada en un enlace por marcación telefónica. Un sistema PPPoE inicia comunicaciones y un sistema PPPoE responde. Por el contrario, el protocolo de PPP no tiene noción de la relación cliente-servidor. PPP considera ambos sistemas como pares.

Los archivos y comandos para configurar un servidor de acceso PPPoE incluyen lo siguiente:

Daemon `/usr/lib/inet/pppoed`

El daemon `pppoed` acepta difusiones para servicios desde posibles clientes PPPoE. Además, `pppoed` negocia el lado del servidor del túnel PPPoE y ejecuta `pppd`, el daemon de PPP, a través del túnel.

Configura servicios `pppoed` en los archivos `/etc/ppp/pppoe` y `/etc/ppp/pppoe.`*device*. Si `/etc/ppp/pppoe` existe cuando se inicia el sistema, `pppoed` se ejecuta automáticamente. También puede ejecutar explícitamente el daemon `pppoed` en la línea de comandos si escribe `/usr/lib/inet/pppoed`.

Archivo `/etc/ppp/pppoe`

El archivo `/etc/ppp/pppoe` describe los servicios que ofrece un servidor de acceso más las opciones que definen cómo PPP se ejecuta a través del túnel PPPoE. Puede definir servicios para interfaces individuales o globalmente, es decir, para todas las interfaces del servidor de acceso. El servidor de acceso envía la información en el archivo `/etc/ppp/pppoe`, en respuesta a una difusión de un posible cliente PPPoE.

La siguiente es la sintaxis básica de `/etc/ppp/pppoe`:

global-options
service service-name
    service-specific-options
    device interface-name

Los parámetros tienen los siguientes significados.

global-options
: Establece las opciones predeterminadas para el archivo `/etc/ppp/pppoe`. Estas opciones pueden ser cualquiera de las opciones disponibles a través de `pppoed` o `pppd`. Para ver una lista completa de opciones, consulte las páginas del comando man `pppoed`(1M) y `pppd`(1M).

  Por ejemplo, debe enumerar las interfaces Ethernet que están disponibles para el túnel PPPoE como parte de *global options*. Si no define dispositivos en `/etc/ppp/pppoe`, los servicios no se ofrecen en ninguna interfaz.

  Para definir `devices` como una opción global, utilice lo siguiente:

  device interface <,interface>

  interfaz especifica la interfaz donde el servicio está atento a posibles clientes PPPoE. Si más de una interfaz está asociada al servicio, separe cada nombre con una coma.

service service-name	Inicia la definición del servicio *service-name*. *service-name* es una cadena que puede ser cualquier frase que sea apropiada para los servicios que se proporcionan.
service-specific-options	Muestra las opciones de PPPoE y PPP específicas para este servicio.
`device` *interface-name*	Especifica la interfaz donde el servicio previamente mencionado está disponible.

Para opciones adicionales para `/etc/ppp/pppoe`, consulte las páginas del comando man `pppoed`(1M) y `pppd`(1M).

Es posible que un archivo `/etc/ppp/pppoe`típico se asemeje a lo siguiente.

EJEMPLO 8-2 Archivo `/etc/ppp/pppoe` básico

```
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"
```

En este archivo, se aplican los siguientes valores.

`hme1,hme2,hme3`	Tres interfaces en el servidor de acceso que se utilizarán para túneles PPPoE.
`service internet`	Anuncia un servicio que se denomina `internet` para posibles clientes. El proveedor que ofrece el servicio determina también cómo `internet` está definido. Por ejemplo, un proveedor puede interpretar `internet` como distintos servicios IP, así como el acceso a Internet.
`pppd`	Establece las opciones de línea de comandos que se utilizan cuando el emisor de llamada invoca `pppd`. La opción `"name internet-server"` proporciona el nombre del equipo local, el servidor de acceso, como `internet-server`.
`service intranet`	Anuncia otro servicio que se denomina `intranet` para posibles clientes.
`pppd "192.168.1.1:"`	Establece las opciones de línea de comandos que se utilizan cuando el emisor de llamada invoca `pppd`. Cuando el emisor de llamada invoca `pppd`, 192.168.1.1 se establece como la dirección IP de la máquina local, el servidor de acceso.

`service debug`	Anuncia un tercer servicio, la depuración, en las interfaces que se definen para PPPoE.
`device hme1`	Restringe la depuración para túneles PPPoE para `hme1`.
`pppd "debug name internet-server"`	Establece las opciones de línea de comandos que se utilizan cuando el emisor de llamada invoca `pppd`, en esta instancia, la depuración de PPP en `internet-server`, el equipo local.

Archivo `/etc/ppp/pppoe.`*device*

El archivo `/etc/ppp/pppoe.`*device* describe los servicios ofrecidos en una interfaz de un servidor de acceso PPPoE. `/etc/ppp/pppoe.`*device* también incluye opciones que definen cómo PPP se ejecuta a través del túnel PPPoE. `/etc/ppp/pppoe.`*device* es un archivo opcional, que funciona exactamente igual que `/etc/ppp/pppoe`. Sin embargo, si `/etc/ppp/pppoe.`*device* se define para una interfaz, sus parámetros tienen precedencia para dicha interfaz sobre los parámetros globales que se definen en `/etc/ppp/pppoe`.

La sintaxis básica de `/etc/ppp/pppoe.`*device* es la siguiente:

`service` *service-name*
    service-specific-options
`service` *another-service-name*
    service-specific-options

La única diferencia entre esta sintaxis y la sintaxis de `/etc/ppp/pppoe` es que no puede utilizar la opción `device` que se muestra en “Archivo `/etc/ppp/pppoe`” [148].

Complemento `pppoe.so`

`pppoe.so` es el archivo de objeto compartido PPPoE que debe ser invocado por clientes y servidores de acceso PPPoE. Este archivo limita MTU y MRU a 1492, filtra paquetes desde el controlador y negocia el túnel PPPoE junto con `pppoed`. En el lado del servidor de acceso, `pppoe.so` es invocado automáticamente por el daemon `pppd`.

Uso de archivos PPPoE y PPP para configurar un servidor de acceso

Esta sección contiene ejemplos de todos los archivos que se utilizan para configurar un servidor de acceso. El servidor de acceso es de hosts múltiples. El servidor está conectado a tres

subredes: green, orange y purple. pppoed se ejecuta como root en el servidor, que es el valor predeterminado.

Los clientes PPPoE pueden acceder a las redes de orange y purple a través de interfaces hme0 y hme1. Los clientes inician sesión en el servidor mediante el inicio de sesión de UNIX estándar. El servidor autentica a los clientes mediante PAP.

La red green no se anuncia para los clientes. La única forma en que los clientes pueden acceder a green es especificar directamente "green-net" y proporcionar credenciales de autenticación CHAP. Además, sólo los clientes joe y mary tienen permiso para acceder a la red green mediante direcciones IP estáticas.

EJEMPLO 8-3 Archivo para un servidor de acceso /etc/ppp/pppoe

```
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
```

Este ejemplo describe los servicios que están disponibles desde el servidor de acceso. La primera sección de servicio describe los servicios de la red orange.

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
```

Los clientes acceden a la red orange a través de interfaces hme0 y hme1. Las opciones que se brindan al comando pppd obligan al servidor a solicitar credenciales de PAP de clientes potenciales. Las opciones pppd establecen el nombre del servidor para orange-server, como se utiliza en el archivo pap-secrets.

La sección de servicio para la red purple es idéntica a la sección de servicio de la red orange a excepción de los nombres de servidor y de red.

La siguiente sección describe los servicios de la red green:

```
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

Esta sección restringe el acceso de cliente a la interfaz hme1. Las opciones que se brindan al comando pppd obligan al servidor que solicite credenciales de CHAP de clientes potenciales. Las opciones pppd también establecen el nombre de servidor para green-server, que se

utilizará en el archivo `chap-secrets`. La opción `nowildcard` especifica que la existencia de la red "green" no se anuncia a los clientes.

Para este escenario de servidor de acceso que acabamos de debatir, es posible que configure el siguiente archivo `/etc/ppp/options`.

EJEMPLO 8-4 Archivo para un servidor de acceso `/etc/ppp/options`

```
auth
proxyarp
nodefaultroute
name no-service # don't authenticate otherwise
```

La opción `name no-service` sustituye el nombre de servidor que normalmente se busca durante la autenticación PAP o CHAP. El nombre predeterminado del servidor es el que se encuentra mediante el comando `/usr/bin/hostname`. La opción `name` en el ejemplo anterior cambia el nombre del servidor a `no-service`. No es muy posible que se encuentre el nombre `no-service` en un archivo `pap` o `chap-secrets`. Esta acción impide que un usuario al azar ejecute `pppd` y cambie las opciones `auth` y `name` establecidas en `/etc/ppp/options`. `pppd` falla debido a que no se pueden encontrar secretos para el cliente con un nombre de servidor de `no-service`.

El escenario de servidor de acceso utiliza el siguiente archivo `/etc/hosts`.

EJEMPLO 8-5 Archivo para un servidor de acceso `/etc/hosts`

```
    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
```

Aquí está el archivo `/etc/ppp/pap-secrets` que se utiliza para autenticación PAP para clientes que intentan acceder a las redes `orange` y `purple`.

EJEMPLO 8-6 Archivo para un servidor de acceso `/etc/ppp/pap-secrets`

```
* orange-server "" 172.16.0.2/16+
* purple-server "" 172.17.0.2/16+
```

Aquí está el archivo `/etc/ppp/chap-secrets` que se utiliza para autenticación CHAP. Tenga en cuenta que sólo los clientes `joe` y `mary` se muestran en el archivo.

EJEMPLO 8-7 Archivo para un servidor de acceso `/etc/ppp/chap-secrets`

```
 joe green-server "joe's secret" joes-pc
mary green-server "mary's secret" marys-pc
```

Archivos y comandos de cliente PPPoE

Para ejecutar PPP a través de un módem DSL, una máquina debe convertirse en un cliente PPPoE. Debe conectar una interfaz para ejecutar PPPoE y, a continuación, utilizar la utilidad `pppoec` para "detectar" la existencia de un servidor de acceso. A partir de ese momento, el cliente puede crear el túnel PPPoE a través del módem DSL y ejecutar PPP.

El cliente PPPoE se relaciona con el servidor de acceso en el modelo cliente-servidor tradicional. El túnel PPPoE no es un enlace por marcación telefónica, pero está configurado y opera casi de la misma manera.

Los archivos y comandos para configurar un cliente PPPoE incluyen lo siguiente:

- “Comando `/usr/sbin/sppptun`” [146]
- “Utilidad `/usr/lib/inet/pppoec`” [153]
- “Objeto compartido `pppoe.so`” [153]
- “Archivo `/etc/ppp/peers/`*peer-name*” [123]
- “Archivo de configuración `/etc/ppp/options`” [117]

Utilidad `/usr/lib/inet/pppoec`

La utilidad `/usr/lib/inet/pppoec` es responsable de negociar el lado del cliente de un túnel PPPoE. `pppoec` es similar a la utilidad `chat`. No invoca `pppoec` directamente. En su lugar, inicia `/usr/lib/inet/pppoec` como un argumento para la opción `connect` de `pppd`.

Objeto compartido `pppoe.so`

`pppoe.so` es el objeto compartido PPPoE que debe ser cargado por PPPoE para proporcionar funciones PPPoE para acceder a servidores y clientes. El objeto compartido `pppoe.so` limita MTU y MRU 1492, filtra paquetes desde el controlador y gestiona mensajes PPPoE de tiempo de ejecución.

En el lado del cliente, `pppd` carga `pppoe.so` cuando el usuario especifica la opción `plugin pppoe.so`.

Archivo para definir un igual de servidor de acceso `/etc/ppp/peers/`*peer-name*

Cuando define un servidor de acceso para que lo detecte `pppoec`, puede usar opciones que se apliquen a `pppoec` y al daemon `pppd`. Un archivo `/etc/ppp/peers/`*peer-name* de un servidor de acceso requiere los siguientes parámetros:

- `sppptun`: nombre para el dispositivo serie utilizado por el túnel PPPoE.
- `plugin pppoe.so`: indica a `pppd` que cargue el objeto compartido `pppoe.so`.
- `connect "/usr/lib/inet/pppoec` *device*`"`: inicia una conexión. `connect` luego invoca la utilidad `pppoec` a través de *device*, la interfaz que está conectada para PPPoE.

Los parámetros restantes del archivo `/etc/ppp/peers/`*peer-name* se deben aplicar al enlace de PPP en el servidor. Utilice las mismas opciones que usaría para `/etc/ppp/peers/`*peer-name* en una máquina de marcación de salida. Intente limitar el número de opciones al mínimo necesario para el enlace de PPP.

El siguiente ejemplo se presenta en Cómo definir un par de servidor de acceso PPPoE [87].

EJEMPLO 8-8 `/etc/ppp/peers/`*peer-name* para definir un servidor de acceso remoto

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

Este archivo define parámetros que se utilizarán al configurar un túnel PPPoE y un enlace de PPP para el servidor de acceso `dslserve`. Las opciones que se incluyen son las siguientes.

Opción	Descripción
`sppptun`	Define `sppptun` como nombre del dispositivo serie.
`plugin pppoe.so`	Indica a `pppd` que cargue el objeto compartido `pppoe.so`.
`connect "/usr/lib/inet/pppoec hme0"`	Ejecuta `pppoec` y designa `hme0` como interfaz para el túnel PPPoE y el enlace de PPP.
`noccp`	Desactiva la compresión CCP en el enlace. **Nota -** Muchos ISP utilizan sólo algoritmos de compresión de propietario. La desactivación del algoritmo CCP disponible públicamente ahorra tiempo de negociación y evita problemas de interoperabilidad frecuentes.
`noauth`	Evita que `pppd` exija credenciales de autenticación desde el servidor de acceso. La mayoría de proveedores de servicios de Internet no proporcionan credenciales de autenticación a los clientes.
`user Red`	Establece el nombre `Red` como nombre de usuario para el cliente, que es requerido para autenticación PAP por el servidor de acceso.
`password redsecret`	Define `redsecret` como la contraseña que se proporcionará al servidor de acceso para autenticación PAP.
`noipdefault`	Asigna 0.0.0.0 como la dirección IP inicial.

Opción	Descripción
`defaultroute`	Indica a `pppd` que instale una ruta IPv4 predeterminada después de la negociación de IPCP. Debe incluir `defaultroute` en `/etc/ppp/peers/`*peer-name* cuando el enlace es el enlace del sistema a Internet, lo que se aplica para un cliente PPPoE.

♦ ♦ ♦ CAPÍTULO 9

Migración desde Solaris PPP asíncrono a Solaris PPP 4.0 (tareas)

Las versiones anteriores del sistema operativo Oracle Solaris incluían una implementación de PPP diferente, Solaris PPP asíncrono (`asppp`). Si desea convertir a los pares que ejecutan `asppp` a la nueva versión PPP 4.0, tendrá que ejecutar una secuencia de comandos de conversión. En este capítulo se tratan los siguientes temas de conversión de PPP:

- "Antes de convertir los archivos `asppp`" [157]
- "Ejecución de la secuencia de comandos de conversión `asppp2pppd` (tareas)" [160]

El capítulo utiliza un ejemplo de configuración de `asppp` para explicar cómo realizar la conversión de PPP. Para obtener una descripción de las diferencias entre Solaris PPP 4.0 y `asppp`, vaya a "Cómo determinar qué versión de Solaris PPP se debe usar" [14].

Antes de convertir los archivos `asppp`

Puede utilizar la secuencia de comandos de conversión `/usr/sbin/asppp2pppd` para convertir los archivos que componen una configuración `asppp` estándar.

- `/etc/asppp.cf`: archivo de configuración de PPP asíncrono
- `/etc/uucp/Systems`: archivo de UUCP que describe las características del par remoto
- `/etc/uucp/Devices`: archivo de UUCP que describe el módem en el equipo local
- `/etc/uucp/Dialers`: archivo de UUCP que contiene la secuencia de comandos de inicio de sesión que utilizará el módem que se describe en el archivo `/etc/uucp/Devices`

Para obtener más información sobre `asppp`, consulte *Colección de administración del sistema Solaris 8, volumen 3*, disponible en http://docs.oracle.com/cd/E19455-01/index.html.

Ejemplo del archivo de configuración /etc/asppp.cf

El procedimiento que se muestra en Cómo convertir de asppp a Solaris PPP 4.0 [161] utiliza el siguiente archivo /etc/asppp.cf.

```
#
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
```

El archivo contiene los siguientes parámetros.

`ifpadm create-if ipdptp0`	Ejecuta el comando `ipadm` para crear una interfaz llamada `ipdptp0`
`ipadm create-addr -T static -a local=mojave,remote=gobi ipdptp0/ppadd`	Ejecuta el comando `ipadm` para configurar un enlace desde la interfaz PPP `ipdptp0` en el equipo local `mojave` hasta el par remoto `gobi`
`inactivity_timeout 120`	Termina la línea después de dos minutos de inactividad
`interface ipdptp0`	Configura la interfaz `ipdptp0` en el equipo de marcación de salida para PPP asíncrono
`peer_system_name Pgobi`	Proporciona el nombre del par remoto, `Pgobi`

Ejemplo del archivo /etc/uucp/Systems

El procedimiento que se muestra en Cómo convertir de asppp a Solaris PPP 4.0 [161] utiliza el siguiente archivo /etc/uucp/Systems.

```
#ident  "@(#)Systems 1.5  92/07/14 SMI"  /* from SVR4 bnu:Systems 2.4 */
#

# .
# .
Pgobi Any ACU 38400 15551212 in:--in: mojave word: sand
```

El archivo contiene los siguientes parámetros:

`Pgobi`	Utiliza `Pgobi` como el nombre de host del par remoto.
`Any ACU`	Indica al módem en el equipo de marcación de salida `mojave` que establezca un enlace con un módem`Pgobi` en cualquier momento del día. Cualquier unidad de llamada automática (ACU) significa "buscar ACU en el archivo `/etc/uucp/Devices`".
`38400`	Establece 38400 como la velocidad máxima del enlace.
`15551212`	Proporciona el número de teléfono de `Pgobi`.
`in:–in: mojave word: sand`	Define la secuencia de comandos de inicio de sesión que requiere `Pgobi` para autenticar la máquina de marcación de salida `mojave`.

Ejemplo del archivo `/etc/uucp/Devices`

El procedimiento que se muestra en Cómo convertir de `asppp` a Solaris PPP 4.0 [161] utiliza el siguiente archivo `/etc/uucp/Devices`.

```
#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
```

El archivo admite cualquier módem Hayes que esté conectado al puerto de serie cua/b.

Ejemplo del archivo /etc/uucp/Dialers

El procedimiento que se muestra en Cómo convertir de asppp a Solaris PPP 4.0 [161] utiliza el siguiente archivo /etc/uucp/Dialers.

```
#
#       <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>
```

Este archivo contiene las secuencias de comandos de chat para todos los tipos de módems, incluido los módems Hayes que se admiten en el archivo /etc/uucp/Dialers.

Ejecución de la secuencia de comandos de conversión asppp2pppd (tareas)

La secuencia de comandos /usr/sbin/asppp2pppd copia la información de PPP en /etc/asppp.cf y los archivos de UUCP relacionados con PPP para ubicaciones apropiadas en los archivos de Solaris PPP 4.0.

Requisitos previos de la tarea

Antes de realizar la siguiente tarea, debe haber hecho lo siguiente:

- Instalado la versión de Oracle Solaris en el equipo que también tiene los archivos de configuración de UUCP y `asppp`.
- Convertido en superusuario en el equipo con los archivos de PPP, por ejemplo, el equipo `mojave`.

▼ Cómo convertir de `asppp` a Solaris PPP 4.0

1. **Inicie la secuencia de comandos de conversión.**

   ```
   # /usr/sbin/asppp2pppd
   ```

   El proceso de conversión se inicia y le muestra la siguiente pantalla.

   ```
   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. **Escriba “Y” para continuar.**

   Recibirá el siguiente resultado.

   ```
   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
   ```

   Los nuevos archivos de Solaris PPP 4.0 se han generado.

▼ Cómo ver los resultados de la conversión

Puede ver los archivos de Solaris PPP 4.0 que se crearon mediante la secuencia de comandos de conversión `/usr/sbin/asppp2pppd` al final del proceso de conversión. La secuencia de comandos muestra la siguiente lista de opciones.

```
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. **Escriba `1` para ver los contenidos de los archivos en la pantalla.**

   La secuencia de comandos solicita el número del archivo que desea ver.

   ```
   File number (1 .. 4):
   ```

   Los números se refieren a los archivos traducidos que se enumeran durante el proceso de conversión, como se muestra en el paso 2 anterior.

2. **Escriba `1` para ver el archivo de chat `/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
   ```

   La secuencia de comandos de chat contiene la información de "chat" del módem que aparece en la línea hayes en el archivo de ejemplo `/etc/uucp/Dialers`. `/etc/ppp/chat.Pgobi.hayes` también contiene la secuencia de inicio de sesión para `Pgobi` que aparece en el archivo de ejemplo `/etc/uucp/Systems`. La secuencia de comandos de chat se encuentra ahora en el archivo `/etc/ppp/chat.Pgobi.hayes`.

3. **Escriba `2` para ver el archivo de los iguales, `/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
   ```

   La información del puerto de serie (`/dev/cua/b`) se obtiene del archivo `/etc/uucp/Devices`. La velocidad del enlace, el tiempo de inactividad, la información de autenticación y los nombres de iguales se obtienen del archivo `/etc/asppp.cf`. "demand" hace referencia a la secuencia de comandos "demand", a la que se llama cuando el equipo de marcación de salida intenta conectarse con el par `Pgobi`.

4. **Escriba `3` para ver el archivo `/etc/ppp/options` que se crea para el equipo de marcación de salida `mojave`.**

   ```
   File number (1 .. 4):  3
   ```

```
#lock
noauth
```

La información de `/etc/ppp/options` se obtiene del archivo `/etc/asppp.cf`.

5. **Escriba `4` para ver los contenidos de la secuencia de comandos `demand`.**

```
File number (1 .. 4):  4
/usr/bin/pppd file /etc/ppp/peers/Pgobi
```

Esta secuencia de comandos, cuando se invoca, ejecuta el comando `pppd` que luego lee `/etc/ppp/peers/Pgobi` para iniciar el enlace entre `mojave` y `Pgobi`.

6. **Escriba `9` para guardar los archivos creados. A continuación, salga de la secuencia de comandos de conversión.**

♦ ♦ ♦ CAPÍTULO 10

Acerca de programa de copia de UNIX a UNIX

En este capítulo, se introducen el programa de copia de UNIX a UNIX (UUCP) y sus daemons. Se tratan los temas siguientes:

El UUCP permite a los equipos transferir archivos e intercambiar correo entre ellos. El programa también permite a los equipos participar en redes de gran tamaño, como Usenet.

El sistema operativo de Oracle Solaris proporciona la versión de utilidades básicas de red (BNU) del UUCP, también conocida como HoneyDanBer UUCP. El término *UUCP* indica el rango completo de utilidades y archivos que componen el sistema, del cual el programa `uucp` es sólo una parte. El rango de utilidades del UUCP abarca desde las utilidades que se utilizan para copiar archivos entre equipos (`uucp` y `uuto`) hasta las utilidades que se utilizan para iniciar sesión y ejecutar comandos de manera remota (`cu` y `uux`).

Configuraciones de hardware del UUCP

El UUCP admite las siguientes configuraciones de hardware:

Enlaces directos	Puede crear un enlace directo a otra máquina colocando cables RS-232 entre los puertos de serie de las dos máquinas Los enlaces directos son útiles cuando dos equipos se comunican regularmente y están físicamente cerca, por ejemplo, dentro de 50 ft (15 m) entre ellos. Puede utilizar un módem de distancia limitada para aumentar esta distancia un poco.
Líneas telefónicas	Al usar una unidad de llamada automática (ACU), como un módem de alta velocidad, el equipo puede comunicarse con otros equipos por medio de líneas de teléfono estándar. El módem marca el número de teléfono solicitado por el UUCP. El equipo destinatario debe tener un módem capaz de responder llamadas entrantes.
Red	El UUCP también puede comunicarse por medio de una red que ejecuta TCP/IP u otra familia de protocolos. Después de que su equipo se

ha establecido como un host en una red, el equipo puede ponerse en contacto con cualquier otro host que está conectado a la red.

En este capítulo, se asume que el hardware del UUCP ya se ha ensamblado y configurado. Si necesita configurar un módem, consulte los manuales que se incluyen con el módem para obtener ayuda.

Software del UUCP

El software del UUCP se incluye automáticamente al ejecutar el programa de instalación de Oracle Solaris y al seleccionar toda la distribución. También puede agregar el software del UUCP mediante `pkgadd`. Los programas del UUCP se pueden dividir en tres categorías: daemons, programas administrativos y programas de usuario.

Daemons del UUCP

El sistema del UUCP tiene cuatro daemons: `uucico`, `uuxqt`, `uusched` y `in.uucpd`. Estos daemons manejan las transferencias de archivos y las ejecuciones de comandos del UUCP. También se pueden ejecutar de forma manual desde el shell, si es necesario.

`uucico`
: Selecciona el dispositivo que se utiliza para el enlace, establece el enlace al equipo remoto y realiza las comprobaciones requeridas de permisos y secuencias de inicio de sesión. Además, `uucico` transfiere archivos de datos, archivos ejecutables y resultados de registros, y notifica al usuario por correo cuando se completan las transferencias. `uucico` actúa como el "shell de inicio de sesión" para las cuentas de entrada del UUCP. Cuando el daemon `uucico` local llama a una máquina remota, se comunica directamente con el daemon `uucico` remoto durante la sesión.

  Después de que todos los archivos necesarios se han creado, los programas `uucp`, `uuto` y `uux` ejecutan el daemon `uucico` para ponerse en contacto con el equipo remoto. `uusched` y `Uutry` ejecutan `uucico`. Consulte la página del comando man `uucico`(1M) para obtener detalles.

`uuxqt`
: Ejecuta solicitudes de ejecución remota. Este daemon busca en el directorio de cola de impresión archivos ejecutables (siempre denominados `X.`*file*) que se han enviado desde un equipo remoto. Cuando se encuentra un archivo `X.`*file*, `uuxqt` lo abre para obtener la lista de los archivos de datos que son necesarios para la ejecución. `uuxqt` después comprueba si los archivos de datos necesarios están disponibles y son accesibles. Si los archivos están disponibles, `uuxqt` comprueba el archivo `Permissions` para verificar si tiene permiso para ejecutar el comando

solicitado. El daemon `uuxqt` es ejecutado por la secuencia de comandos de shell `uudemon.hour`, que es iniciada por `cron`. Consulte la página del comando man `uuxqt`(1M) para obtener detalles.

`uusched` — Programa el trabajo en cola en el directorio de cola de impresión. `uusched` se ejecuta inicialmente en el momento del inicio mediante la secuencia de comandos de shell `uudemon.hour`, iniciado por `cron`. Consulte la página del comando man `uusched`(1M) para obtener detalles. Antes de iniciar el daemon `uucico`, `uusched` selecciona al azar el orden en el que los equipos remotos se llaman.

`in.uucpd` — Admite conexiones del UUCP por medio de redes. `inetd` en el host remoto invoca a `in.uucpd` cada vez que se establece una conexión del UUCP. `uucpd`, a continuación, solicita un nombre de inicio de sesión. `uucico` en el host que llama debe responder con un nombre de inicio de sesión. `in.uucpd`, a continuación, solicita una contraseña, a menos que no sea necesaria. Consulte la página del comando man `in.uucpd`(1M) para obtener detalles.

Programas administrativos del UUCP

La mayoría de los programas administrativos del UUCP están en `/usr/lib/uucp`. La mayoría de los archivos de base de datos básicos están en `/etc/uucp`. La única excepción es `uulog`, que está en `/usr/bin`. El directorio raíz del ID de inicio de sesión `uucp` es `/usr/lib/uucp`. Al ejecutar los programas administrativos mediante `su` o `login`, utilice el ID de usuario `uucp`. El ID de usuario posee los programas y los archivos de datos en cola de impresión.

`uulog` — Muestra el contenido de los archivos log de un equipo especificado. Los archivos log se crean para cada equipo remoto con el que su equipo se comunica. Los archivos log registran cada uso de `uucp`, `uuto` y `uux`. Consulte la página del comando man `uucp`(1C) para obtener detalles.

`uucleanup` — Limpia el directorio de la cola de impresión. `uucleanup` es normalmente ejecutado desde la secuencia de comandos de shell `uudemon.cleanup`, que es iniciada por `cron`. Consulte la página del comando man `uucleanup`(1M) para obtener detalles.

`Uutry` — Prueba las capacidades de procesamiento de llamadas y realiza una depuración moderada. `Uutry` invoca el daemon `uucico` para establecer un enlace de comunicación entre su equipo y el equipo remoto que especifique. Consulte la página del comando man `Uutry`(1M) para obtener detalles.

`uucheck` Comprueba la presencia de directorios, programas y archivos de compatibilidad del UUCP. `uucheck` también puede comprobar determinadas partes del archivo `/etc/uucp/Permissions` para buscar errores sintácticos evidentes. Consulte la página del comando man `uucheck`(1M) para obtener detalles.

Programas de usuario del UUCP

Los programas de usuario del UUCP están en `/usr/bin`. No es necesario un permiso especial para usar estos programas.

`cu` Conecta la máquina con un equipo remoto para que pueda iniciar sesión en ambas máquinas al mismo tiempo. `cu` le permite transferir archivos o ejecutar comandos en cualquiera de las máquinas sin necesidad de abandonar el enlace inicial. Consulte la página del comando man `cu`(1C) para obtener detalles.

`uucp` Permite copiar un archivo de una máquina a otra. `uucp` crea archivos de trabajo y archivos de datos, pone en cola trabajos para transferencia y llama al daemon `uucico`, que, a su vez, intenta ponerse en contacto con la máquina remota. Consulte la página del comando man `uucp`(1C) para obtener detalles.

`uuto` Copia archivos de la máquina local al directorio de cola de impresión público `/var/spool/uucppublic/receive` en la máquina remota. A diferencia de `uucp`, que permite copiar un archivo en cualquier directorio accesible del equipo remoto, `uuto` coloca el archivo en un directorio de cola de impresión adecuado e indica al usuario remoto que recoja el archivo con `uupick`. Consulte la página del comando man `uuto`(1C) para obtener detalles.

`uupick` Recupera los archivos en `/var/spool/uucppublic/receive` cuando los archivos se transfieren a un equipo mediante `uuto`. Consulte la página del comando man `uuto`(1C).

`uux` Crea los archivos de trabajo, de datos y ejecutables que son necesarios para ejecutar comandos en una máquina remota. Consulte la página del comando man `uux`(1C) para obtener detalles.

`uustat` Muestra el estado de transferencias solicitadas (`uucp`, `uuto` o `uux`). `uustat` también proporciona un medio para controlar transferencias en cola. Consulte la página del comando man `uustat`(1C) para obtener detalles.

Archivos de base de datos del UUCP

Una parte importante de la configuración del UUCP es la configuración de los archivos que componen la base de datos del UUCP. Estos archivos están en el directorio `/etc/uucp`. Debe editar estos archivos para configurar el UUCP o `asppp` en su equipo. Los archivos incluyen lo siguiente:

`Config`	Contiene una lista de parámetros variables. Estos parámetros se pueden definir manualmente para configurar la red.
`Devconfig`	Se utiliza para configurar las comunicaciones de red.
`Devices`	Se utiliza para configurar las comunicaciones de red.
`Dialcodes`	Contiene abreviaturas de código de marcación que se pueden utilizar en el campo de número de teléfono de las entradas del archivo `Systems`. Aunque no se requiere, `Dialcodes` puede ser utilizado por `asppp` y por el UUCP.
`Dialers`	Contiene cadenas de caracteres que son necesarias para negociar con módems y establecer conexiones con equipos remotos. `Dialers` es usado por `asppp` y por el UUCP.
`Grades`	Define niveles de trabajos, y los permisos que se relacionan con cada nivel de trabajo, que los usuarios pueden especificar para poner en cola trabajos en un equipo remoto.
`Limits`	Define el número máximo de ejecuciones simultáneas `uucico`, `uuxqt` y `uusched` que se permiten en la máquina.
`Permissions`	Define el nivel de acceso que se otorga a hosts remotos que intentan transferir archivos o ejecutar comandos en la máquina.
`Poll`	Define las máquinas que van a ser sondeadas por el sistema y cuándo van a ser sondeadas.
`Sysfiles`	Asigna diferentes o varios archivos para usar con `uucico` y `cu`, como los archivos `Systems`, `Devices` y `Dialers`.
`Sysname`	Permite definir un único nombre del UUCP para una máquina, además de su nombre de host TCP/IP.
`Sistemas`	Contiene información que necesita el daemon `uucico`, `cu` y `asppp` para establecer un enlace con un equipo remoto. Esta información incluye lo siguiente:

- Nombre del host remoto
- Nombre del dispositivo de conexión asociado con el equipo remoto
- Hora en la que se puede acceder al host
- Número de teléfono
- ID de inicio de sesión
- Contraseña

Otros archivos se pueden considerar parte de la base de datos auxiliar, pero no participan directamente en el establecimiento de un enlace ni en la transferencia de archivos.

Configuración de archivos de base de datos del UUCP

La base de datos del UUCP consta de los archivos que se muestran en “Archivos de base de datos del UUCP” [169]. Sin embargo, la configuración básica del UUCP sólo involucra los siguientes archivos críticos:

- `/etc/uucp/Systems`
- `/etc/uucp/Devices`
- `/etc/uucp/Dialers`

Debido a que `asppp` utiliza algunas de las bases de datos del UUCP, debe comprender, como mínimo, estos archivos de base de datos críticos si planea configurar `asppp`. Después de que estas bases de datos se configuran, la administración del UUCP es bastante sencilla. Normalmente, primero edita el archivo `Systems` y luego edita el archivo `Devices`. Por lo general, puede utilizar el archivo predeterminado `/etc/uucp/Dialers`, a menos que planee agregar marcadores que no están en el archivo predeterminado. Además, es posible que también desee utilizar los siguientes archivos para la configuración básica del UUCP y `asppp`:

- `/etc/uucp/Sysfiles`
- `/etc/uucp/Dialcodes`
- `/etc/uucp/Sysname`

Dado que estos archivos trabajan de forma estrecha entre ellos, debe comprender todo su contenido antes de realizar cambios. Un cambio en una entrada de un archivo puede exigir un cambio en una entrada relacionada de otro archivo. El resto de los archivos que aparecen en “Archivos de base de datos del UUCP” [169] no están tan críticamente entrelazados.

Nota - `asppp` utiliza sólo los archivos que se describen en esta sección. `asppp` no utiliza los otros archivos de base de datos del UUCP.

♦ ♦ ♦ CAPÍTULO 11

Administración de programa de copia de UNIX a UNIX

En este capítulo, se explica cómo iniciar operaciones del UUCP después de modificar el archivo de base de datos que corresponde a sus equipos. El capítulo contiene información sobre procedimientos y resolución de problemas para configurar y mantener el UUCP en equipos que ejecutan el sistema operativo Oracle Solaris, como los siguientes:

Administración del UUCP (mapa de tareas)

En la siguiente tabla, se proporcionan referencias a los procedimientos que se cubren en este capítulo, además de una breve descripción de cada procedimiento.

TABLA 11-1 Mapa de tareas para la administración del UUCP

Tarea	Descripción	Para obtener instrucciones
Permitir que los equipos remotos tengan acceso al sistema	Edite el archivo `/etc/passwd` para agregar entradas con el fin de identificar los equipos que tienen permiso para acceder al sistema.	Cómo agregar inicios de sesión del UUCP [172]
Iniciar el UUCP	Utilice las secuencias de comandos de shell proporcionadas para iniciar el UUCP.	Cómo iniciar el UUCP [173]
Activar el UUCP para trabajar con TCP/IP	Editar los archivos `/etc/uucp/Systems` para activar el UUCP para TCP/IP.	Cómo activar el UUCP para TCP/IP [175]
Solucionar algunos problemas comunes del UUCP	Utilice los pasos de diagnóstico para comprobar si existen módems o ACU con errores.	Cómo comprobar si existen módems o ACU con errores [178]
	Utilice los pasos de diagnóstico para depurar transmisiones.	Cómo depurar transmisiones [178]

Agregación de inicios de sesión del UUCP

Para que las solicitudes (`uucico`) entrantes del UUCP de las máquinas remotas se administren correctamente, cada máquina debe tener un inicio de sesión en su sistema.

▼ Cómo agregar inicios de sesión del UUCP

Para permitir que un equipo remoto acceda al sistema, es necesario agregar una entrada al archivo `/etc/passwd` de la siguiente manera:

1. **Conviértase en administrador.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Edite el archivo `/etc/passwd` y agregue la entrada para identificar el equipo que tiene permiso para acceder al sistema.**
   Una entrada típica que puede incluir en el archivo `/etc/passwd` para una máquina remota que tiene permitido acceder al sistema con una conexión del UUCP sería de la siguiente manera:

   ```
   Ugobi:*:5:5:gobi:/var/spool/uucppublic:/usr/lib/uucp/uucico
   ```

   Por convención, el nombre de inicio de sesión de un equipo remoto es el nombre de equipo precedido por la letra en mayúscula `U`. Tenga en cuenta que el nombre no debe exceder los ocho caracteres. De lo contrario, puede que tenga que truncar o abreviar el nombre.
   La entrada anterior muestra que una solicitud de inicio de sesión por `Ugobi` es respondida por `/usr/lib/uucp/uucico`. El directorio principal es `/var/spool/uucppublic`. La contraseña se obtiene del archivo `/etc/shadow`. Debe coordinar la contraseña y el nombre de inicio de sesión con el administrador del UUCP del equipo remoto. El administrador remoto debe agregar una entrada adecuada, con el nombre de inicio de sesión y la contraseña sin cifrar, en el archivo `Systems`de la máquina remota.

3. **Coordine el nombre del equipo con los administradores del UUCP de otros sistemas.**
   De manera similar, debe coordinar el nombre y la contraseña de la máquina con los administradores del UUCP de todas las máquinas que desea alcanzar mediante el UUCP.

Inicio del UUCP

El UUCP incluye cuatro secuencias de comandos de shell que sondean máquinas remotas, reprograman transmisiones y borran archivos log antiguos y transmisiones incorrectas. Las secuencias de comandos son las siguientes:

- `uudemon.poll`
- `uudemon.hour`
- `uudemon.admin`
- `uudemon.cleanup`

Estas secuencias de comandos de shell se deben ejecutar con regularidad para garantizar que el UUCP se ejecute sin problemas. El archivo `crontab` para ejecutar las secuencias de comandos se crea automáticamente en `/usr/lib/uucp/uudemon.crontab` como parte del proceso de instalación de Oracle Solaris si selecciona la instalación completa. De lo contrario, el archivo se crea al instalar el paquete del UUCP.

También puede ejecutar las secuencias de comandos de shell del UUCP manualmente. El siguiente es el archivo `uudemon.crontab` prototipo que puede personalizar para un equipo determinado:

```
#
#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
```

Nota - De manera predeterminada, las operaciones del UUCP están desactivadas. Para activar el UUCP, edite la programación de tiempo y elimine el comentario de las líneas adecuadas en el archivo `uudemon.crontab`.

▼ Cómo iniciar el UUCP

Para activar el archivo `uudemon.crontab`, realice los siguientes pasos:

1. **Conviértase en administrador.**
   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Edite el archivo `/usr/lib/uucp/uudemon.crontab` y cambie las entradas según sea necesario.**

3. **Active el archivo `uudemon.crontab` mediante la ejecución de este comando:**

   ```
   crontab < /usr/lib/uucp/uudemon.crontab
   ```

Secuencia de comandos de shell `uudemon.poll`

La secuencia de comandos de shell `uudemon.poll` predeterminada lee el archivo `/etc/uucp/Poll` una vez por hora. Si alguna máquina en el archivo `Poll` está programada para ser sondeada, un archivo de trabajo (`C.`*sysnxxxx*) se coloca en el directorio `/var/spool/uucp/`*nodename*. *nodename* representa el nombre de nodo del UUCP de la máquina.

La secuencia de comandos de shell está programada para ejecutarse una vez por hora, antes de `uudemon.hour`, para que los archivos de trabajo estén en su lugar cuando se llama a `uudemon.hour`.

Secuencia de comandos de shell `uudemon.hour`

La secuencia de comandos de shell `uudemon.hour` predeterminada realiza lo siguiente:

- Llama al programa `uusched` para buscar en los directorios de cola de impresión archivos de trabajo (`C.`) que no han sido procesados. La secuencia de comandos programa estos archivos para transferirlos a un equipo remoto.
- Llama al daemon `uuxqt` para buscar en los directorios de cola de impresión archivos ejecutables (`X.`) que se transfirieron a su equipo y no se procesaron cuando se transfirieron.

De manera predeterminada, `uudemon.hour` se ejecuta dos veces por hora. Puede que desee que `uudemon.hour` se ejecute con más frecuencia si espera un elevado porcentaje de fallos de llamadas a equipos remotos.

Secuencia de comandos de shell `uudemon.admin`

La secuencia de comandos de shell `uudemon.admin` predeterminada realiza lo siguiente:

- Ejecuta el comando `uustat` con las opciones `p` y `q`. La opción `q` informa sobre el estado de archivos de trabajo (`C.`), archivos de datos (`D.`) y archivos ejecutables (`X.`) que están en cola. La opción `p` imprime información de proceso de procesos de red que figuran en los archivos de bloqueo (`/var/spool/locks`).
- Envía información de estado resultante al inicio de sesión administrativo de `uucp` mediante `mail`.

Secuencia de comandos de shell `uudemon.cleanup`

La secuencia de comandos de shell `uudemon.cleanup` predeterminada realiza lo siguiente:

- Recopila archivos log para máquinas individuales del directorio `/var/uucp/.Log`, fusiona dichos archivos y coloca los archivos en el directorio `/var/uucp/.Old` con la otra información de registro antigua.
- Elimina los archivos de trabajo (`C.`) de siete días o más de antigüedad, los archivos de datos (`D.`) de siete días o más de antigüedad y archivos ejecutables (`X.`) de dos días o más de antigüedad de los archivos de la cola de impresión.
- Devuelve correo que no se puede entregar al remitente.
- Envía un resumen de la información de estado recopilada durante el día actual de inicio administrativo del UUCP (`uucp`)

Ejecución del UUCP mediante TCP/IP

Para ejecutar el UUCP en una red TCP/IP, debe efectuar algunas modificaciones, como se describe en esta sección.

▼ Cómo activar el UUCP para TCP/IP

1. **Conviértase en administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Edite el archivo `/etc/uucp/Systems` para garantizar que las entradas tengan los siguientes campos:**

   System-Name Time TCP Port networkname Standard-Login-Chat

   Una entrada típica sería similar a la siguiente:

   ```
   rochester Any TCP - ur-seneca login: Umachine password: xxx
   ```

   Tenga en cuenta que el campo *networkname* permite especificar de forma explícita el nombre de host del TCP/IP. Esta capacidad es importante para algunos sitios. En el ejemplo anterior, el sitio tiene el nombre de nodo `rochester` del UUCP, que es diferente del nombre de host `ur-seneca` del TCP/IP. Además, un equipo completamente diferente podría ejecutar el UUCP con facilidad y tener el nombre de host `rochester` para el TCP/IP.

   El campo Port del archivo `Systems` debe tener la entrada `-`. Esta sintaxis equivale a enumerar la entrada como `uucp`. En casi todas las situaciones, el campo *networkname* es el mismo que el nombre del sistema, y el campo Port es `-`, que indica que se debe utilizar el puerto uucp estándar de la base de datos `services`. El daemon `in.uucpd` espera que el equipo remoto envíe su inicio de sesión y contraseña para la autenticación, y, además, el daemon `in.uucpd` los solicita, al par que los comandos `getty` y `login`.

3. **Edite el archivo `/etc/inet/services` para configurar un puerto para el UUCP:**

```
uucp    540/tcp    uucpd        # uucp daemon
```

No debería tener que cambiar la entrada. Sin embargo, si su máquina ejecuta NIS como servicio de nombres, debe asegurarse de que `config/service` del servicio `svc:/system/name-service/switch` compruebe `files` antes que `nis`. Si la propiedad `config/service` no está definida, marque la propiedad `config/default`.

4. **Verifique que el UUCP esté activado.**

```
# svcs network/uucp
```

El servicio UUCP es administrado por la utilidad de gestión de servicios. Para consultar el estado de este servicio, puede utilizar el comando `svcs`. Para obtener una descripción general de la Utilidad de gestión de servicios, consulte “Gestión de instancias de servicio SMF” de “Gestión de los servicios del sistema en Oracle Solaris 11.2 ”.

5. **(Opcional) Si es necesario, active el UUCP escribiendo lo siguiente:**

```
# inetadm -e network/uucp
```

Seguridad y mantenimiento del UUCP

Una vez que ha configurado el UUCP, el mantenimiento es sencillo. En esta sección, se explican las tareas del UUCP en curso que se relacionan con la seguridad, el mantenimiento y la resolución de problemas.

Configuración de la seguridad del UUCP

El archivo `/etc/uucp/Permissions` predeterminado proporciona el mayor nivel de seguridad para los enlaces del UUCP. El archivo `Permissions` predeterminado no contiene entradas.

Puede configurar parámetros adicionales para cada uno de los equipos remotos para definir lo siguiente:

- Las maneras en las que el equipo remoto puede recibir archivos de su equipo.
- Los directorios para los cuales el equipo remoto leyó y escribió permisos.
- Los comandos que el equipo remoto puede utilizar para la ejecución remota.

Una entrada `Permissions` típica es de la siguiente manera:

```
MACHINE=datsun LOGNAME=Udatsun VALIDATE=datsun
COMMANDS=rmail REQUEST=yes SENDFILES=yes
```

Esta entrada permite que los archivos sean enviados hacia los directorios “comunes” del UUCP y que sean recibidos desde ellos, y no desde cualquier lugar en el sistema. La entrada también genera que el nombre de usuario del UUCP sea validado en el momento del inicio de sesión.

Mantenimiento regular del UUCP

El UUCP no requiere demasiado mantenimiento. Sin embargo, debe asegurarse de que el archivo `crontab` esté en su lugar, como se describe en la sección Cómo iniciar el UUCP [173]. Su preocupación debe ser el aumento de la cantidad de archivos de correo y el directorio público.

Correo electrónico para el UUCP

Todos los mensajes de correo electrónico generados por secuencias de comandos y programas del UUCP son enviados al ID de usuario `uucp`. Si no inicia sesión con frecuencia como ese usuario, es posible que no se dé cuenta de que el correo se está acumulando y está consumiendo espacio en el disco. Para solucionar este problema, cree un alias en `/etc/mail/aliases` y redirija ese correo electrónico a `root` o a usted o a otras personas que sean responsables de mantener el UUCP. Recuerde ejecutar el comando `newaliases` después de modificar el archivo `aliases`.

Directorio público del UUCP

El directorio `/var/spool/uucppublic` es el único lugar de cada sistema en el cual el UUCP puede copiar archivos de manera predeterminada. Cada usuario tiene permiso para cambiar a `/var/spool/uucppublic` y leer y escribir archivos en el directorio. Sin embargo, el bit de permanencia del directorio está establecido, por lo que el modo del directorio es 01777. Como consecuencia, los usuarios no pueden eliminar archivos que se han copiado en él y que pertenecen a `uucp`. Sólo usted, como administrador del UUCP que inició sesión como `root` o `uucp`, puede eliminar archivos de este directorio. Para evitar la acumulación sin control de archivos en este directorio, debe asegurarse de eliminar archivos de él periódicamente.

Si este mantenimiento no es conveniente para los usuarios, debe alentarlos a que utilicen `uuto` y `uupick` en lugar de eliminar el bit de permanencia, que está establecido por motivos de seguridad. Consulte la página del comando man `uuto`(1C) para obtener instrucciones sobre cómo utilizar `uuto` y `uupick`. También puede restringir el modo del directorio a un único grupo de personas. Si no desea arriesgarse a que alguien llene su disco, incluso puede denegar el acceso del UUCP a él.

Resolución de problemas del UUCP

Estos procedimientos describen cómo resolver problemas comunes del UUCP.

▼ Cómo comprobar si existen módems o ACU con errores

Puede comprobar si los módems u otras unidades de llamada automática no están funcionando correctamente de varias maneras.

1. **Conviértase en administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Para obtener recuentos y motivos del error de contacto, ejecute el siguiente comando:**

   ```
   # uustat -q
   ```

3. **Llame por una línea en particular e imprima la información de depuración en el intento.**

   La línea se debe definir como `direct` en el archivo `/etc/uucp/Devices`. Debe agregar un número de teléfono al final de la línea de comandos si la línea está conectada a un marcador automático, o el dispositivo debe estar configurado como `direct`. Escriba:

   ```
   # cu -d -lline
   ```

   line es `/dev/cua/a`.

▼ Cómo depurar transmisiones

Si no puede ponerse en contacto con una máquina particular, puede comprobar las comunicaciones con esa máquina mediante `Uutry` y `uucp`.

1. **Conviértase en administrador.**

   Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

2. **Intente establecer contacto:**

```
# /usr/lib/uucp/Uutry -r machine
```

Reemplace *machine* con el nombre de host del equipo con el cual no puede establecer contacto. Este comando realiza lo siguiente:

- Inicia el daemon de transferencia (`uucico`) con depuración. Puede obtener más información sobre depuración si usted es `root`.
- Dirige los resultados de la depuración a `/tmp/`*machine*.
- Imprime la salida de depuración en el terminal mediante la ejecución de este comando:

  ```
  # tail -f
  ```

  Presione Control+C para finalizar la salida. Puede copiar la salida de `/tmp/`*machine* si desea guardar la salida.

3. **Si `Uutry` no aísla el problema, intente poner en cola un trabajo:**

```
# uucp -r file machine\!/dir/file
```

file	Utilice el nombre del archivo que desea transferir.
machine	Utilice el nombre del equipo en el que desee copiar.
/dir/file	Especifique la ubicación del archivo para el otro equipo.

4. **Use el siguiente comando:**

```
# Uutry
```

Si aún no puede resolver el problema, es posible que tenga que llamar a su representante de asistencia técnica local. Guarde la salida de depuración, que puede ayudar a diagnosticar el problema.

Nota - También puede aumentar o disminuir el nivel de depuración proporcionado por `Uutry` por medio de la opción `-x` *n*. *n* indica el nivel de depuración. El nivel de depuración predeterminado para `Uutry` es 5.

El nivel de depuración 3 proporciona información básica sobre cuándo y cómo se establece la conexión, pero no proporciona mucha información sobre la transmisión. El nivel de depuración 9, sin embargo, proporciona información exhaustiva sobre el proceso de transmisión. Tenga en cuenta que la depuración se produce en ambos extremos de la transmisión. Si tiene previsto utilizar un nivel superior al 5 en un texto moderadamente extenso, póngase en contacto con el administrador de otro sitio y decida cuándo cambiar el nivel.

Comprobación del archivo `/etc/uucp/Systems` del UUCP

Verifique que cuenta con información actualizada en el archivo `Systems` si tiene problemas para ponerse en contacto con una máquina determinada. La información que puede estar desactualizada para un equipo es la siguiente:

- Número de teléfono
- ID de inicio de sesión
- Contraseña

Comprobación de mensajes de error del UUCP

El UUCP tiene dos tipos de mensajes de error: `ASSERT` y `STATUS`.

- Cuando un proceso se cancela, los mensajes de error, `ASSERT` se registran en `/var/uucp/.Admin/errors`. Estos mensajes incluyen el nombre de archivo, `sccsid`, el número de línea y el texto. Estos mensajes, por lo general, se generan a partir de problemas del sistema.
- Los mensajes de error `STATUS` se almacenan en el directorio `/var/uucp/.Status`. El directorio contiene un archivo separado para cada uno de los equipos remotos con los cuales su equipo intenta comunicarse. Estos archivos contienen información de estado sobre la comunicación que se intentó establecer y si la comunicación se ha realizado correctamente.

Comprobación de información básica

Hay varios comandos disponibles para comprobar la información básica de la red:

- Utilice el comando `uuname` para enumerar las máquinas con los cuales su máquina se puede poner en contacto.
- Utilice el comando `uulog` para visualizar el contenido de los directorios de registro de hosts particulares.
- Utilice el comando `uucheck -v` para comprobar la presencia de archivos y directorios que son necesarios para `uucp`. Este comando también comprueba el archivo `Permissions` y muestra información sobre los permisos que ha configurado.

♦ ♦ ♦ CAPÍTULO 12

Archivos de programa de copia de UNIX a UNIX

En este capítulo, se proporciona información de referencia para trabajar con el UUCP. Se tratan los temas siguientes:

Archivo `/etc/uucp/Systems` del UUCP

El archivo `/etc/uucp/Systems` contiene la información que necesita el daemon `uucico` para establecer un enlace de comunicación a un equipo remoto. `/etc/uucp/Systems` es el primer archivo que necesita editar para configurar el UUCP.

Cada entrada del archivo `Systems` representa un equipo remoto con el cual se comunica el host. Un host determinado puede tener más de una entrada. Las entradas adicionales representan rutas de comunicación alternativas que se prueban en orden secuencial. Además, de manera predeterminada, el UUCP evita que cualquier equipo que no aparece en `/etc/uucp/Systems` inicie sesión en el host.

Al usar el archivo `Sysfiles`, puede definir varios archivos que se utilizarán como archivos `Systems`. Consulte "Archivo `/etc/uucp/Sysfiles` del UUCP" [200] para obtener una descripción de `Sysfiles`.

La siguiente es la sintaxis de una entrada del archivo `Systems`:

```
System-Name    Time    Type    Speed    Phone    Chat Script
```

Consulte el ejemplo siguiente de una entrada en el archivo `Systems`.

EJEMPLO 12-1 Entrada en `/etc/uucp/Systems`

```
Arabian     Any  ACUEC 38400 111222  ogin: Puucp ssword:beledi
```

`Arabian`	Entrada para el campo System-Name. Para obtener más información, consulte "Campo System-Name en el archivo /etc/uucp/Systems" [182].
`Any`	Entrada para el campo Time. Para obtener más información, consulte "Campo Time en el archivo /etc/uucp/Systems" [182].
`ACUEC`	Entrada para el campo Type. Para obtener más información, consulte "Campo Type en el archivo /etc/uucp/Systems" [184].
`38400`	Entrada para el campo Speed. Para obtener más información, consulte "Campo Speed en el archivo /etc/uucp/Systems" [184].
`111222`	Entrada para el campo Phone. Para obtener más información, consulte "Campo Phone en el archivo /etc/uucp/Systems" [184].
`ogin: Puucp ssword:beledi`	Entrada para el campo Chat Script. Para obtener más información, consulte "Campo Chat-Script en el archivo /etc/uucp/Systems" [185].

Campo System-Name en el archivo `/etc/uucp/Systems`

Este campo contiene el nombre de nodo del equipo remoto. En redes TCP/IP, este nombre puede ser el nombre de host del equipo o un nombre que se crea específicamente para las comunicaciones del UUCP por medio del archivo `/etc/uucp/Sysname`. Consulte "Archivo /etc/uucp/Systems del UUCP" [181]. En el Ejemplo 12-1, "Entrada en /etc/uucp/Systems", el campo System-Name contiene una entrada para el host remoto `Arabian`.

Campo Time en el archivo `/etc/uucp/Systems`

Este campo especifica el día de la semana y la hora del día en los que se puede llamar al equipo remoto. El formato del campo Time es el siguiente:

```
daytime[;retry]
```

Parte *day* del campo Time

La parte *day* puede ser una lista que contiene algunas de las siguientes entradas.

`Su Mo Tu We Th Fr Sa`	Para días individuales.
`Wk`	Para cualquier día de la semana.
`Any`	Para cualquier día.
`Never`	El host nunca inicia una llamada al equipo remoto. La llamada debe ser iniciada por el equipo remoto. El host funciona en *modo pasivo*.

Parte *time* del campo Time

Ejemplo 12-1, “Entrada en `/etc/uucp/Systems`” muestra `Any` en el campo Time, lo que indica que es posible llamar al host `Arabian`en cualquier momento.

La parte *time* debe ser un rango de horas que se especifican en una notación de 24 h, por ejemplo, `0800-1230` para el rango de 8:30 a. m. a 12:30 p. m. Si no hay ninguna parte *time* especificada, se asume que cualquier hora del día está permitida para la llamada.

Un rango de horas que abarca 0000 está permitido. Por ejemplo, `0800-0600` significa que todas las horas están permitidas, excepto las horas entre 6 a. m. y 8 a. m.

Parte *retry* del campo Time

El subcampo *retry* permite especificar el tiempo mínimo (en minutos) antes de un reintento, después de un intento fallido. La espera predeterminada es de 60 min. El separador de subcampo es un punto y coma (;). Por ejemplo, `Any;9` se interpreta como que se puede llamar en cualquier momento, pero se debe esperar al menos 9 min antes de volver a intentar después de que se produce un fallo.

Si no especifica una entrada *retry*, se utiliza un algoritmo de interrupción exponencial. Esto significa que el UUCP se inicia con un tiempo de espera predeterminado que aumenta a medida que el número de intentos fallidos aumenta. Por ejemplo, suponga que el tiempo de reintento inicial es de 5 min. Si no se produce ninguna respuesta, el siguiente reintento es 10 min más tarde. El siguiente reintento es 20 min más tarde, y así sucesivamente hasta que se alcanza el

máximo tiempo de reintento de 23 h. Si *retry* se especifica, el valor especificado es siempre el tiempo de reintento. De lo contrario, se utiliza el algoritmo de interrupción.

Campo Type en el archivo /etc/uucp/Systems

Este campo contiene el tipo de dispositivo que debe utilizarse para establecer el enlace de comunicación al equipo remoto. La palabra clave que se utiliza en este campo se compara con el primer campo de las entradas del archivo Devices.

EJEMPLO 12-2 Palabra clave con el campo Type

```
Arabian    Any    ACUEC, g    38400    1112222    ogin: Puucp ssword:beledi
```

Puede definir el protocolo que se utiliza para ponerse en contacto con el sistema agregando el protocolo en el campo Type. El ejemplo anterior muestra la forma de agregar el protocolo g al tipo de dispositivo ACUEC. Para obtener más información sobre protocolos, consulte "Definiciones de protocolo en el archivo /etc/uucp/Devices" [194].

Campo Speed en el archivo /etc/uucp/Systems

Este campo, también conocido como el campo Class, especifica la velocidad de transferencia del dispositivo que se utiliza para establecer el enlace de comunicación. El campo de velocidad del UUCP puede contener una letra y una velocidad, como C1200 o D1200, para diferenciar entre las clases de marcadores. Consulte "Campo Class en el archivo /etc/uucp/Devices" [191].

Algunos dispositivos se pueden utilizar a cualquier velocidad, por lo que la palabra clave Any se puede utilizar. Este campo debe coincidir con el campo Class en la entrada del archivo Devices asociada.

EJEMPLO 12-3 Entrada en el campo Speed

```
eagle    Any    ACU, g    D1200    NY3251    ogin: nuucp ssword:Oakgrass
```

Si no se requiere información para este campo, utilice un guión (-) como marcador de posición para el campo.

Campo Phone en el archivo /etc/uucp/Systems

Este campo permite especificar el número de teléfono, conocido como *token*, del equipo remoto para marcadores automáticos, conocidos como *port selectors*. El número de teléfono consta de

una abreviatura alfabética opcional y una parte numérica. Si se utiliza una abreviatura, dicha abreviatura debe estar enumerada en el archivo Dialcodes.

EJEMPLO 12-4 Entrada en el campo Phone

```
nubian    Any    ACU       2400    NY555-1212    ogin: Puucp ssword:Passuan
eagle     Any    ACU, g    D1200   NY=3251       ogin: nuucp ssword:Oakgrass
```

En el campo Phone, un signo igual (=) indica a la ACU que espere un tono de marcación secundario antes de marcar el resto de los dígitos. Un guión (-) en la cadena indica a la ACU que pause 4 s antes de marcar el siguiente dígito.

Si su equipo se encuentra conectado a un selector de puerto, puede acceder a otros equipos que están conectados a dicho selector. Las entradas del archivo Systems para esas máquinas remotas no deben tener un número de teléfono en el campo Phone. En cambio, este campo debe contener el token que se transferirá al conmutador. De esta forma, el selector de puerto sabe el equipo remoto con el que el host se desea comunicar. Por lo general, sólo sabe el nombre del sistema. La entrada del archivo Devices asociada debe indicar \D al final de la entrada para asegurarse de que este campo no sea traducido mediante el archivo Dialcodes.

Campo Chat-Script en el archivo /etc/uucp/Systems

Este campo, también conocido como el campo Login, contiene una cadena de caracteres denominada *chat-script*. La secuencia de comandos de chat contiene los caracteres que los equipos local y remoto se deben pasar entre ellos en la conversación inicial. Las secuencias de comandos de chat tienen el siguiente formato:

expect send [expect send] ....

expect representa la cadena que el host local espera recibir del host remoto para iniciar la conversación. *send* es la cadena que el host local envía después de que el host local recibe la cadena *expect* del host remoto. Una secuencia de comandos de chat puede tener más de una secuencia expect-send.

Una secuencia de comandos de chat básica puede contener lo siguiente:

- Indicador de inicio de sesión que el host local espera recibir del equipo remoto.
- Nombre de inicio de sesión que el host local envía al equipo remoto para iniciar la sesión.
- Indicador de contraseña que el host local espera recibir del equipo remoto.
- Contraseña que el host local envía al equipo remoto.

El campo *expect* puede estar compuesto por subcampos con el siguiente formato:

expect[-send-expect]...

El subcampo *-send* se envía si el subcampo *expect* anterior no se lee correctamente. El subcampo *-expect* que sigue al subcampo *-send* es la siguiente cadena esperada.

Por ejemplo, con cadenas `login--login`, el UUCP en el host local espera a `login`. Si el UUCP recibe `login` de la máquina remota, el UUCP pasa al campo siguiente. Si el UUCP no recibe a `login`, el UUCP envía un retorno de carro y, a continuación, busca a `login` de nuevo. Si el equipo local inicialmente no espera ningún carácter, utilice los caracteres `""`, para la cadena NULL, en el campo *expect*. Todos los campos *send* se envían con un retorno de carro agregado, a menos que la cadena *send* termine con `\c`.

El siguiente es un ejemplo de una entrada del archivo `Systems` que utiliza una cadena *expect-send*:

```
sonora Any ACUEC 9600 2223333 "" \r \r ogin:-BREAK-ogin: Puucpx ssword:xyzzy
```

En este ejemplo, se indica al UUCP en el host local que envíe dos retornos de carro y que espere por `ogin:` (para `Login:`). Si `ogin`: no se recibe, envíe un `BREAK`. Cuando se reciba `ogin:`, enviar el nombre de inicio de sesión `Puucpx`. Cuando se reciba `ssword:` (para `Password:`), enviar la contraseña `xyzzy`.

En la siguiente tabla, se muestran algunos caracteres de escape útiles.

TABLA 12-1 Caracteres de escape utilizados en el campo Chat-Script del archivo `Systems`

Carácter de escape	Significado
`\b`	Envía o espera un carácter de retroceso.
`\c`	Si se encuentra al final de una cadena, suprime el retorno de carro que normalmente se envía. De lo contrario, se ignora.
`\d`	Retrasa entre 1 s y 3 s antes de enviar más caracteres.
`\E`	Inicia la comprobación de eco. A partir de este punto, siempre que se transmite un carácter, el UUCP espera que se reciba el carácter antes de continuar las comprobaciones.
`\e`	Transmite la comprobación.
`\H`	Ignora un bloqueo del sistema. Utilice esta opción para módems con devolución de llamada.
`\K`	Envía un carácter de interrupción.
`\M`	Activa el indicador `CLOCAL`.
`\m`	Desactiva el indicador `CLOCAL`.
`\n`	Envía o espera un carácter de línea nueva.
`\N`	Envía un carácter nulo (ASCII NUL).
`\p`	Realiza una pausa de 1/4 s a 1/2 s aproximadamente.
`\r`	Envía o espera un retorno de carro.
`\s`	Envía o espera un carácter de espacio.
`\t`	Envía o espera un carácter de tabulación.
`EOT`	Envía un EOT, seguido de una línea nueva dos veces.
`BREAK`	Envía un carácter de interrupción.
`\`*ddd*	Envía o espera el carácter que está representado por los dígitos octales (*ddd*).

Activación de devolución de llamada por medio de la secuencia de comandos de chat

Algunas empresas configuran servidores de marcación de entrada para administrar llamadas de equipos remotos. Por ejemplo, su compañía puede tener un servidor de marcación de entrada con un módem de devolución de llamada al que los empleados pueden llamar desde sus equipos domésticos. Después de que el servidor de marcación de entrada identifica el equipo remoto, el servidor de llamada entrante desconecta el enlace al equipo remoto y, a continuación, devuelve la llamada al equipo remoto. Luego, el enlace de comunicación se restablece.

Puede facilitar la devolución de llamada mediante la opción `\H` en la secuencia de comandos de chat del archivo `Systems` en el lugar donde la devolución de llamada debe producirse. Incluya la opción `\H` como parte de una cadena expect en el lugar donde se espera que el servidor de marcación de entrada se bloquee.

Por ejemplo, suponga que la secuencia de comandos de chat que llama al servidor de marcación de entrada contiene la siguiente cadena:

```
INITIATED\Hogin:
```

La utilidad de marcación del UUCP en el equipo local espera recibir los caracteres `INITIATED` del servidor de marcación de entrada. Después de que los caracteres `INITIATED` se han comparado, la utilidad de marcación borra los caracteres subsiguientes que la utilidad de marcación recibe hasta que el servidor de marcación de entrada se bloquea. La utilidad de marcación local espera hasta recibir la parte siguiente de la cadena expect, los caracteres `ogin:`, del servidor de marcación de entrada. Cuando recibe a `ogin:`, la utilidad de marcación continúa a lo largo de la secuencia de comandos de chat.

Una cadena de caracteres no necesita preceder ni seguir directamente a `\H`, como se muestra en la cadena de ejemplo anterior.

Control de flujo de hardware en el archivo `/etc/uucp/Systems`

También puede utilizar la cadena pseudo-send `STTY=`*value* para definir las características del módem. Por ejemplo, `STTY=crtscts` permite el control de flujo de hardware saliente. `STTY` acepta todos los modos de `stty`. Consulte las páginas del comando man `stty`(1) y `termio`(7I) para obtener más información.

En el ejemplo siguiente, se activa el control de flujo de hardware en una entrada del archivo `Systems`:

```
unix Any ACU 2400 12015551212 "" \r ogin: Puucp ssword:Passuan "" \ STTY=crtscts
```

También puede utilizar la cadena pseudo-send en las entradas del archivo Dialers.

Configuración de paridad en el archivo /etc/uucp/Systems

En algunas situaciones, tiene que restablecer la paridad porque el sistema al que llama comprueba la paridad del puerto y elimina la línea si es incorrecta. El pareado expect-send "" P_ZERO establece el bit de orden superior (bit de paridad) en 0. Observe este pareado expect-send en el siguiente ejemplo:

```
unix Any ACU 2400 12015551212 "" P_ZERO "" \r ogin: Puucp ssword:Passuan
```

Los siguientes son pareados de paridad que pueden seguir al pareado expect-send "" P_ZERO:

"" P_EVEN	Establece la paridad en par, que es la predeterminada
"" P_ODD	Establece la paridad en impar
"" P_ONE	Establece el bit de paridad en 1

Estos pareados de paridad se pueden insertar en cualquier lugar de la secuencia de comandos de chat. Los pareados de paridad se aplican a toda la información de la secuencia de comandos de chat que sigue a "" P_ZERO, el pareado expect-send. Un pareado de paridad también se puede utilizar en las entradas del archivo Dialers. El ejemplo siguiente incluye el pareado de paridad "" P_ONE:

```
unix Any ACU 2400 12015551212 "" P_ZERO "" P_ONE "" \r ogin: Puucp ssword:Passuan
```

Archivo /etc/uucp/Devices del UUCP

El archivo /etc/uucp/Devices contiene información para todos los dispositivos que se pueden utilizar para establecer un enlace a un equipo remoto. Estos dispositivos incluyen ACU (que incluyen módems de alta velocidad), enlaces directos y conexiones de red.

Una entrada en el archivo /etc/uucp/Devices tiene la siguiente sintaxis:

```
Type   Line   Line2   Class   Dialer-Token-Pairs
```

La siguiente es una entrada del archivo Devices para un módem V.32 bis de U.S. Robotics que está agregado al puerto A y que se está ejecutando a 38.400 bps.

```
ACUEC   cua/a   -   38400   usrv32bis-ec
```

ACUEC	Entrada en el campo Type. Para obtener más información, consulte “Campo Type en el archivo /etc/uucp/Devices” [189].
cua/a	Entrada en el campo Line. Para obtener más información, consulte “Campo Line en el archivo /etc/uucp/Devices” [190].
-	Entrada en el campo Line2. Para obtener más información, consulte “Campo Line2 del archivo /etc/uucp/Devices” [191].
38400	Entrada en el campo Class. Para obtener más información, consulte “Campo Class en el archivo /etc/uucp/Devices” [191].
usrv32bis-ec	Entrada en el campo Dialer-Token-Pairs. Para obtener más información, consulte “Campo Dialer-Token-Pairs en el archivo /etc/uucp/Devices” [191].

Cada campo se describe en la siguiente sección.

Campo Type en el archivo /etc/uucp/Devices

Este campo describe el tipo de enlace que el dispositivo establece. El campo Type del UUCP puede contener una de las palabras clave que se describen en las secciones a continuación.

Palabra clave Direct

La palabra clave Direct aparece principalmente en las entradas para las conexiones del comando cu. Esta palabra clave indica que el enlace es un enlace directo a otro equipo o un selector de puerto. Cree una entrada separada para cada línea a la que desea hacer referencia por medio de la opción -l del comando cu.

Palabra clave ACU

La palabra clave ACU indica que el enlace a un equipo remoto (ya sea mediante cu, UUCP, asppp o Solaris PPP 4.0) se realiza por medio de un módem. Este módem puede conectarse directamente al equipo o indirectamente por medio de un selector de puerto.

Variable Port Selector

El selector de puerto es una variable que se reemplaza en el campo Type con el nombre de un selector de puerto. Los selectores de puerto son dispositivos que se adjuntan a una red que

solicita el nombre de un módem que llama y, a continuación, otorgan acceso. El archivo /etc/uucp/Dialers contiene secuencias de comandos de emisor de llamada solamente para los selectores de puerto micom y develcon. Puede agregar sus propias entradas de selector de puerto al archivo Dialers. Consulte “Archivo /etc/uucp/Dialers del UUCP” [195] para obtener más información.

Variable System-Name

Esta variable se sustituye por el nombre de una máquina en el campo Type e indica que el enlace es un enlace directo a ese equipo particular. Este esquema de denominación se utiliza para asociar la línea en esta entrada Devices con una entrada en /etc/uucp/Systems para el equipo *System-Name*.

Campos Type en el archivo Devices y en el archivo Systems

Ejemplo 12-5, “Comparación de los campos Type en el archivo Devices y en el archivo Systems” muestra una comparación de los campos de /etc/uucp/Devices y los campos de /etc/uucp/Systems. La palabra clave que se usa en el campo Type del archivo Devices se compara con el tercer campo de las entradas del archivo Systems. En el archivo Devices, el campo Type tiene la entrada ACUEC, que indica una unidad de llamada automática, en esta instancia, un módem V.32 bis. Este valor se compara con el campo Type del archivo Systems, que también contiene la entrada ACUEC. Consulte “Archivo /etc/uucp/Systems del UUCP” [181] para obtener más información.

EJEMPLO 12-5 Comparación de los campos Type en el archivo Devices y en el archivo Systems

A continuación se muestra un ejemplo de una entrada en el archivo Devices.

```
ACUEC cua/a - 38400 usrv32bis-ec
```

A continuación se muestra un ejemplo de una entrada en el archivo Systems.

```
Arabian Any ACUEC 38400 111222 ogin: Puucp ssword:beledi
```

Campo Line en el archivo /etc/uucp/Devices

Este campo contiene el nombre del dispositivo de la línea (conocido como puerto) que está asociado con la entrada Devices. Si el módem que está asociado con una entrada concreta se adjuntara al dispositivo /dev/cua/a (puerto de serie A), el nombre que se introduciría en este campo sería cua/a. Un indicador de control de módem opcional, M, se puede utilizar en el campo Line para indicar que el dispositivo debe abrirse sin esperar a un portador. Por ejemplo:

```
cua/a,M
```

Campo Line2 del archivo /etc/uucp/Devices

Este campo es un marcador de posición. Utilice siempre un guión (-) aquí. Los marcadores del tipo 801, que no son compatibles con el sistema operativo Oracle Solaris, utilizan el campo Line2. Los marcadores que no son del tipo 801, normalmente, no usan esta configuración, pero aún necesitan un guión en este campo.

Campo Class en el archivo /etc/uucp/Devices

El campo Class contiene la velocidad del dispositivo si la palabra clave ACU o Direct se utiliza en el campo Type. Sin embargo, el campo Class puede contener una letra y una velocidad, como C1200 o D1200, para diferenciar entre clases de marcadores, como Centrex o Dimension PBX.

Esta diferenciación es necesaria porque muchas oficinas más grandes pueden tener más de un tipo de red telefónica. Una red podría estar dedicada a atender sólo comunicaciones de oficina internas, mientras que otra red podría manejar las comunicaciones externas. En esta situación, debe distinguir las líneas que se deben utilizar para las comunicaciones internas y las líneas que se deben utilizar para las comunicaciones externas.

La palabra clave que se utiliza en el campo Class del archivo Devices se compara con el campo Speed del archivo Systems.

EJEMPLO 12-6 Campo Class en el archivo Devices

```
ACU   cua/a   -   D2400  hayes
```

Algunos dispositivos se pueden utilizar a cualquier velocidad, por lo que se puede utilizar la palabra clave Any en el campo Class. Si Any se utiliza, la línea coincide con cualquier velocidad solicitada en el campo Speed del archivo Systems. Si este campo es Any y el campo Speed del archivo Systems es Any, la velocidad predeterminada es 2400 bps.

Campo Dialer-Token-Pairs en el archivo /etc/uucp/Devices

El campo Dialer-Token-Pairs (DTP) contiene el nombre de un marcador y el token para pasarlo. El campo DTP tiene esta sintaxis:

dialer token [dialer token]

La parte *dialer* puede ser el nombre de un módem, un monitor de puerto o `direct` o `uudirect` para un dispositivo de enlace directo. Puede tener cualquier número de pares de marcador y token. Si la parte *dialer* no está presente, se toma de una entrada relacionada en el archivo `Systems`. La parte *token* se puede indicar inmediatamente después de la parte dialer.

El último par de marcador y token puede no estar presente, según el marcador asociado. En la mayoría de las situaciones, el último par contiene solamente una parte *dialer*. La parte *token* se recupera del campo Phone de la entrada del archivo `Systems` asociada.

Una entrada válida en la parte *dialer* puede estar definida en el archivo `Dialers` o puede ser uno de los tipos de marcador especiales. Estos tipos de marcador especiales se compilan con el software y, por lo tanto, están disponibles sin que haya entradas en el archivo `Dialers`. En la siguiente lista, se muestran los tipos de marcador especiales.

`TCP` Red TCP/IP

`TLI` Red de interfaz de nivel de transporte (sin STREAMS)

`TLIS` Red de interfaz de nivel de transporte (con STREAMS)

Consulte “Definiciones de protocolo en el archivo /etc/uucp/Devices” [194] para obtener más información.

Estructura del campo Dialer-Token-Pairs en el archivo `/etc/uucp/Devices`

El campo DTP se puede estructurar de cuatro maneras diferentes, según el dispositivo asociado con la entrada.

Consulte la primera manera en la que el campo DTP se puede estructurar:

Módems conectados directamente: si un módem está conectado directamente a un puerto en el equipo, el campo DTP de la entrada del archivo `Devices` tiene solamente un par. Este par sería, normalmente, el nombre del módem. Este nombre se utiliza para comparar la entrada del archivo `Devices` particular con una entrada en el archivo `Dialers`. Por lo tanto, el campo Dialer debe coincidir con el primer campo de la entrada de un archivo `Dialers`.

EJEMPLO 12-7 Campo Dialers para módems conectados directamente

```
Dialers   hayes =,-,  ""          \\dA\pTE1V1X1Q0S2=255S12=255\r\c
                                  \EATDT\T\r\c CONNECT
```

Tenga en cuenta que sólo la parte dialer (`hayes`) está presente en el campo DTP de la entrada del archivo `Devices`. Esto significa que el *token* que se pasará al marcador (en este caso, el

número de teléfono) se toma del campo Phone de la entrada de un archivo Systems. (\T está implícito, como se describe en el Ejemplo 12-9, “Campo Dialers del UUCP para módems conectados al selector de puerto”).

Consulte la segunda y la tercera maneras en las que el campo DTP se puede estructurar:

- **Enlace directo**: para un enlace directo a un equipo particular, el campo DTP de la entrada asociada debería contener la palabra clave direct. Esta condición es verdadera para ambos tipos de entradas de enlace directo, Direct y *System-Name*. Consulte “Campo Type en el archivo /etc/uucp/Devices” [189].
- **Equipos en el mismo selector de puerto**: si un equipo con el que se desea comunicar se encuentra en el mismo conmutador del selector de puerto que su equipo, su equipo primero debe acceder al conmutador. Luego, el conmutador establece la conexión con el otro equipo. Este tipo de entrada tiene sólo un par. La parte *dialer* se utiliza para comparar la entrada de un archivo Dialers.

EJEMPLO 12-8 Campo Dialers del UUCP para equipos en el mismo selector de puerto

```
Dialers    develcon ,""   ""            \pr\ps\c est:\007 \E\D\e \007
```

Tal como se indica, la parte *token* se deja en blanco. Esta designación indica que se recuperará del archivo Systems. La entrada del archivo Systems para este equipo contiene el token en el campo Phone, que se suele reservar para el número de teléfono del equipo. Consulte “Archivo /etc/uucp/Systems del UUCP” [181] para obtener detalles. Este tipo de DTP contiene un carácter de escape (\D), lo que asegura que el contenido del campo Phone no se interpreta como una entrada válida en el archivo Dialcodes.

Consulte la cuarta manera en la que el campo DTP se puede estructurar:

Módems conectados al selector de puerto: si un módem de alta velocidad está conectado a un selector de puerto, su equipo primero debe acceder al conmutador del selector de puerto. El conmutador establece la conexión con el módem. Este tipo de entrada necesita dos pares de marcador y token. La parte *dialer* de cada par (el quinto y el séptimo campos de la entrada) se utiliza para comparar entradas en el archivo Dialers, de la siguiente manera.

EJEMPLO 12-9 Campo Dialers del UUCP para módems conectados al selector de puerto

```
develcon ""     ""    \pr\ps\c  est:\007    \E\D\e      \007
ventel   =&-%   t""   \r\p\r\c  $           <K\T%\r>\c  ONLINE!
```

En el primer par, develcon es el marcador y vent es el token que se pasa al conmutador Develcon para indicarle qué dispositivo, como un módem Ventel, se debe conectar al equipo. Este token es único para cada selector de puerto, ya que cada conmutador se puede configurar de forma distinta. Después de que el módem Ventel se ha conectado, se accede al segundo par. Ventel es el marcador, y el token se recupera del archivo Systems.

Dos caracteres de escape pueden aparecer en un campo DTP:

- \T: indica que el campo Phone (*token*) se debe traducir mediante el archivo /etc/uucp/Dialcodes. Este carácter de escape se coloca normalmente en el archivo /etc/uucp/Dialers para cada secuencia de comandos de emisor de llamada que está asociada con un módem, como Hayes y U.S. Robotics. Por lo tanto, la traducción no se produce hasta que se accede a la secuencia de comandos del emisor.
- \D: indica que el campo Phone (*token*) no se debe traducir mediante el archivo /etc/uucp/Dialcodes file. Si no hay ningún carácter de escape especificado al final de una entrada Devices, \D se asume de manera predeterminada. \D también se utiliza en el archivo /etc/uucp/Dialers con entradas que están asociadas con conmutadores de red develcon y micom.

Definiciones de protocolo en el archivo /etc/uucp/Devices

Puede definir el protocolo para utilizar con cada dispositivo en /etc/uucp/Devices. Esta especificación suele ser innecesaria debido a que puede utilizar el valor predeterminado o definir el protocolo con el sistema particular al que está llamando. Consulte “Archivo /etc/uucp/Systems del UUCP” [181] para obtener detalles. Si no especifica el protocolo, debe utilizar el siguiente formato:

Type,*Protocol [parameters]*

Por ejemplo, puede utilizar TCP,te para especificar el protocolo TCP/IP.

En la siguiente tabla, se muestran los protocolos disponibles para el archivo Devices.

TABLA 12-2 Protocolos que se utilizan en /etc/uucp/Devices

Protocolo	Descripción
t	Este protocolo se utiliza normalmente para las transmisiones por medio de TCP/IP y otras conexiones fiables. t asume transmisiones libres de errores.
g	Este protocolo es un protocolo nativo del UUCP. g es lento, fiable y bueno para la transmisión por medio de líneas telefónicas ruidosas.
e	Este protocolo asume la transmisión por medio de canales libres de errores que están orientados a los mensajes, en contraposición a los canales orientados a la secuencia de bytes, como TCP/IP.
f	Este protocolo se utiliza para la transmisión por medio de conexiones X.25. f se basa en el control de flujo de la secuencia de datos y está destinado para trabajar mediante enlaces que se pueden (casi) garantizar como libres de errores, específicamente, los enlaces X.25/PAD. Una suma de comprobación se aprueba por medio de un archivo completo solamente. Si un transporte falla, el receptor puede solicitar retransmisión o retransmisiones.

A continuación aparece un ejemplo que muestra una designación de protocolo para una entrada de dispositivo:

```
TCP,te - - Any TCP -
```

En este ejemplo, se indica que, para el dispositivo `TCP`, debe intentar utilizar el protocolo `t`. Si el otro extremo de la transmisión lo rechaza, utilice el protocolo `e`.

Ni `e` ni `t` son apropiados para utilizar mediante módems. Incluso si el módem garantiza una transmisión libre de errores, los datos aún se pueden perder entre el módem y la CPU.

Archivo `/etc/uucp/Dialers` del UUCP

El archivo `/etc/uucp/Dialers` contiene instrucciones de marcación para los módems que se utilizan con más frecuencia. Es probable que no sea necesario cambiar ni agregar entradas en este archivo, a menos que planee utilizar un módem no estándar o planee personalizar el entorno del UUCP. No obstante, debe comprender lo que hay en el archivo y cómo se relaciona con los archivos `Systems` y `Devices`.

El texto especifica la conversación inicial que debe producirse en una línea antes de que la línea pueda ponerse disponible para la transferencia de datos. Esta conversación, conocida como secuencia de comandos de chat, suele ser una secuencia de cadenas ASCII que se transmite y se espera. Una secuencia de comandos de chat se suele utilizar para marcar un número de teléfono.

Como se muestra en los ejemplos en “Archivo /etc/uucp/Devices del UUCP” [188], el quinto campo en una entrada del archivo `Devices` es un índice en el archivo `Dialers` o un tipo de marcador especial, como `TCP`, `TLI` o `TLIS`. El daemon `uucico` intenta comparar el quinto campo del archivo `Devices` con el primer campo de cada entrada del archivo `Dialers`. Además, cada campo `Devices` impar, a partir de la séptima posición, se utiliza como un índice en el archivo `Dialers`. Si la comparación tiene éxito, la entrada `Dialers` se interpreta para realizar la conversación del marcador.

Cada entrada en el archivo `Dialers` tiene la siguiente sintaxis:

```
dialer   substitutions   expect-send
```

El ejemplo siguiente muestra la entrada de un módem V.32 bis de U.S. Robotics.

EJEMPLO 12-10 Entrada en el archivo `/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`

Entrada en campo Dialer. El campo Dialer coincide con el quinto campo y con los campos impares adicionales en el archivo `Devices`.

`=,-, ""`

Entrada en el campo Substitutions. El campo Substitutions es una cadena de traducción. El primero de cada par de caracteres se asigna al segundo carácter del par. Esta asignación se utiliza normalmente para traducir = y - en lo que necesite el marcador para "esperar tono de marcación" y "pausar".

`dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r`

Entrada en el campo Expect-Send. Los campos Expect-Send son cadenas de caracteres.

`\EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts`

Más información sobre el campo Expect-Send.

A continuación, se muestran entradas de ejemplo en el archivo `Dialers` file, como se distribuyen al instalar el UUCP como parte del programa de instalación de Oracle Solaris.

EJEMPLO 12-11 Segmentos de `/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
```

En la siguiente tabla, se muestran los caracteres de escape que se utilizan normalmente en las cadenas de envío del archivo `Dialers`.

TABLA 12-3 Caracteres de barra diagonal inversa para `/etc/uucp/Dialers`

Carácter	Descripción
`\b`	Envía o espera un carácter de retroceso.
`\c`	No hay una línea nueva ni un retorno de carro.
`\d`	Retrasa durante 2 s aproximadamente.
`\D`	Número de teléfono o token sin traducción de `Dialcodes`.
`\e`	Desactiva la comprobación de eco.
`\E`	Activa la comprobación de eco para dispositivos lentos.
`\K`	Inserta un carácter de interrupción.
`\n`	Envía una línea nueva.
`\nnn`	Envía un número octal. En la sección “Archivo /etc/uucp/Systems del UUCP” [181], se muestran los caracteres de escape adicionales que se pueden utilizar.
`\N`	Envía o espera un carácter nulo (ASCII NUL).
`\p`	Realiza una pausa de 12 s a 14 s aproximadamente.
`\r`	Devuelve.
`\s`	Envía o espera un carácter de espacio.
`\T`	Número de teléfono o token con traducción de `Dialcodes`.

Esta es una entrada `penril` en el archivo `Dialers`:

```
penril =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
```

En primer lugar, se establece el mecanismo de sustitución para el argumento de número de teléfono, de modo que cualquier `=` se reemplaza por una `W` (esperar tono de marcación) y cualquier `-` se reemplaza por una `P` (pausar).

El protocolo de enlace indicado por el resto de la línea funciona como se muestra:

- `""`: no espera nada, lo que significa que se debe continuar con el siguiente paso.

- \d: retrasa 2 s y luego envía un retorno de carro.
- >: espera un >.
- Q\c: envía una Q sin un retorno de carro.
- ::: espera un :.
- \d-: retrasa 2 s y envía un - y un retorno de carro.
- >: espera un >.
- s\p9\c: envía una s, pausa y envía un 9 sin ningún retorno de carro.
-)-W\p\r\ds\p9\c-): espera un). Si) no se recibe, procesa la cadena entre los caracteres -, como se indica a continuación. Envía una W, pausa, envía un retorno de carro, retrasa, envía una s, pausa, envía un 9 sin un retorno de carro y, a continuación, espera el).
- y\c: envía una y sin ningún retorno de carro.
- ::: espera un :.
- \E\TP – \E activa la comprobación de eco. A partir de este punto, siempre que se transmite un carácter, el UUCP espera que se reciba el carácter antes de continuar. A continuación, el UUCP envía el número de teléfono. \T significa que se debe tomar el número de teléfono que se pasa como un argumento. \T aplica la traducción de Dialcodes y la traducción de la función del módem especificada por el campo 2 de esta entrada. A continuación, \T envía una P y un retorno de carro.
- >: espera un >.
- 9\c: envía un 9 sin una línea nueva.
- OK: espera la cadena OK.

Activación del control de flujo de hardware en el archivo /etc/uucp/Dialers

También puede utilizar la cadena pseudo-send STTY=*value* para definir las características del módem. Por ejemplo, STTY=crtscts permite el control de flujo de hardware saliente. STTY=crtsxoff permite el control de flujo de hardware entrante. STTY=crtscts,crtsxoff permite el control de flujo de hardware entrante y saliente.

STTY acepta todos los modos de stty. Consulte las páginas del comando man stty(1) y termio(7I).

En el ejemplo siguiente, se activaría el control de flujo de hardware en una entrada Dialers:

```
dsi =,–, "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts
```

Esta cadena pseudo-send también se puede utilizar en las entradas del archivo Systems.

Configuración de paridad en el archivo `/etc/uucp/Dialers`

En algunas situaciones, tiene que restablecer la paridad porque el sistema al que llama comprueba la paridad del puerto y elimina la línea si es incorrecta. El pareado expect-send `P_ZERO` establece la paridad en cero:

```
foo =,-, "" P_ZERO "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r\EATDT\T\r\c CONNECT
```

Los siguientes son pareados de paridad que pueden seguir al pareado expect-send:

`"" P_EVEN`	Establece la paridad en par, que es la predeterminada
`"" P_ODD`	Establece la paridad en impar
`"" P_ONE`	Establece la paridad en uno

Esta cadena pseudo-send también se puede utilizar en las entradas del archivo `Systems`.

Otros archivos de configuración básica del UUCP

Puede utilizar archivos de esta sección además de los archivos `Systems`, `Devices` y `Dialers` al realizar la configuración básica del UUCP.

Archivo `/etc/uucp/Dialcodes` del UUCP

El archivo `/etc/uucp/Dialcodes` permite definir abreviaturas de código de marcación que se pueden utilizar en el campo Phone del archivo `/etc/uucp/Systems`. Puede utilizar el archivo `Dialcodes` con el fin de proporcionar información adicional sobre un número de teléfono básico utilizado por varios sistemas en el mismo sitio.

Cada entrada tiene la siguiente sintaxis:

```
Abbreviation   Dial-Sequence
```

`Abreviatura`	Este campo proporciona la abreviatura que se utiliza en el campo Phone del archivo `Systems`.
`Dial-Sequence`	Este campo proporciona la secuencia de marcación que se pasa al marcador cuando se accede a esa entrada particular del archivo `Systems`.

Compare los campos de los dos archivos. A continuación, se muestran los campos en el archivo `Dialcodes`.

```
Abbreviation   Dial-Sequence
```

A continuación, se muestran los campos en el archivo `Systems`.

```
System-Name   Time   Type   Speed   Phone   Chat Script
```

En la tabla siguiente, se muestra el contenido de ejemplo para los campos de un archivo `Dialcodes`.

TABLA 12-4 Entradas en el archivo `Dialcodes`

Abreviatura	Dial-Sequence
NY	1=212
jt	9+847

En la primera fila, NY es la abreviatura que aparece en el campo Phone del archivo `Systems`. Por ejemplo, el archivo `Systems` podría tener la siguiente entrada:

```
NY5551212
```

Cuando `uucico` lee `NY` en el archivo `Systems`, `uucico` busca en el archivo `Dialcodes` `NY` y obtiene la secuencia de marcación `1=212`. `1=212` es la secuencia de marcación necesaria para cualquier llamada telefónica a Nueva York. Esta secuencia incluye el número `1`, un "signo igual" (`=`) que significa pausar y esperar un tono de marcación secundario, y el código de área `212`. `uucico` envía esta información al marcador y, a continuación, vuelve al archivo `Systems` para el resto del número de teléfono, `5551212`.

La entrada `jt 9=847-` funcionaría con un campo Phone, como `jt7867`, en el archivo `Systems`. Cuando `uucico` lee la entrada que contiene `jt7867` en el archivo `Systems`, `uucico` envía la secuencia `9=847-7867` al marcador si el token del par de marcador y token es `\T`.

Archivo `/etc/uucp/Sysfiles` del UUCP

El archivo `/etc/uucp/Sysfiles` le permite asignar distintos archivos que serán utilizados por `uucp` y `cu` como archivos `Systems`, `Devices` y `Dialers`. Para obtener más información acerca de `cu`, consulte la página del comando man `cu`(1C). Puede utilizar `Sysfiles` para lo siguiente:

- Diferentes archivos `Systems` para que las solicitudes de servicios de inicio de sesión se puedan realizar para direcciones diferentes que los servicios de `uucp`.
- Diferentes archivos `Dialers` para que pueda asignar diferentes protocolos de enlace a `cu` y `uucp`.

- Varios archivos `Systems`, `Dialers` y `Devices`. El archivo `Systems`, en particular, puede volverse grande, lo que hace que el archivo sea más adecuado para dividir en varios archivos más pequeños.

La siguiente es la sintaxis de una entrada del archivo `Sysfiles`:

```
service=w systems=x:x dialers=y:y devices=z:z
```

w	Representa `uucico`, `cu` o ambos comandos separados por dos puntos
x	Representa uno o más archivos que se utilizarán como el archivo `Systems`, con cada nombre de archivo separado por dos puntos y leído en el orden que se presenta
y	Representa uno o más archivos que se utilizarán como el archivo `Dialers`
z	Representa uno o más archivos que se utilizarán como el archivo `Devices`

Se asume que cada nombre de archivo está relacionado con el directorio `/etc/uucp`, a menos que se proporcione una ruta de acceso completa.

El siguiente ejemplo, `/etc/uucp/Sysfiles`, define un archivo `Systems` local (`Local_Systems`) además del archivo `/etc/uucp/Systems` estándar:

```
service=uucico:cu systems=Systems :Local_Systems
```

Cuando esta entrada está en `/etc/uucp/Sysfiles`, tanto `uucico` como `cu` primero comprueban en el archivo `/etc/uucp/Systems` estándar. Si el sistema al que se llama no tiene una entrada en ese archivo o si las entradas en el archivo fallan, ambos comandos comprueban `/etc/uucp/Local_Systems`.

Como se especifica en la entrada anterior, `cu` y `uucico` comparten los archivos `Dialers` y `Devices`.

Cuando diferentes archivos `Systems` se definen para servicios de `uucico` y `cu`, su máquina almacena dos listas diferentes de `Systems`. Puede imprimir la lista de `uucico` utilizando el comando `uuname` o la lista de `cu` utilizando el comando `uuname -C`. El siguiente es otro ejemplo del archivo, que muestra que los archivos alternativos se consultan en primer lugar y los archivos predeterminados se consultan si es necesario:

```
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
```

Archivo /etc/uucp/Sysname del UUCP

Cada máquina que utiliza el UUCP debe tener un nombre de identificación, a menudo conocido como el *nombre de nodo*. El nombre de nodo aparece en el archivo /etc/uucp/Systems del equipo remoto, junto con la secuencia de comandos de chat y otra información de identificación. Normalmente, el UUCP utiliza el mismo nombre de nodo devuelto por el comando uname -n, que también es utilizado por TCP/IP.

Puede especificar un nombre de nodo del UUCP independiente del nombre de host del TCP/IP mediante la creación del archivo /etc/uucp/Sysname. El archivo tiene una entrada de una línea que contiene el nombre de nodo del UUCP para el sistema.

Archivo /etc/uucp/Permissions del UUCP

El archivo /etc/uucp/Permissions especifica los permisos que los equipos remotos tienen para el inicio de sesión, el acceso a archivos y la ejecución de comandos. Algunas opciones restringen la capacidad del equipo remoto de solicitar archivos y recibir archivos que el equipo local pone en cola. Hay otra opción disponible que especifica los comandos que un equipo remoto puede ejecutar en el equipo local.

Entradas de estructuración del UUCP

Cada entrada es una línea lógica, con líneas físicas que terminan con una barra diagonal inversa (\) para indicar continuación. Las entradas están compuestas por opciones que están delimitadas por un espacio en blanco. Cada opción es un par de nombre y valor en el siguiente formato:

name=value

Valores pueden ser listas separadas por dos puntos. No se permiten espacios en blanco dentro de una asignación de opción.

Las líneas de comentario comienzan con un signo de almohadilla (#) y ocupan toda la línea hasta un carácter de línea nueva. Las líneas en blanco se ignoran, incluso dentro de las entradas de varias líneas.

Los tipos de entrada del archivo Permissions son los siguientes:

- LOGNAME: especifica los permisos que entran en vigor cuando un equipo remoto inicia sesión en su equipo (es decir, llama a su equipo).

Nota - Cuando un equipo remoto lo llama, su identidad es cuestionable, a menos que el equipo remoto tenga un inicio de sesión único y una contraseña verificable.

- MACHINE: especifica los permisos que entran en vigor cuando un equipo remoto inicia sesión en su equipo (es decir, llama a su equipo).

Las entradas de LOGNAME contienen una opción LOGNAME. Las entradas de MACHINE contienen una opción MACHINE. Una entrada puede contener ambas opciones.

Consideraciones del UUCP

Al utilizar el archivo Permissions para restringir el nivel de acceso que se otorga a equipos remotos, es conveniente tener en cuenta las siguientes consideraciones:

- Todos los ID de inicio de sesión utilizados por equipos remotos para iniciar sesión para comunicaciones del UUCP deben aparecer en una y sólo una entrada LOGNAME.
- Cualquier sitio que se llama con un nombre que no aparece en una entrada MACHINE tiene los permisos o las restricciones predeterminados que se indican a continuación:
  - Se ejecutan solicitudes locales de envío y recepción.
  - El equipo remoto puede enviar archivos al directorio /var/spool/uucppublic de su equipo.
  - Los comandos enviados por el equipo remoto para ejecutarse en su equipo deben ser uno de los comandos predeterminados, normalmente rmail.

Opción REQUEST del UUCP

Cuando un equipo remoto llama a su equipo y solicita recibir un archivo, esa solicitud se puede otorgar o rechazar. La opción REQUEST especifica si el equipo remoto puede solicitar configurar transferencias de archivos desde su equipo. La cadena REQUEST=yes especifica que el equipo remoto puede solicitar transferir archivos desde su equipo. La cadena REQUEST=no especifica que el equipo remoto no puede solicitar recibir archivos desde su equipo. REQUEST=no, el valor predeterminado, se usa si la opción REQUEST no se especifica. La opción REQUEST puede aparecer en una entrada LOGNAME para que el equipo remoto lo llame o en una entrada MACHINE para que usted llame al equipo remoto.

Opción SENDFILES del UUCP

Cuando un equipo remoto llama a su equipo y completa su trabajo, el equipo remoto puede intentar recuperar el trabajo que su equipo ha puesto en cola para él. La opción SENDFILES especifica si su equipo puede enviar el trabajo que está en cola para el equipo remoto.

La cadena SENDFILES=yes especifica que su equipo puede enviar el trabajo que está en cola para el equipo remoto si inició sesión con uno de los nombres de la opción LOGNAME. Esta

cadena es *obligatoria* si ha introducido Never en el campo Time de /etc/uucp/Systems. Esta designación configura el equipo local en modo pasivo, pero no está permitido iniciar una llamada a ese equipo remoto particular. Consulte “Archivo /etc/uucp/Systems del UUCP” [181] para obtener más información.

La cadena SENDFILES=call especifica que los archivos que están en cola en su equipo se envían sólo cuando su equipo llama al equipo remoto. El valor call es el valor predeterminado para la opción SENDFILES. Esta opción sólo es significativa en entradas LOGNAME porque las entradas MACHINE se aplican cuando se envían llamadas a equipos remotos. Si la opción se utiliza con una entrada MACHINE, la opción se ignora.

Opción MYNAME del UUCP

Esta opción permite designar un nombre de nodo único del UUCP para su equipo, además del nombre de host del TCP/IP, como lo devuelve el comando hostname. Por ejemplo, si asignó sin darse cuenta al host el mismo nombre que el de algún otro sistema, puede definir la opción MYNAME del archivo Permissions. Suponga que desea que su organización sea conocida como widget. Si todos los módems están conectados a una máquina con el nombre de host gadget, puede tener una entrada en el archivo Permissions de gadget que se lee de la siguiente manera:

```
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
```

Ahora, el sistema world puede iniciar sesión en la máquina gadget como si estuviera iniciando sesión en widget. Para que el equipo world lo conozca también por el alias widget cuando lo llama, puede tener una entrada que lea de la siguiente manera:

```
MACHINE=world MYNAME=widget
```

También puede utilizar la opción MYNAME para fines de prueba, ya que esta opción permite que su equipo se llame a sí mismo. Sin embargo, debido a que esta opción se podría utilizar para enmascarar la identidad real de un equipo, debe utilizar la opción VALIDATE, como se describe en “Opción VALIDATE del UUCP” [207].

Opciones READ y WRITE del UUCP

Estas opciones especifican las partes del sistema de archivos que uucico puede leer o escribir. Puede designar las opciones READ y WRITE con las entradas MACHINE o LOGNAME.

El valor predeterminado para las opciones READ y WRITE es el directorio uucppublic, como se muestra en las siguientes cadenas:

```
READ=/var/spool/uucppublic WRITE=/var/spool/uucppublic
```

Las cadenas READ=/ y WRITE=/ especifican permiso para acceder a cualquier archivo al que puede acceder un usuario local con otros permisos.

El valor de estas entradas es una lista separada por dos puntos de nombres de ruta. La opción READ sirve para solicitar archivos y la opción WRITE sirve para depositar archivos. Uno de los valores debe ser el prefijo de cualquier nombre de ruta de acceso completa de un archivo que entra o sale. Para otorgar permiso para depositar archivos en /usr/news así como en el directorio público, utilice los siguientes valores con la opción WRITE:

```
WRITE=/var/spool/uucppublic:/usr/news
```

Si se utilizan las opciones READ y WRITE, se deben especificar todos los nombres de ruta porque los nombres de ruta no se agregan a la lista predeterminada. Por ejemplo, si el nombre de ruta /usr/news fuera la única ruta especificada en una opción WRITE, el permiso para depositar archivos en el directorio público sería denegado.

Preste atención a qué directorios permite que los sistemas remotos lean o escriban. Por ejemplo, el directorio /etc contiene muchos archivos del sistema esenciales. Los usuarios remotos no deben tener permiso para depositar archivos en ese directorio.

Opciones NOREAD y NOWRITE del UUCP

Las opciones NOREAD y NOWRITE especifican excepciones a las opciones READ y WRITE, o valores predeterminados. La siguiente entrada permite leer cualquier archivo, excepto aquellos archivos en el directorio /etc (y sus subdirectorios). Recuerde que estas opciones son prefijos.

```
READ=/ NOREAD=/etc WRITE=/var/spool/uucppublic
```

Esta entrada permite escribir únicamente en el directorio /var/spool/uucppublic predeterminado. La opción NOWRITE funciona de la misma manera que la opción NOREAD. Puede utilizar las opciones NOREAD y NOWRITE en las entradas LOGNAME y MACHINE.

Opción CALLBACK del UUCP

Puede utilizar la opción CALLBACK en las entradas LOGNAME para especificar que no ocurra ninguna transacción hasta que se devuelva la llamada al sistema que llama. Los motivos para configurar CALLBACK son los siguientes:

- Por motivos de seguridad: si le devuelve la llamada a un equipo, puede estar seguro de que es el equipo correcto.

- Por motivos contables: si realiza grandes transmisiones de datos, puede seleccionar la máquina que se factura para la llamada más larga.

La cadena CALLBACK=yes especifica que el equipo debe devolver la llamada al equipo remoto antes de que pueda ocurrir alguna transferencia de archivos.

El valor predeterminado para la opción CALLBACK es CALLBACK=no. Si define CALLBACK en yes, los permisos que afectan el resto de la conversación deben especificarse en la entrada MACHINE que corresponde al emisor de llamada. No especifique estos permisos en LOGNAME ni en la entrada LOGNAME que el equipo remoto puede haber definido para el host.

Nota - Si dos sitios tienen la opción CALLBACK definida para cada uno, la conversación no se inicia nunca.

Opción COMMANDS del UUCP

Atención - La opción COMMANDS puede poner en peligro la seguridad del sistema. Utilice esta opción con mucho cuidado.

Puede utilizar la opción COMMANDS en las entradas MACHINE para especificar los comandos que un equipo remoto puede ejecutar en su equipo. El programa uux genera solicitudes de ejecución remota y pone en cola las solicitudes que se van a transferir al equipo remoto. Los archivos y comandos se envían al equipo de destino para la ejecución remota, que es una excepción a la regla que las entradas MACHINE aplican únicamente cuando su sistema realiza la llamada.

Tenga en cuenta que COMMANDS no se utiliza en una entrada LOGNAME. La opción COMMANDS en las entradas MACHINE define permisos de comandos si usted llama al sistema remoto o si el sistema remoto lo llama a usted.

La cadena COMMANDS=rmail especifica los comandos predeterminados que un equipo remoto puede ejecutar en su equipo. Si una cadena de comandos se utiliza en una entrada MACHINE, los comandos predeterminados se sobrescriben. Por ejemplo, la siguiente entrada sobrescribe la opción COMMAND predeterminada para que los equipos que se denominan owl, raven, hawk y dove ahora puedan ejecutar rmail, rnews y lp en su equipo.

```
MACHINE=owl:raven:hawk:dove COMMANDS=rmail:rnews:lp
```

Además de los nombres especificados, puede tener nombres de ruta de acceso completos de comandos. Por ejemplo, la siguiente entrada especifica que el comando rmail utiliza la ruta de búsqueda predeterminada.

```
COMMANDS=rmail:/usr/local/rnews:/usr/local/lp
```

La ruta de búsqueda predeterminada para el UUCP es /bin y /usr/bin. Cuando el equipo remoto especifica rnews o /usr/local/rnews para que el comando se ejecute, /usr/local/rnews se ejecuta independientemente de la ruta predeterminada. Del mismo modo, /usr/local/lp es el comando lp que se ejecuta.

La inclusión del valor ALL en la lista significa que se ejecuta cualquier comando de los equipos remotos que se especifican en la entrada. Si utiliza este valor, otorga a los equipos remotos acceso completo a su equipo.

Atención - Este valor permite mucho más acceso que el que tienen los usuarios comunes. Debe utilizar este valor sólo cuando ambos equipos están en la misma ubicación, cuando ambos equipos están estrechamente conectados y cuando los usuarios son de confianza.

Ésta es la cadena con el valor ALL agregado:

```
COMMANDS=/usr/local/rnews:ALL:/usr/local/lp
```

Esta cadena ilustra dos puntos:

- El valor ALL puede aparecer en cualquier parte de la cadena.
- Los nombres de ruta que se especifican para rnews y lp se utilizan (en lugar de los predeterminados) si el comando solicitado no contiene los nombres de ruta de acceso completa para rnews o lp.

Debe utilizar la opción VALIDATE cada vez que se especifiquen comandos potencialmente peligrosos, como cat y uucp, con la opción COMMANDS. Cualquier comando que lee o escribe archivos es potencialmente peligroso para la seguridad local cuando el comando es ejecutado por el daemon de ejecución remota del UUCP (uuxqt).

Opción VALIDATE del UUCP

Use la opción VALIDATE junto con la opción COMMANDS cada vez que especifique comandos que sean posiblemente peligrosos para la seguridad de la máquina. VALIDATE es simplemente un nivel adicional de seguridad además de la opción COMMANDS, aunque es una manera más segura de abrir el acceso a comandos que ALL.

VALIDATE proporciona un cierto grado de verificación de la identidad del emisor comprobando el nombre de host de un equipo que llama con el nombre de inicio de sesión que utiliza. La siguiente cadena garantiza que si una máquina que no sea widget ni gadget intenta iniciar sesión como Uwidget, la conexión se rechaza.

```
LOGNAME=Uwidget VALIDATE=widget:gadget
```

La opción VALIDATE requiere que los equipos con privilegios tengan un inicio de sesión y una contraseña únicos para las transacciones del UUCP. Un aspecto importante de esta validación

es que el inicio de sesión y la contraseña que están asociados con esta entrada están protegidos. Si un desconocido obtiene esa información, esa opción VALIDATE particular ya no puede considerarse segura.

Considere cuidadosamente a qué equipos remotos otorga inicios de sesión y contraseñas con privilegios para transacciones del UUCP. Proporcionar a un equipo remoto un inicio de sesión y una contraseña especiales con las capacidades de acceso a archivos y ejecución remota es como otorgar a cualquier usuario de dicho equipo un inicio de sesión y una contraseña comunes en su equipo. Por lo tanto, si no puede confiar en algún usuario del equipo remoto, no proporcione a ese equipo un inicio de sesión y una contraseña con privilegios.

La siguiente entrada LOGNAME especifica que si uno de los equipos remotos que afirma ser eagle, owl o hawk inicia sesión en su equipo, debe haber utilizado el inicio de sesión uucpfriend:

```
LOGNAME=uucpfriend VALIDATE=eagle:owl:hawk
```

Si un desconocido obtiene la contraseña y el inicio de sesión uucpfriend, el enmascaramiento es sencillo.

No obstante, ¿en qué se relaciona esta entrada con la opción COMMANDS, que aparece sólo en las entradas MACHINE? Esta entrada enlaza la entrada MACHINE (y la opción COMMANDS) a una entrada LOGNAME que está asociada con un inicio de sesión con privilegios. Este enlace es necesario porque el daemon de ejecución no se ejecuta mientras el equipo remoto tiene una sesión iniciada. En realidad, el enlace es un proceso asíncrono que no sabe qué equipo envió la solicitud de ejecución. Por lo tanto, la verdadera pregunta es: ¿cómo sabe el equipo de dónde vinieron los archivos de ejecución?

Cada equipo remoto tiene su propio directorio de cola de impresión en el equipo local. Estos directorios de cola de impresión tienen permiso de escritura que se otorga únicamente a programas del UUCP. Los archivos de ejecución del equipo remoto se colocan en el directorio de cola de impresión después de que se transfieren a su equipo. Cuando el daemon uuxqt se ejecuta, puede utilizar el nombre del directorio de cola de impresión para buscar la entrada MACHINE en el archivo Permissions y obtener la lista COMMANDS. O bien si el nombre del equipo no aparece en el archivo Permissions, se utiliza la lista predeterminada.

En este ejemplo, se muestra la relación entre las entradas MACHINE y 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=/
```

El valor de la opción COMMANDS significa que los usuarios remotos pueden ejecutar rmail y /usr/local/rnews.

En la primera entrada, debe asumir que cuando desea llamar a uno de los equipos de la lista, en realidad llama a eagle, owl o hawk. Por lo tanto, los archivos que se colocan en uno de los directorios de cola de impresión de eagle, owl o hawk son colocados allí por uno de esos equipos. Si un equipo remoto inicia sesión e indica que es uno de esos tres equipos, los archivos de ejecución también se colocan en el directorio de cola de impresión con privilegios. Por lo tanto, tiene que validar que el equipo tenga el inicio de sesión uucpz con privilegios.

Entrada MACHINE para OTHER del UUCP

Es posible que desee especificar diferentes valores de opción para equipos remotos que no están mencionados en entradas MACHINE específicas. La necesidad puede surgir cuando muchos equipos llaman al host, y el conjunto de comandos cambia de vez en cuando. El nombre OTHER para el nombre de equipo se utiliza para esta entrada, como se muestra en este ejemplo:

```
MACHINE=OTHER \
COMMANDS=rmail:rnews:/usr/local/Photo:/usr/local/xp
```

Todas las demás opciones que están disponibles para la entrada MACHINE también se pueden establecer para los equipos que no están mencionados en otras entradas MACHINE.

Combinación de entradas MACHINE y LOGNAME para el UUCP

Puede combinar las entradas MACHINE y LOGNAME en una sola entrada cuando las opciones comunes son las mismas. Por ejemplo, los siguientes dos conjuntos de entradas comparten las mismas opciones REQUEST, READ y WRITE:

```
MACHINE=eagle:owl:hawk REQUEST=yes \
READ=/ WRITE=/
```

y

```
LOGNAME=uupz REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

Puede fusionar estas entradas, tal como se muestra:

```
MACHINE=eagle:owl:hawk REQUEST=yes \
logname=uucpz SENDFILES-yes \
READ=/ WRITE=/
```

Combinar las entradas MACHINE y LOGNAME hace que el archivo Permissions sea más manejable y eficaz.

Reenvío del UUCP

Al enviar archivos mediante una serie de máquinas, las máquinas intermediarias deben tener el comando uucp entre sus opciones COMMANDS. Si escribe el siguiente comando, la operación de reenvío funciona sólo si el equipo willow permite que el equipo oak ejecute el programa uucp.

```
% uucp sample.txt oak\!willow\!pine\!/usr/spool/uucppublic
```

El equipo oak también debe permitir que su equipo ejecute el programa uucp. La máquina pine, como la última máquina designada, no tiene que permitir el comando uucp porque la máquina no está realizando ninguna operación de reenvío. Normalmente, los equipos no se configuran de esta manera.

Archivo /etc/uucp/Poll del UUCP

El archivo /etc/uucp/Poll contiene información para sondear equipos remotos. Cada entrada del archivo Poll contiene el nombre de un equipo remoto para llamar, seguido por un carácter de tabulación o un espacio y, por último, las horas en las que el equipo debe ser llamado. El formato de las entradas en el archivo Poll es el siguiente:

sys-name hour ...

Por ejemplo, la entrada **eagle 0 4 8 12 16 20** proporciona sondeo del equipo eagle cada 4 h.

La secuencia de comandos uudemon.poll script procesa el archivo Poll pero, en realidad, no realiza el sondeo. La secuencia de comandos solamente configura un archivo de trabajo de sondeo (siempre denominado C.*file*) en el directorio de cola de impresión. La secuencia de comandos uudemon.poll inicia el programador, y el programador examina todos archivos de trabajo en el directorio de cola de impresión.

Archivo /etc/uucp/Config del UUCP

El archivo /etc/uucp/Config permite sobrescribir ciertos parámetros manualmente. Cada entrada en el archivo Config tiene este formato:

parameter=value

Consulte el archivo Config que se proporciona con el sistema para obtener una lista completa de nombres de parámetros configurables.

La siguiente entrada Config establece el orden del protocolo predeterminado en Gge y cambia los valores predeterminados del protocolo G a 7 ventanas y paquetes de 512 bytes.

```
Protocol=G(7,512)ge
```

Archivo /etc/uucp/Grades del UUCP

El archivo /etc/uucp/Grades contiene las definiciones de los niveles de trabajo que se pueden utilizar para poner en cola trabajos en un equipo remoto. Este archivo también contiene los permisos para cada nivel de trabajo. Cada entrada de este archivo representa una definición de un nivel de trabajo definido por el administrador que permite a los usuarios poner en cola trabajos.

Cada entrada en el archivo Grades tiene el siguiente formato:

User-job-grade System-job-grade Job-size Permit-type ID-list

Cada entrada contiene campos que están separados por un espacio en blanco. El último campo de la entrada está compuesto por subcampos que también están separados por espacios. Si una entrada ocupa más de una línea física, puede utilizar una barra diagonal inversa para continuar la entrada en la siguiente línea. Las líneas de comentario comienzan con un signo de almohadilla (#) y ocupan toda la línea. Las líneas en blanco siempre se ignoran.

Campo User-job-grade del UUCP

Este campo contiene un nombre de nivel de trabajo de usuario definido por el administrador de hasta 64 caracteres.

Campo System-job-grade del UUCP

Este campo contiene un nivel de trabajo de un solo carácter al cual *User-job-grade* está asignado. La lista válida de caracteres es A-Z, a-z, en donde A tiene la prioridad más alta y z la prioridad más baja.

Relación entre niveles de trabajo de sistemas y usuarios

El nivel de trabajo de usuario se puede enlazar a más de un nivel de trabajo de sistema. Tenga en cuenta que el archivo Grades se busca secuencialmente para encontrar instancias de un nivel de trabajo de usuario. Por lo tanto, cualesquiera instancias de un nivel de trabajo de sistema deben aparecer en cumplimiento con la restricción sobre el máximo tamaño del trabajo.

Si bien no existe ningún número máximo para los niveles de trabajo de usuario, el número máximo de niveles de trabajo de sistema permitido es 52. El motivo es que más de un *User-*

job-grade se puede asignar a un *System-job-grade*, pero cada *User-job-grade* debe estar en una línea diferente en el archivo. A continuación le mostramos un ejemplo:

```
mail N Any User Any netnews N Any User Any
```

Si realiza esta configuración en un archivo `Grades`, estos dos campos *User-job-grade* comparten el mismo *System-job-grade*. Debido a que los permisos para un *Job-grade* están asociados con un *User-job-grade* y no con un *System-job-grade*, dos *User-job-grade* pueden compartir el mismo *System-job-grade* y tener dos conjuntos diferentes de permisos.

Nivel predeterminado

Puede definir el enlace de un *User-job-grade* predeterminado a un nivel de trabajo de sistema. Debe usar la palabra clave predeterminada como el nivel de trabajo de usuario en el campo *User-job-grade* del archivo `Grades` y el nivel de trabajo de sistema al que está enlazado. Las restricciones y los campos de ID deben estar definidos como `Any` para que cualquier usuario y cualquier tamaño de trabajo se puedan poner en cola en este nivel. A continuación le mostramos un ejemplo:

```
default a Any User Any
```

Si no define el nivel de trabajo de usuario predeterminado, se utiliza el nivel predeterminado integrado `Z`. Debido a que el campo de restricción predeterminado es `Any`, no se comprueban varias instancias del nivel predeterminado.

Campo Job-size del UUCP

Este campo especifica el tamaño máximo de trabajo que se puede introducir en la cola. *Job-size* es medido en bytes y puede ser una lista de las opciones que se describen en la siguiente lista.

nnnn	Número entero que especifica el tamaño máximo de trabajo para este nivel de trabajo
n`K`	Número decimal que representa el número de kilobytes (`K` es la abreviatura de kilobyte)
n`M`	Número decimal que representa el número de megabytes (`M` es la abreviatura de megabyte)
`Any`	Palabra clave que especifica que no existe un tamaño máximo de trabajo

Aquí se muestran algunos ejemplos:

- `5000` representa 5000 bytes
- `10K` representa 10 Kbytes
- `2M` representa 2 Mbytes

Campo Permit-type del UUCP

Este campo contiene una palabra clave que indica cómo interpretar la lista de ID. En la siguiente tabla, se enumeran las palabras clave y sus significados.

TABLA 12-5 Campo Permit-type

Palabra clave	Contenido de la lista de ID
`User`	Nombres de inicio de sesión de usuarios que están autorizados a utilizar este nivel de trabajo
`Non-user`	Nombres de inicio de sesión de usuarios que no están autorizados a utilizar este nivel de trabajo
`Group`	Nombres de grupos cuyos miembros están autorizados a utilizar este grupo
`Non-group`	Nombres de grupos cuyos miembros no están autorizados a utilizar este nivel de trabajo

Campo ID-list del UUCP

Este campo contiene una lista de nombres de inicios de sesión o nombres de grupos a los cuales se va a permitir o rechazar la puesta en cola en este nivel de trabajo. Los nombres de la lista están separados por un espacio en blanco y terminan con un carácter de línea nueva. La palabra clave `Any` se utiliza para indicar que cualquier usuario puede poner en cola en este nivel de trabajo.

Otros archivos de configuración del UUCP

En esta sección, se describen tres modificados con menos frecuencia que afectan el uso de las utilidades del UUCP.

Archivo `/etc/uucp/Devconfig` del UUCP

El archivo `/etc/uucp/Devconfig` permite configurar dispositivos por servicio, como `uucp` o `cu`. Las entradas de `Devconfig` definen los módulos STREAMS que se utilizan para un dispositivo concreto. Estas entradas tienen el siguiente formato:

`service=`*x* `device=`*y* `push=`*z*[:*z*...]

x puede ser `cu`, `uucico` o ambos servicios separados por dos puntos. *y* es el nombre de una red y debe coincidir con una entrada en el archivo `Devices`. *z* es reemplazado por los nombres de los módulos STREAMS en el orden en que se van a insertar en la secuencia. Se pueden definir diferentes módulos y dispositivos para servicios `cu` y `uucp`.

Las entradas siguientes son para una red STARLAN y se utilizarían con más frecuencia en el archivo:

```
service=cu       device=STARLAN     push=ntty:tirdwr
service=uucico   device=STARLAN     push=ntty:tirdwr
```

Este ejemplo inserta `ntty` y, a continuación, `tirdwr`.

Archivo `/etc/uucp/Limits` del UUCP

El archivo `/etc/uucp/Limits` controla las ejecuciones simultáneas máximas de `uucico`, `uuxqt` y `uusched` que se ejecutan en la red `uucp`. En la mayoría de las situaciones, los valores predeterminados son aceptables y no se necesitan cambios. Si desea cambiarlos, sin embargo, utilice cualquier editor de texto.

El formato del archivo `Limits` es el siguiente:

`service=`*x* `max=`*y*:

x puede ser `uucico`, `uuxqt` o `uusched`, e *y* es el límite que está permitido para ese servicio. Los campos pueden estar en cualquier orden y en minúsculas.

Las entradas siguientes se deben utilizar con más frecuencia en el archivo `Limits`:

```
service=uucico max=5
service=uuxqt max=5
service=uusched max=2
```

El ejemplo permite que cinco comandos `uucico`, cinco `uuxqt` y dos `uusched` se ejecuten en la máquina.

Archivo `remote.unknown` del UUCP

El otro archivo que afecta el uso de las utilidades de comunicación es el archivo `remote.unknown`. Este archivo es un programa binario que se ejecuta cuando un equipo que no se encuentra en ninguno de los archivos `Systems` inicia una conversación. Este programa registra el intento de conversación y elimina la conexión.

Atención - Si cambia los permisos del archivo `remote.unknown` de modo que el archivo no se pueda ejecutar, el sistema acepta las conexiones de cualquier sistema.

Este programa se ejecuta cuando una máquina que no está en ninguno de los archivos `Systems` inicia una conversación. El programa registra el intento de conversación, pero no puede establecer una conexión. Si cambia los permisos de este archivo de manera que el archivo

no se pueda ejecutar (`chmod 000 remote.unknown`), el sistema acepta cualquier solicitud de conversación. Este cambio no es trivial. Debe tener buenas razones para efectuar el cambio.

Archivos administrativos del UUCP

Los archivos administrativos del UUCP se describen a continuación. Estos archivos se crean en directorios de cola de impresión para bloquear dispositivos, conservar datos temporales o mantener información acerca de ejecuciones o transferencias remotas.

- *Archivos de datos temporales* (`TM`): estos archivos de datos son creados por procesos del UUCP en el directorio de cola de impresión `/var/spool/uucp/`*x* cuando se recibe un archivo de otro equipo. El directorio *x* tiene el mismo nombre que el equipo remoto que envía el archivo. Los nombres de los archivos de datos temporales tienen el siguiente formato:

  `TM.`*pid.ddd*

  pid es un ID de proceso y *ddd* es un número secuencial de tres dígitos que comienza con 0.

  Cuando todo el archivo se recibe, el archivo `TM.`*pid.ddd* se mueve al nombre de ruta especificado en el archivo `C.`*sysnxxxx* (que se abarca más adelante) que generó la transmisión. Si el procesamiento se termina de modo anormal, el archivo `TM.`*pid.ddd* puede permanecer en el directorio *x*. Estos archivos deben ser eliminados automáticamente por `uucleanup`.
- *Lock files* (`LCK`): los archivos de bloqueo se crean en el directorio `/var/spool/locks` para cada dispositivo en uso. Los archivos de bloqueo evitan conversaciones duplicadas y varios intentos de utilizar el mismo dispositivo que llama. En la siguiente tabla, se muestran los distintos tipos de archivos de bloqueo del UUCP.

TABLA 12-6 Archivos de bloqueo del UUCP

Nombre del archivo	Descripción
`LCK.`*sys*	*sys* representa el nombre del equipo que está utilizando el archivo
`LCK.`*dev*	*dev* representa el nombre de un dispositivo que está utilizando el archivo
`LCK.`*LOG*	*LOG* representa un archivo log bloqueado del UUCP

Estos archivos pueden permanecer en el directorio de cola de impresión si el enlace de comunicaciones se elimina inesperadamente, como cuando un equipo falla. Un archivo de bloqueo se ignora (se elimina) una vez que el proceso principal ya no está activo. El archivo de bloqueo contiene el ID de proceso del proceso que ha creado el bloqueo.

- *Work file* (`C.`): los archivos de trabajo se crean en un directorio de cola de impresión cuando el trabajo se ha puesto en cola, como transferencias de archivos o ejecuciones remotas de comandos, para un equipo remoto. Los nombres de archivos de trabajo tienen el siguiente formato:

`C.`*sysnxxxx*

sys es el nombre del equipo remoto, *n* es el carácter ASCII que representa el nivel (la prioridad) del trabajo y *xxxx* es el número de secuencia de trabajo de cuatro dígitos asignado por el UUCP. Los archivos de trabajo contienen la siguiente información:

- Nombre de ruta de acceso completa del archivo que se va a enviar o solicitar.
- Nombre de ruta de acceso completa del destino o el nombre de archivo o usuario.
- Nombre de inicio de sesión del usuario.
- Lista de opciones.
- Nombre de archivos de datos asociados en el directorio de cola de impresión. Si se especificó la opción `uucp -C` o `uuto -p`, se utiliza un nombre ficticio (`D.0`).
- Bits de modo del archivo de origen.
- Nombre de inicio de sesión de usuario remoto al que se notificará cuando se complete la transferencia.

- *Archivo de datos* (`D.`): los archivos de datos se crean cuando se especifica en la línea de comandos que se copie el archivo de origen en el directorio de cola de impresión. Los nombres de archivos de datos tienen el siguiente formato:

  `D.`*systmxxxxyyy*: *systm* son los primeros cinco caracteres del nombre del equipo remoto. *xxxx* es un número de secuencia de trabajo de cuatro dígitos asignado por `uucp`. El número de secuencia de trabajo de cuatro dígitos puede ir seguido de un número posterior. *yyy* se utiliza cuando varios archivos `D.` se crean para un archivo de trabajo (`C.`).

- `X.` *(execute file)*: los archivos ejecutables se crean en el directorio de cola de impresión antes de las ejecuciones remotas de comandos. Los nombres de archivos ejecutables tienen el siguiente formato:

  `X.`*sysnxxxx*

  sys es el nombre del equipo remoto. *n* es el carácter que representa el nivel (la prioridad) del trabajo. *xxxx* es un número de secuencia de cuatro dígitos asignado por el UUCP. Los archivos ejecutables contienen la siguiente información:

  - Nombre de inicio de sesión y nombre de equipo del solicitante.
  - Nombres de los archivos que son necesarios para la ejecución.
  - Entrada que se utilizará como la entrada estándar para la cadena de comandos.
  - Nombre de archivo y equipo para recibir la salida estándar de la ejecución de comandos.
  - Cadena de comandos
  - Líneas de opción para solicitudes de estado de retorno

Mensajes de error del UUCP

En esta sección, se muestran los mensajes de error que están asociados con el UUCP.

Mensajes de error ASSERT del UUCP

En la siguiente tabla, se muestran mensajes de error ASSERT.

TABLA 12-7 Mensajes de error ASSERT

Mensaje de error	Descripción o acción
`CAN'T OPEN`	Falló un comando `open()` o `fopen()`.
`CAN'T WRITE`	Falló un comando `write()`, `fwrite()`, `fprint()`, o un comando similar.
`CAN'T READ`	Falló un comando `read()` o `fgets()`, o un comando similar.
`CAN'T CREATE`	Falló una llamada `creat()`.
`CAN'T ALLOCATE`	Falló una asignación dinámica.
`CAN'T LOCK`	Falló un intento de realizar un archivo `LCK` (bloqueo). En algunas situaciones, este error es fatal.
`CAN'T STAT`	Falló una llamada `stat()`.
`CAN'T CHMOD`	Falló una llamada `chmod()`.
`CAN'T LINK`	Falló una llamada `link()`.
`CAN'T CHDIR`	Falló una llamada `chdir()`.
`CAN'T UNLINK`	Falló una llamada `unlink()`.
`WRONG ROLE`	Éste es un problema lógico interno.
`CAN'T MOVE TO CORRUPTDIR`	Falló un intento de mover algunos archivos `C.` o `X.` incorrectos al directorio `/var/spool/uucp/.Corrupt`. Es posible que el directorio no esté o tenga propietarios o modos incorrectos.
`CAN'T CLOSE`	Falló una llamada `close()` o `fclose()`.
`FILE EXISTS`	Se intenta crear un archivo `C.` o `D.`, pero el archivo existe. Este error se produce cuando surge un problema con el acceso a archivos de secuencia, lo que, normalmente, indica un error de software.
`NO uucp SERVICE NUMBER`	Se intenta una llamada TCP/IP, pero no hay ninguna entrada en `/etc/services` para el UUCP.
`BAD UID`	El ID de usuario no está en la base de datos de contraseñas. Compruebe la configuración del servicio de nombres.
`BAD LOGIN_UID`	Igual que la descripción anterior.
`BAD LINE`	Hay una línea incorrecta en el archivo `Devices`. No hay suficientes argumentos en una o más líneas.
`SYSLST OVERFLOW`	Desbordó una tabla interna en `gename.c`. Un solo trabajo intentó comunicarse con más de 30 sistemas.
`TOO MANY SAVED C FILES`	Igual que la descripción anterior.
`RETURN FROM fixline ioctl`	Falló un comando `ioctl(2)`, que nunca debe fallar. Se produjo un problema en el controlador del sistema.
`BAD SPEED`	Aparece una velocidad de línea incorrecta en el archivo `Devices` o `Systems` (campo Class o Speed).
`BAD OPTION`	Hay una opción o línea incorrecta en el archivo `Permissions`. Este error se debe solucionar inmediatamente.
`PKCGET READ`	El equipo remoto probablemente se colgó. No es necesaria ninguna acción.
`PKXSTART`	El equipo remoto se interrumpió de una manera no recuperable. Este error, por lo general, se puede ignorar.
`TOO MANY LOCKS`	Se produjo un problema interno. Póngase en contacto con el proveedor del sistema.
`XMV ERROR`	Se produjo un problema con algún archivo o directorio. El directorio de cola de impresión es la causa probable, ya que supuestamente se debían comprobar los modos de los destinos antes de intentar realizar este proceso.

Mensaje de error	Descripción o acción
CAN'T FORK	Falló un intento de ejecutar un comando `fork` y `exec`. El trabajo actual no se debe perder, pero se intentará realizar más tarde (`uuxqt`). No es necesaria ninguna acción.

Mensajes de error STATUS del UUCP

En la tabla siguiente, se muestra una lista de los mensajes de error STATUS más comunes.

TABLA 12-8 Mensajes STATUS del UUCP

Mensaje de error	Descripción o acción
OK	El estado es aceptable.
NO DEVICES AVAILABLE	Actualmente no hay ningún dispositivo disponible para la llamada. Compruebe si hay un dispositivo válido en el archivo `Devices` para el sistema concreto. Compruebe el archivo `Systems` para el dispositivo que se va a utilizar para llamar al sistema.
WRONG TIME TO CALL	Se realizó una llamada al sistema en un horario diferente del especificado en el archivo `Systems`.
TALKING	Explicativo.
LOGIN FAILED	Falló el inicio de sesión para el equipo en particular. La causa podría ser un inicio de sesión o una contraseña incorrectos, un número equivocado, un equipo lento o un fallo al ejecutar la secuencia de comandos Dialer-Token-Pairs.
CONVERSATION FAILED	La conversación falló después del inicio con éxito. Normalmente, este error significa que una parte dejó de funcionar, el programa se canceló o la línea (el enlace) se eliminó.
DIAL FAILED	El equipo remoto nunca respondió. La causa puede ser un marcador incorrecto o un número de teléfono incorrecto.
BAD LOGIN/MACHINE COMBINATION	El equipo llamó con un nombre de equipo o inicio de sesión que no concuerda con el archivo `Permissions`. Este error puede ser un intento de enmascaramiento.
DEVICE LOCKED	El dispositivo que llama que se va a utilizar está actualmente bloqueado y en uso por otro proceso.
ASSERT ERROR	Se produjo un error `ASSERT`. Consulte el archivo `/var/uucp/.Admin/errors` para obtener información sobre el mensaje de error y consulte la sección "Mensajes de error ASSERT del UUCP" [217].
SYSTEM NOT IN Systems FILE	El sistema no está en el archivo `Systems`.
CAN'T ACCESS DEVICE	El dispositivo probado no existe o los modos son incorrectos. Compruebe las entradas apropiadas en los archivos `Systems` y `Devices`.
DEVICE FAILED	El dispositivo no se puede abrir.
WRONG MACHINE NAME	El equipo que llamó informa un nombre diferente del esperado.
CALLBACK REQUIRED	El equipo que llamó requiere que llame a su equipo.
REMOTE HAS A LCK FILE FOR ME	El equipo remoto tiene un archivo `LCK` para su equipo. El equipo remoto puede estar intentando llamar a su equipo. Si el equipo remoto tiene una versión más antigua del UUCP, el proceso que se estaba comunicando con su equipo puede haber fallado y puede haber dejado el archivo `LCK`. Si el equipo remoto tiene la nueva versión del UUCP y no se está comunicando con su equipo, el proceso que tiene un archivo `LCK` se bloquea.
REMOTE DOES NOT KNOW ME	El equipo remoto no tiene el nombre del nodo de su equipo en el archivo `Systems`.

Mensaje de error	Descripción o acción
REMOTE REJECT AFTER LOGIN	El nombre de inicio de sesión que ha sido utilizado por su equipo para iniciar sesión no concuerda con el que el equipo remoto estaba esperando.
REMOTE REJECT, UNKNOWN MESSAGE	El equipo remoto rechazó la comunicación con su equipo por un motivo desconocido. Es posible que el equipo remoto no esté ejecutando una versión estándar del UUCP.
STARTUP FAILED	El inicio de sesión se completó con éxito, pero el protocolo de enlace inicial falló.
CALLER SCRIPT FAILED	Este error suele ser igual que el error DIAL FAILED. Sin embargo, si este error se produce a menudo, puede deberse a la secuencia de comandos del emisor en el archivo Dialers. Use Uutry para comprobar.

Mensajes de error numéricos del UUCP

En la siguiente tabla, se muestran los números de código de salida de los mensajes de estado de error producidos por el archivo /usr/include/sysexits.h. No todos son utilizados actualmente por uucp.

TABLA 12-9 Mensajes de error por número del UUCP

Número de mensaje	Descripción	Significado
64	Valor de base para mensajes de error	Los mensajes de error comienzan en este valor.
64	Error de uso de línea de comandos	El comando se utilizó de manera incorrecta, por ejemplo, con el número de argumentos incorrecto, un indicador erróneo o una sintaxis incorrecta.
65	Error de formato de datos	Los datos de entrada son incorrectos de alguna forma. Este formato de datos sólo se debe usar para datos del usuario y no para archivos del sistema.
66	No se puede abrir la entrada	Un archivo de entrada, no un archivo del sistema, no existe o no se puede leer. Este problema también puede incluir otros errores, como “Ningún mensaje” para una aplicación de correo.
67	Dirección desconocida	El usuario que se especificó no existe. Este error se puede utilizar para direcciones de correo o inicios de sesión remotos.
68	Nombre de host desconocido	El host no existe. Este error se utiliza en direcciones de correo o solicitudes de red.
69	Servicio no disponible	Un servicio no está disponible. Este error puede ocurrir si un archivo o programa de respaldo no existe. Este mensaje también puede indicar simplemente que algo no funciona y que la causa no se puede identificar actualmente.
70	Error interno de software	Un error interno de software se ha detectado. Este error se debe limitar a errores relacionados con sistemas no operativos, si es posible.
71	Error de sistema	Un error del sistema operativo se ha detectado. Este error se utiliza para ciertas condiciones, como “no es posible bifurcar”, “no es posible crear canalización”. Por ejemplo, este error incluye un retorno getuid de un usuario que no existe en el archivo passwd.
72	Falta archivo crítico del sistema operativo	Un archivo del sistema, como, por ejemplo, /etc/passwd o /var/admin/utmpx, no existe, no se puede abrir o tiene un error, como un error de sintaxis.
73	No es posible crear el archivo de salida	Un archivo de salida especificado por el usuario no se puede crear.
74	Error de entrada o salida	Se produjo un error al realizar la entrada y la salida en algún archivo.

Número de mensaje	Descripción	Significado
75	Fallo temporal. Se indica al usuario que vuelva a intentar	Fallo temporal que no es realmente un error. En `sendmail`, esto significa que una aplicación de correo, por ejemplo, no puede establecer una conexión, y la solicitud se debe volver a intentar más tarde.
76	Error remoto en protocolo	El sistema remoto devolvió algo que “no era posible” durante un intercambio de protocolo.
77	Permiso denegado	No tiene permiso suficiente para efectuar la operación. Este mensaje no está destinado para problemas del sistema de archivos, que debe usar `NOINPUT` o `CANTCREAT`, sino que está destinado para permisos de nivel superior. Por ejemplo, `kre` utiliza este mensaje para restringir a los estudiantes a los que se puede enviar correos.
78	Error de configuración	El sistema detectó un error en la configuración.
79	No se encuentra la entrada	Entrada no encontrada.
79	Valor máximo mostrado	El valor más alto para mensajes de error.

Índice

B

C

D

E

N

O

P

R

S

T

U

V

X