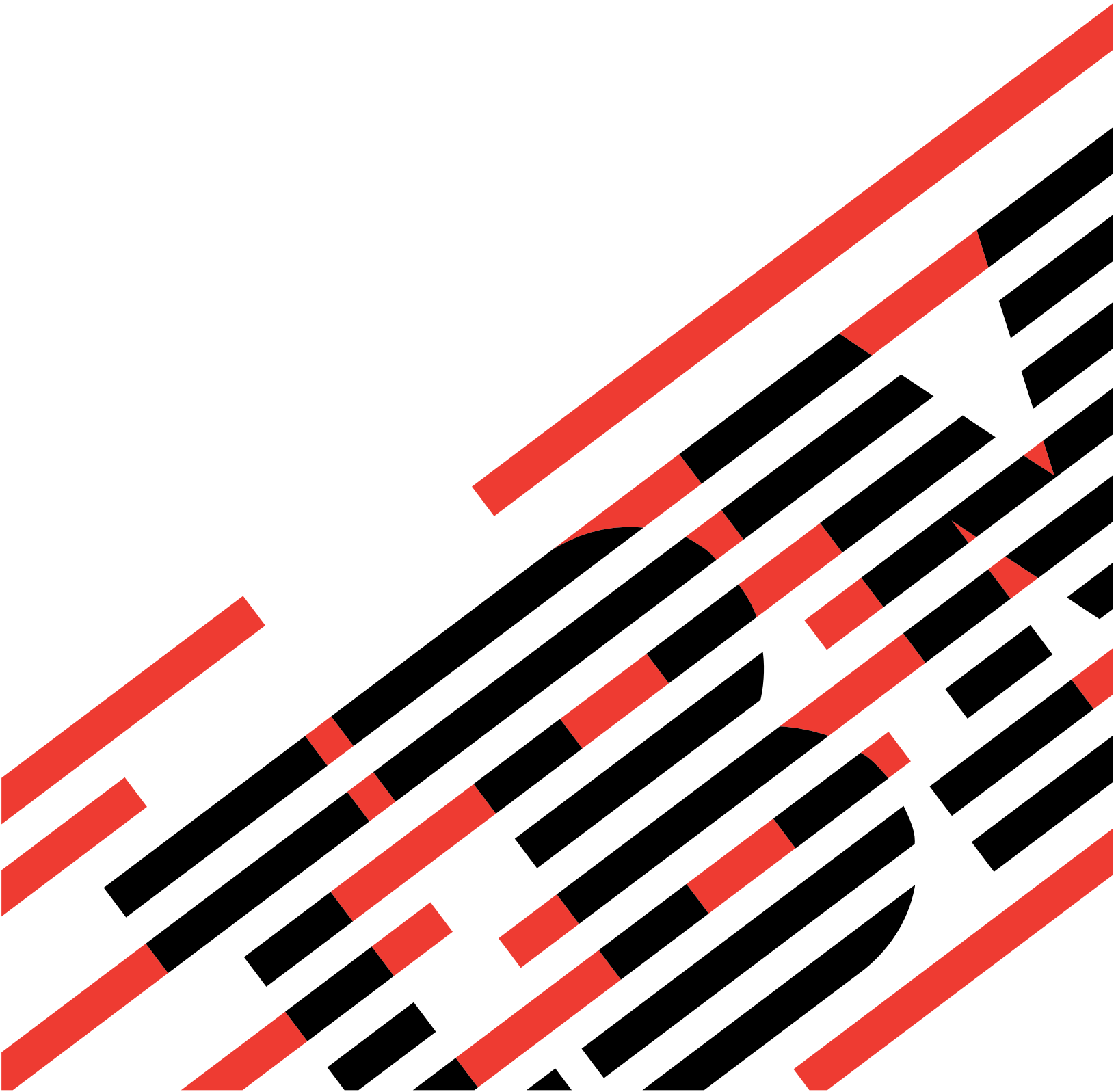
IBM

eserver

iSeries

Servicios de acceso remoto: conexiones PPP



iSeries

Servicios de acceso remoto: conexiones PPP

Contenido

Parte 1. Servicios de acceso remoto: conexiones PPP

El **protocolo punto a punto** (PPP) es un estándar de Internet para transmitir datos a través de líneas serie. Es el protocolo de conexión que más se utiliza entre los proveedores de servicios de Internet (ISP). PPP permite que las máquinas individuales puedan acceder a las redes, las cuales proporcionan a su vez acceso a Internet. El servidor iSeries incluye soporte PPP de TCP/IP como parte de la conectividad de red de área amplia (WAN).

Podrá intercambiar datos entre ubicaciones si utiliza PPP para conectar una máquina remota al servidor iSeries. Mediante PPP, los sistemas remotos conectados al servidor iSeries pueden acceder a los recursos o a las otras máquinas que pertenecen a la misma red que el servidor. También podrá configurar su servidor iSeries para que se conecte a Internet utilizando PPP. El *asistente de conexión a Internet de Operations Navigator* le podrá orientar durante el proceso de conectar el servidor iSeries a Internet.

- Novedades en la versión V5R1: este capítulo describe las actualizaciones que se han hecho en los servicios de acceso remoto en este release.
- El capítulo Imprimir este tema le indica cómo puede bajar o imprimir la versión PDF de esta información.

Qué son los servicios de acceso remoto: conexiones PPP

Estos temas son una introducción a los servicios de acceso remoto que están disponibles en el servidor iSeries 400. Los temas que figuran más abajo pueden ayudarle a planificar un entorno PPP para la red.

- **Escenarios de PPP** son ejemplos de distintas implementaciones de conectividad PPP. Cada ejemplo proporciona instrucciones y especifica valores de ejemplo para configurar la conexión PPP.
- **Planificar PPP** facilita información sobre los conceptos de PPP y los requisitos del servidor iSeries 400 para las conexiones PPP.

Utilizar los servicios de acceso remoto: conexiones PPP

Estos temas pretenden servirle de ayuda a medida que configura y gestiona las conexiones PPP en el servidor iSeries 400.

- **Configurar PPP** presenta los pasos básicos para configurar una conexión PPP.
- **Gestionar PPP** proporciona información que pretende orientarle en el proceso de gestionar las conexiones PPP.
- **Resolución de problemas de PPP** expone los errores básicos de las conexiones PPP y le indica dónde puede encontrar información relacionada con la resolución de problemas.

Aquí también puede encontrar más información sobre PPP. En esta página hay enlaces que permiten acceder a información útil relacionada con el servidor iSeries.

Capítulo 1. Novedades en la versión V5R1

Una interfaz de Operations Navigator mejorada y más fácil de usar

- Ahora, en Operations Navigator, a PPP se le conoce como **Servicios de acceso remoto**. Es una carpeta que está en el directorio Red. En **Servicios de acceso remoto** están los siguientes objetos:
  - **Perfiles de conexión de originador**, que son conexiones punto a punto que se originan en el servidor iSeries local y se reciben en un sistema remoto. Con este objeto podrá configurar las conexiones salientes.
  - **Perfiles de conexión de receptor**, que son conexiones punto a punto que se originan en un sistema remoto y se reciben en el servidor iSeries local. Con este objeto podrá configurar las conexiones entrantes.
  - **Módems**, que le permite trabajar con los módems y sus propiedades. Podrá establecer parámetros para un módem o para un adaptador de terminal de red digital de servicios integrados (RDSI).

  El elemento de menú **Servicios** asociado a la carpeta de servicios de acceso remoto permite al usuario configurar los servicios de RADIUS y DHCP que están disponibles para todos los perfiles de conexión de receptor nuevos y existentes.
- En este release está disponible el soporte del protocolo multienlace PPP y del protocolo de asignación de ancho de banda (BAP).
- Se ha añadido soporte de políticas de grupo bajo **Políticas de acceso de grupo**. Puede utilizar este soporte para definir los parámetros de configuración que se aplican a las conexiones entrantes y para administrar las políticas de grupos de usuarios de acceso remoto. **Políticas de acceso de grupo** le permite controlar las opciones de conectividad PPP a nivel de usuario, en vez de controlarlas solo a nivel de perfil PPP. También puede controlar opciones de conectividad como los ID de filtro y el reenvío de IP. **Políticas de acceso de grupo** está bajo la carpeta **Perfiles de conexión de receptor**.
- Se puede configurar y utilizar el soporte de cliente de WAN DHCP mediante un perfil de conexión de receptor para gestionar las direcciones IP asignadas a los usuarios de acceso remoto.
- Se puede configurar y utilizar el soporte RADIUS mediante un perfil de conexión de receptor. RADIUS proporciona servicios centralizados de gestión de autenticación, contabilidad y direcciones IP.
- Se han añadido cuatro modalidades nuevas de operación para los perfiles de conexión L2TP: marcación remota, marcación remota a petición, iniciador a petición e iniciador multisalto. Hallará más información en la ayuda en línea.
- Se ha añadido EAP al soporte de autenticación PPP. El soporte actual permite utilizar el protocolo de autenticación CHAP o PAP.
- Se ha añadido el asistente de conexión universal como opción para los perfiles de conexión de originador. Se utiliza para configurar un perfil que el software de soporte electrónico al cliente puede emplear para conectarse a IBM.
- Han dejado de estar soportados los perfiles del protocolo SLIP definidos con los tipos de línea ASYNC. En Operations Navigator está disponible una vía de migración manual para migrar esos perfiles a un perfil de conexión SLIP o PPP utilizando el tipo de línea PPP.
- Se han añadido nuevos adaptadores de hardware (el IOA 2771 y el IOA 2772).
- Se ha cambiado el nombre del asistente de conexión por línea telefónica de IBM Global Network, que ahora se llama **asistente de conexión por línea telefónica de AT&T Global Network**. Este asistente orienta al usuario en el proceso de crear un perfil de conexión de originador para acceder a una aplicación de intercambio de correo o de acceso telefónico a redes en AT&T Global Network.
- El **asistente Nueva conexión por línea telefónica de IBM** orienta a los usuarios en el proceso de crear un perfil de conexión de originador para acceder a un proveedor de servicios de Internet (ISP) o a una intranet.

Información más reciente acerca de PPP y L2TP:

Si desea obtener los últimos arreglos temporales del programa (PTF) y la información de configuración más reciente acerca de PPP y L2TP, acceda al enlace PPP desde la página de presentación de TCP/IP para el servidor iSeries  .

Este enlace proporciona la información más reciente que complementa y prevalece sobre la información incluida en el tema **Servicios de acceso remoto: conexiones PPP**.

Información solicitada por los usuarios:

- Consejos para gestionar las conexiones PPP utilizando Operations Navigator
- Información de resolución de problemas de PPP básica

Capítulo 2. Imprimir este tema

Puede ver o bajar una versión PDF de este documento para verlo o imprimirlo. Si desea ver los archivos PDF, necesitará Adobe® Acrobat® Reader. Puede bajar una copia desde Adobe .

Para ver o bajar la versión PDF, seleccione Servicios de acceso remoto: conexiones PPP (277 KB o, aproximadamente, 58 páginas).

Si quiere guardar un archivo PDF en la estación de trabajo para verlo e imprimirlo:

1. Abra el archivo PDF en el navegador (pulse el enlace anterior).
2. En el menú del navegador, pulse **Archivo**.
3. Pulse **Guardar como**.
4. Navegue hasta el directorio en el que desea guardar el archivo PDF.
5. Pulse **Guardar**.

Capítulo 3. Escenarios de PPP

Los siguientes escenarios pretenden ayudarle a comprender cómo funciona PPP y de qué manera puede implementar un entorno PPP en la red. Estos escenarios presentan conceptos fundamentales de PPP de los que se pueden beneficiar los usuarios principiantes y los experimentados antes de pasar a las tareas de planificación y configuración.

Conectar clientes remotos al servidor iSeries

Los usuarios remotos, como los teletrabajadores o los clientes móviles, necesitan acceder con frecuencia a la red de una empresa. Estos clientes de acceso telefónico pueden obtener acceso a un servidor iSeries con PPP.

Conectar la LAN de oficina a Internet con un módem

Normalmente, los administradores configuran redes de oficina que permiten a los empleados acceder a Internet. Pueden conectar un módem para conectar el servidor iSeries a un proveedor de servicios de Internet (ISP). Los clientes PC conectados a la LAN pueden comunicarse con Internet utilizando el servidor iSeries como pasarela.

Conectar las redes corporativa y remota con un módem

El módem permite que dos ubicaciones remotas (como una oficina central y una sucursal) intercambien datos entre ellas. PPP puede conectar las dos LAN entre sí estableciendo una conexión entre un servidor iSeries situado en la oficina central y otro servidor iSeries situado en la sucursal.

PPP y DHCP en un solo servidor iSeries

Los clientes de acceso telefónico o los usuarios remotos pueden obtener acceso a un servidor iSeries situado en la red de una empresa con PPP. Los servicios DHCP existentes en ese mismo servidor iSeries asignan dinámicamente direcciones IP a esos clientes.

Perfil DHCP y PPP en distintos servidores iSeries

Por cuestiones de seguridad o debido al diseño físico de una red, la mayoría de las empresas deciden separar los servicios de red y distribuirlos en distintos servidores. Este escenario maneja la complejidad adicional que supone tener un servidor PPP y un servidor DHCP independientes. Al igual que en el escenario anterior, esta configuración permite a los usuarios remotos establecer conexión por línea telefónica y obtener acceso a la red de una empresa.

PPP y VPN: túnel voluntario L2TP protegido por VPN

Una sucursal se puede conectar a la oficina corporativa por medio del protocolo L2TP (Layer 2 Tunnel Protocol). Un túnel voluntario L2TP establece un enlace PPP virtual. En efecto, L2TP amplía la red de la oficina corporativa, de manera que la sucursal entra a formar parte en apariencia de la subred corporativa. VPN protege el tráfico de datos a través del túnel L2TP.

Conectar clientes remotos al servidor iSeries

Situación: como administrador de la red de su empresa, debe mantener el servidor iSeries y los clientes de la red. En vez de venir a trabajar para resolver y arreglar problemas, tal vez preferiría tener la posibilidad de trabajar desde una ubicación remota, como desde su casa. Puesto que su empresa no tiene una conexión de red enlazada a Internet, usted podría establecer conexión por línea telefónica con el servidor iSeries utilizando una conexión PPP. Además, el único módem que tiene actualmente es el módem ECS 7852-400, que desea utilizar para la conexión.

Figura 1. Conectar clientes remotos al servidor iSeries

Solución: puede emplear PPP para conectar el PC de su casa al servidor iSeries utilizando el módem que tiene. Puesto que va a emplear el módem ECS para este tipo de conexión PPP, deberá asegurarse de que el módem está configurado para las dos modalidades, la síncrona y la asíncrona. La ilustración anterior representa un servidor iSeries con servicios PPP que está conectado a una LAN con dos PC. A continuación, el trabajador remoto establece conexión telefónica con el servidor iSeries, se autentica y luego entra a formar parte de la red de trabajo (`192.168.1.0`). En este caso, es más fácil asignar una dirección IP estática al cliente de acceso telefónico.

El trabajador remoto utiliza CHAP-MD5 para autenticarse en el servidor iSeries. El servidor iSeries no puede utilizar MS_CHAP, por lo que será necesario asegurarse de que el cliente PPP está establecido para usar CHAP-MD5.

Si desea que los trabajadores remotos tengan acceso a la red de la empresa tal como se ha indicado más arriba, será preciso activar el reenvío de IP en la pila de TCP/IP y también el perfil de receptor PPP. Si quiere limitar o proteger las acciones que el cliente remoto puede realizar en la red, existe la posibilidad de que utilice reglas de filtrado para manejar los paquetes IP de los clientes remotos.

La ilustración anterior solo tiene un cliente de acceso telefónico remoto, porque el módem ECS solo puede manejar las conexiones de una en una. Si usted necesita que haya múltiples clientes de acceso telefónico simultáneos, vea el apartado de planificación, donde hallará consideraciones sobre el hardware y el software.

Configuración de ejemplo:

1. Configure el acceso telefónico a redes y cree una conexión por línea telefónica en el PC remoto.

2. Configure un perfil de conexión de receptor en el servidor iSeries.

   Asegúrese de que entra esta información:

   - **Tipo de protocolo**: PPP
   - **Tipo de conexión**: línea conmutada
   - **Modalidad de operación**: respuesta
   - **Configuración de enlace**: puede ser una sola línea, una agrupación de líneas o una línea RDSI, en función del entorno que tenga.

3. En la página **General** de las propiedades del nuevo perfil punto a punto, entre un nombre y una descripción para el perfil de receptor.
4. Pulse la página **Conexión**. Elija el **Nombre de línea** apropiado o cree uno nuevo, tecleando un nombre nuevo y pulsando **Nuevo**.
   a. En la página **General**, resalte un recurso de hardware existente y establezca la trama en **Asíncrona**.
   b. Pulse la página **Módem**. En la lista de selección de nombre, elija **IBM 7852-400** (o **IBM 7852-400 International** para la mayoría de las aplicaciones que no son de EE. UU.).
   c. Pulse **Aceptar** para regresar a la página de propiedades del nuevo perfil punto a punto.
5. Pulse la página **Autenticación**.
   a. Seleccione **Exigir que este AS/400 verifique la identidad del sistema remoto**.
   b. Seleccione **Autenticar localmente utilizando una lista de validación** y añada un nuevo usuario remoto a la lista de validación.
   c. Seleccione **Permitir contraseña cifrada (CHAP-MD5)**.
6. Pulse la página **Valores de TCP/IP**.
   a. Seleccione la dirección IP local `192.168.1.1`.
   b. Para la dirección remota, seleccione **Dirección IP fija** con la dirección inicial `192.168.1.11`.
   c. Seleccione **Permitir a sistema remoto acceder a otras redes**.
7. Pulse **Aceptar** para completar el perfil.

Conectar la LAN de oficina a Internet con un módem

Situación: ahora, para la aplicación corporativa utilizada por su empresa, es preciso que los usuarios accedan a Internet. Debido a que la aplicación no necesita intercambiar grandes cantidades de datos, usted desea poder utilizar un módem para conectar a Internet el servidor iSeries y los clientes PC conectados a la LAN. La siguiente ilustración describe un ejemplo en el que se da esta situación.

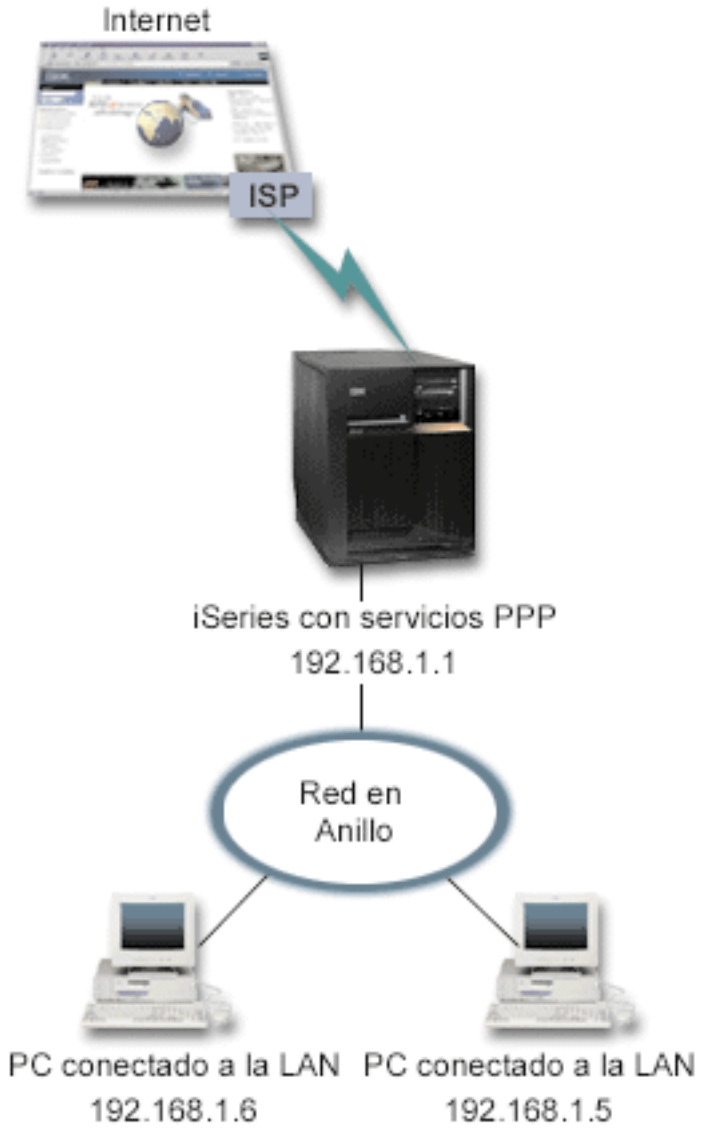


Figura 2. Conectar la LAN de oficina a Internet con un módem

Solución: puede emplear el módem ECS (u otro que sea compatible) para conectar el servidor iSeries al proveedor de servicios de Internet (ISP). Tendrá que crear un perfil de originador PPP en el servidor para establecer la conexión PPP con el ISP.

Una vez establecida la conexión entre iSeries y el ISP, los PC conectados a la LAN podrán comunicarse con Internet utilizando iSeries como pasarela. En el perfil de originador, convendrá que se asegure de que está activa la opción Ocultar direcciones, para que los clientes de la LAN, que tienen direcciones IP reservadas, puedan comunicarse con Internet.

Ahora que iSeries y la red están conectados a Internet, deberá comprender el riesgo que ello supone para la seguridad. En colaboración con el ISP, intente comprender cómo es la política de seguridad del ISP y tome medidas adicionales para proteger el servidor y la red.

Si va a emplear el módem ECS para este tipo de conexión PPP, configúrelo para las dos modalidades, la síncrona y la asíncrona. En función del uso que haga de Internet, debería plantearse la posibilidad de

aumentar el ancho de banda. Para obtener más información sobre cómo aumentar el ancho de banda de su conexión, consulte los apartados de planificación y multienlace.

Configuración de ejemplo:

1. Configure un perfil de conexión de originador en el servidor iSeries.

   Asegúrese de que selecciona esta información:

   - **Tipo de protocolo**: PPP
   - **Tipo de conexión**: línea conmutada
   - **Modalidad de operación**: marcación
   - **Configuración de enlace**: puede ser una sola línea, una agrupación de líneas o una línea RDSI, en función del entorno que tenga.
2. En la página **General** de las propiedades del nuevo perfil punto a punto, entre un nombre y una descripción para el perfil de originador.
3. Pulse la página **Conexión**. Elija el nombre de línea apropiado o cree uno nuevo, tecleando un nombre nuevo y pulsando **Nuevo**.
   a. En la página **General** de las propiedades de la línea nueva, resalte un recurso de hardware existente y establezca la trama en **Asíncrona**.
   b. Pulse la página **Módem**. En la lista de selección de nombre, elija el módem que va a utilizar.
   c. Pulse **Aceptar** para regresar a la página de propiedades del nuevo perfil punto a punto.
4. Pulse **Añadir** y teclee el número de teléfono que hay que marcar para establecer conexión con el servidor del ISP. No olvide incluir el prefijo que se necesite.
5. Pulse la página **Autenticación**, seleccione **Permitir al sistema remoto verificar la identidad de este AS/400**. Seleccione el protocolo de autenticación y entre la información de nombre de usuario o contraseña que sea necesaria.
6. Pulse la página Valores de TCP/IP.
   a. Seleccione **Asignada por sistema remoto** para las direcciones IP local y remota.
   b. Seleccione **Añadir sistema remoto como ruta por omisión**.
   c. Marque **Ocultar direcciones** para que las direcciones IP internas no se direccionen a Internet.
7. Pulse la página **DNS** y entre la dirección IP del servidor DNS proporcionada por el ISP.
8. Pulse **Aceptar** para completar el perfil.

Para utilizar el perfil de conexión con el fin de conectarse a Internet, vaya a Operations Navigator, pulse el perfil de conexión con el botón derecho del ratón y seleccione **Iniciar**. La conexión se habrá establecido satisfactoriamente cuando el estado pase a ser **Activo**. Renueve para actualizar la pantalla.

Nota: También debe asegurarse de que los demás sistemas de la red tengan definido un direccionamiento adecuado para que el tráfico TCP/IP enlazado a Internet de esos sistemas se envíe al servidor iSeries.

Conectar las redes corporativa y remota con un módem

Situación: suponga que tiene una red de sucursal y una red corporativa en dos ubicaciones distintas. Todos los días, la sucursal tiene que conectarse a la oficina corporativa con objeto de intercambiar información de base de datos para las aplicaciones de entrada de datos. La cantidad de datos intercambiados no compensa la compra de una conexión de red física, por lo que usted decide utilizar módems para conectar debidamente las dos redes.

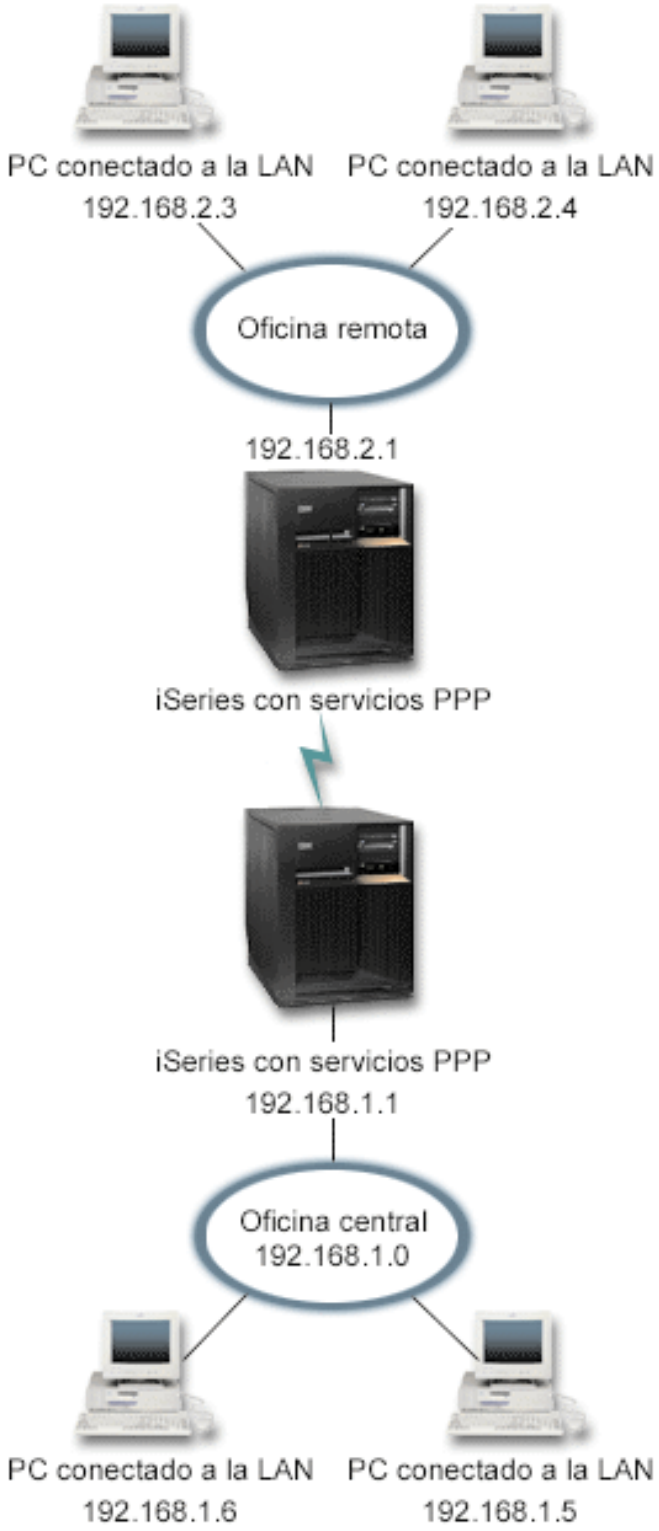


Figura 3. Conectar las redes corporativa y remota con un módem

Solución: PPP puede conectar las dos LAN entre sí estableciendo una conexión entre cada servidor iSeries como se indica en la ilustración anterior. En este caso, imagine que la oficina remota es la que

inicia la conexión con la oficina central. Debería configurar un perfil de originador en el servidor iSeries remoto, y un perfil de receptor en el servidor de la oficina central.

Si los PC de la oficina remota tienen que acceder a la LAN corporativa (192.168.1.0), habría que activar el reenvío de IP en el perfil de receptor de la oficina central. También tendría que estar activo el reenvío de IP de la pila de TCP/IP. Ello habilitaría la comunicación TCP/IP básica entre las LAN. Debería tomar en consideración factores de seguridad y un DNS para resolver los nombres de sistema principal entre las LAN.

Configuración de ejemplo:

1. Configure un perfil de conexión de originador en el servidor iSeries de la oficina remota.

   Asegúrese de que selecciona esta información:

   - **Tipo de protocolo**: PPP
   - **Tipo de conexión**: línea conmutada
   - **Modalidad de operación**: marcación
   - **Configuración de enlace**: puede ser una sola línea, una agrupación de líneas o una línea RDSI, en función del entorno que tenga.
2. En la página **General** de las propiedades del nuevo perfil punto a punto, entre un nombre y una descripción para el perfil de originador.
3. Pulse la página **Conexión**. Elija el nombre de línea apropiado o cree uno nuevo, tecleando un nombre nuevo y pulsando **Nuevo**.
   a. En la página **General** de las propiedades de la línea nueva, resalte un recurso de hardware existente y establezca la trama en **Asíncrona**.
   b. Pulse la página **Módem**. En la lista de selección de nombre, elija el módem que va a utilizar.
   c. Pulse **Aceptar** para regresar a la página de propiedades del nuevo perfil punto a punto.
4. Pulse **Añadir** y teclee el número de teléfono que hay que marcar para establecer conexión con el servidor iSeries de la oficina central. No olvide incluir el prefijo que se necesite.
5. Pulse la página **Autenticación** y seleccione **Permitir al sistema remoto verificar la identidad de este AS/400**. Seleccione **Exigir contraseña cifrada (CHAP-MD5)** y entre la información de nombre de usuario o contraseña necesaria.
6. Pulse la página **Valores de TCP/IP**.
   a. Para la dirección IP local, seleccione la dirección IP de la interfaz de LAN de la oficina remota (192.168.2.1) en el cuadro de selección **Utilizar dirección IP fija**.
   b. Para la dirección IP remota, elija **Asignada por sistema remoto**.
   c. En la sección de direccionamiento, seleccione **Añadir sistema remoto como ruta por omisión**.
   d. Pulse **Aceptar** para completar el perfil de originador.
7. Configure un **Perfil de conexión de receptor** en el servidor iSeries de la oficina central.

   Asegúrese de que selecciona esta información:

   - **Tipo de protocolo**: PPP
   - **Tipo de conexión**: línea conmutada
   - **Modalidad de operación**: respuesta
   - **Configuración de enlace**: puede ser una sola línea, una agrupación de líneas o una línea RDSI, en función del entorno que tenga.
8. En la página **General** de las propiedades del nuevo perfil punto a punto, entre un nombre y una descripción para el perfil de receptor.
9. Pulse la página **Conexión**. Elija el nombre de línea apropiado o cree uno nuevo, tecleando un nombre nuevo y pulsando **Nuevo**.
   a. En la página **General**, resalte un recurso de hardware existente y establezca la trama en **Asíncrona**.

b. Pulse la página **Módem**. En la lista de selección de nombre, elija el módem que va a utilizar.
c. Pulse **Aceptar** para regresar a la página de propiedades del nuevo perfil punto a punto.

10. Pulse la página **Autenticación**.
    a. Marque **Exigir que este AS/400 verifique la identidad del sistema remoto**.
    b. Añada un nuevo usuario remoto a la lista de validación.
    c. Marque la autenticación CHAP-MD5.
11. Pulse la página **Valores de TCP/IP**.
    a. Para la dirección IP local, seleccione la dirección IP de la interfaz de oficina central (192.168.1.1) en el cuadro de selección.
    b. Para la dirección IP remota, seleccione **Basada en ID de usuario del sistema remoto**. Aparecerá el diálogo Direcciones IP definidas por nombre de usuario. Pulse **Añadir**. Rellene los campos Nombre de usuario llamante, Dirección IP y Máscara de subred. En nuestro escenario, los valores apropiados serían:
       - Nombre de usuario llamante: `Sitio_remoto`
       - Dirección IP: `192.168.2.1`
       - Máscara de subred: `255.255.255.0`

       Pulse **Aceptar** y después otra vez **Aceptar** para regresar a la página Valores de TCP/IP.
    c. Seleccione **Reenvío de IP** para permitir a los demás sistemas de la red utilizar estos servidores iSeries como pasarela.
12. Pulse **Aceptar** para completar el perfil de receptor.

Capítulo 4. Planificar PPP

La planificación asegura que se tienen en cuenta todos los aspectos críticos al configurar un entorno PPP antes de llevar a la práctica las tareas de configuración. Estos enlaces proporcionan información pertinente que podrá ayudarle a configurar un entorno PPP.

- ¿Qué es PPP?
- Requisitos de hardware y de software
- Perfiles de conexión
- Visión general de RADIUS
- Consideraciones sobre las direcciones IP
- Autenticación del sistema
- Alternativas de conexión
- Equipo de conexión
- Consideraciones sobre el ancho de banda
- Soporte L2TP (túneles) para conexiones PPP
- Soporte de políticas de grupo
- Filtrado de paquetes IP

¿Qué es PPP?

Las máquinas emplean **PPP**, o **protocolo punto a punto**, para comunicarse a través de Internet mediante líneas telefónicas. Existe una conexión PPP cuando dos sistemas están conectados físicamente por medio de una línea telefónica. Podrá emplear PPP para conectar un sistema con otro. Por ejemplo, una conexión PPP establecida entre una sucursal y una oficina central permite a cada una de las oficinas transferir datos a la otra mediante la red.

PPP es un estándar de Internet. Es el protocolo de conexión que más se utiliza entre los proveedores de servicios de Internet (ISP). Podrá utilizar PPP para conectarse con el ISP; luego, el ISP le dará conectividad con Internet.

PPP permite la interoperatividad entre el software de acceso remoto de distintos fabricantes. También permite que múltiples protocolos de comunicaciones de red utilicen una misma línea de comunicaciones física.

A continuación figuran estándares de petición de comentarios (RFC) que describen el protocolo PPP. Hallará más información sobre las RFC en http://www.rfc-editor.org.

- RFC 1661 Protocolo punto a punto
- RFC 1662 PPP en trama al estilo de HDLC
- RFC 1994 CHAP de PPP

Requisitos de hardware y de software

En un entorno PPP se necesitan dos o más máquinas que den soporte a PPP. Una de esas máquinas, el servidor iSeries, puede ser el originador o el receptor. El servidor iSeries debe satisfacer los siguientes prerrequisitos para que los sistemas remotos puedan acceder a él:

- **Operations Navigator** Versión 4 Release 4 (V4R4) o superior con soporte de TCP/IP
- Uno de los dos perfiles de conexión:
  - Un perfil de conexión de originador para manejar las conexiones PPP salientes
  - Un perfil de conexión de receptor para manejar las conexiones PPP entrantes

- Una consola de estación de trabajo PC instalada con **Client Access Express para Windows (95/98/NT/Millenium)** habilitado con el soporte de red de Operations Navigator.
- Un adaptador instalado

  Puede elegir uno de los siguientes adaptadores:
  - 2699*: adaptador de E/S (IOA) de WAN de dos líneas
  - 2720*: adaptador de E/S PCI de WAN/Twinaxial
  - 2721*: adaptador de E/S PCI de WAN de dos líneas
  - 2745*: adaptador de E/S PCI de WAN de dos líneas (sustituye al IOA 2721)
  - 2750: adaptador de E/S PCI de interfaz de velocidad básica RDSI U (interfaz de dos hilos)
  - 2751: adaptador de E/S PCI de interfaz de velocidad básica RDSI S/T (interfaz de cuatro hilos)
  - 2761: adaptador de E/S de módem analógico de ocho puertos
  - 2771: adaptador de E/S de WAN de dos puertos, con un módem integrado V.90 en el puerto 1 y una interfaz de comunicaciones estándar en el puerto 2 (para utilizar el puerto 2 del adaptador 2771, se necesita un módem externo o un adaptador de terminal RDSI con el cable apropiado)
  - 2772: adaptador de E/S de WAN de dos puertos con módem integrado V.90

  * Para estos adaptadores se necesita un módem V.24 externo, o un adaptador de terminal RDSI, y el cable apropiado.
- Uno de los siguientes elementos, en función del tipo de conexión y de la línea:
  - módem externo o interno, o unidad de servicio de canal (CSU)/unidad de servicio de datos (DSU)
  - adaptador de terminal de red digital de servicios integrados (RDSI)
- En caso de que piense conectarse a Internet, deberá establecer una cuenta de acceso telefónico con un proveedor de servicios de Internet (ISP). El ISP debe darle los números de teléfono necesarios e información para la conexión a Internet.

Perfiles de conexión

En la versión V5R1 podemos distinguir entre dos tipos de perfiles de conexión:

- **Perfiles de conexión de originador**, que son conexiones punto a punto que se originan en el servidor iSeries local y se reciben en un sistema remoto. Con este objeto podrá configurar las conexiones salientes.
- **Perfiles de conexión de receptor**, que son conexiones punto a punto que se originan en un sistema remoto y se reciben en el servidor iSeries local. Con este objeto podrá configurar las conexiones entrantes.

Los perfiles de conexión especifican cómo debe funcionar una conexión PPP. La información incluida en los perfiles de conexión responde a estas preguntas:

- ¿Qué tipo de protocolo de conexión se va a utilizar? (PPP o SLIP)
- ¿Hace el servidor iSeries una llamada por línea telefónica para contactar con la otra máquina (originador)? ¿Espera el servidor iSeries recibir una llamada del otro sistema (receptor)?
- ¿Qué línea de comunicaciones utilizará la conexión?
- ¿Cómo debe determinar el servidor iSeries la dirección IP que va a utilizar?
- ¿Cómo debe autenticar el servidor iSeries a otro sistema? ¿Dónde ha de almacenar el servidor iSeries la información de autenticación?

El perfil de conexión es la representación lógica de los siguientes detalles de la conexión:

- Tipo de línea y de perfil
- Valores de multienlace
- Números de teléfono remotos
- Autenticación

- Valores de TCP/IP: direcciones IP y direccionamiento
- Gestión de trabajos y personalización de la conexión
- Servidores de nombres de dominio

El servidor iSeries almacena esta información de configuración en un perfil de conexión. Esta información proporciona el contexto necesario para que el servidor iSeries establezca una conexión PPP con otro sistema informático. En un perfil de conexión se incluye esta información:

- **El tipo de protocolo**. Se puede elegir entre PPP y SLIP. IBM le recomienda que utilice PPP siempre que sea posible.
- **La selección de modalidad**. El tipo de conexión y la modalidad de operación para este perfil de conexión.

  El **tipo de conexión** especifica el tipo de línea en el que se basan las conexiones y si estas son de **marcación** o de **respuesta** (originador o receptor, respectivamente). Puede elegir de entre estos tipos de conexión:
  - Línea conmutada
  - Línea alquilada (dedicada)
  - L2TP (línea virtual)

  Las opciones de modalidad de operación dependen del tipo de conexión que seleccione.
- **La configuración de enlace**. Especifica qué tipo de servicio de línea utiliza esta conexión.

  Las opciones dependen del tipo de selección de modalidad que elija. En el caso de una línea conmutada y de una línea alquilada, puede elegir de entre estas opciones:
  - Una sola línea
  - Agrupación de líneas
  - Línea RDSI

  En el caso de una línea L2TP, la opción es una línea virtual.

Visión general de RADIUS

RADIUS (Remote Authentication Dial In User Service) es un protocolo estándar de Internet que proporciona servicios centralizados de gestión de autenticación, contabilidad e IP para los usuarios de acceso remoto en una red de acceso telefónico distribuida.

El modelo cliente-servidor de RADIUS tiene un servidor de acceso a red (NAS) que funciona como cliente para un servidor RADIUS. El servidor iSeries, al actuar como NAS, envía información de usuario y conexión a un servidor RADIUS designado, mediante el protocolo estándar de RADIUS definido en la RFC 2865.

Los servidores RADIUS actúan en las peticiones de conexión de usuario recibidas autenticando al usuario y luego devuelven toda la información de configuración necesaria al NAS, para que el NAS (el servidor iSeries) pueda prestar servicios autorizados al usuario de marcación de entrada autenticado.

Las peticiones de contabilidad de RADIUS se manejan de manera similar. La información de contabilidad de los usuarios remotos se puede enviar a un servidor de contabilidad RADIUS designado. El protocolo estándar de contabilidad de RADIUS está definido en la RFC 2866.

El servidor de contabilidad RADIUS actúa en las peticiones de contabilidad recibidas anotando la información de la petición de contabilidad RADIUS.

Consideraciones sobre las direcciones IP

Perfiles de conexión de originador:

Normalmente, las direcciones IP local y remota definidas para un perfil de originador se definirán como **Asignadas por el sistema remoto**. Esto permite a los administradores del sistema remoto tener el control sobre las direcciones IP que se utilizarán para la conexión. La mayoría de las conexiones con los proveedores de servicios de Internet (ISP) estarán definidas de esta forma, aunque muchos ISP pueden ofrecer direcciones IP fijas cobrando una tarifa adicional.

Si define direcciones IP fijas para la dirección local o remota, tendrá que asegurarse de que el sistema remoto está definido para aceptar las direcciones que usted haya definido. Una aplicación típica lo que hace es definir la dirección local como dirección IP fija, y la remota como asignada por el sistema remoto. El sistema que va a conectar se puede definir de la misma manera para que, en el momento de la conexión, los dos sistemas se intercambien las direcciones como procedimiento para averiguar la dirección del sistema remoto. Esto podría ser de utilidad en el caso de una oficina que llamara a otra para obtener conectividad temporal.

Otra consideración a tener en cuenta es si desea habilitar el enmascaramiento de dirección IP. Por ejemplo, si el servidor iSeries se conecta a Internet por medio de un ISP, esto podría permitir que una red conectada detrás del servidor iSeries accediera también a Internet. Básicamente, el servidor iSeries 'ocultará' las direcciones IP de los sistemas de la red que hay detrás de la dirección IP local asignada por el ISP, haciendo así que todo el tráfico IP proceda en apariencia del servidor iSeries. También podrá tener en cuenta consideraciones adicionales sobre el direccionamiento para los dos sistemas de la LAN (con el fin de asegurar que el tráfico Internet de los dos sistemas se envíe al servidor iSeries) y para el servidor iSeries, en el que tendrá que habilitar el recuadro 'añadir sistema remoto como ruta por omisión'.

Perfiles de conexión de receptor:

Para estos tipos de perfiles de conexión se deben tener en cuenta muchas más consideraciones y opciones sobre las direcciones IP que para los perfiles de conexión de originador. La manera de configurar las direcciones IP depende totalmente de lo que esté intentando lograr:

- Permitir que en un momento dado se conecte un solo usuario o múltiples usuarios.
- Definir direcciones tomando como base el ID del usuario llamante.
- Permitir al usuario remoto definir su propia dirección IP.
- Utilizar DHCP o RADIUS para definir una dirección IP.
- Permitir a los usuarios remotos acceder a recursos situados en una LAN conectada.

Dirección IP local

En el caso de un perfil de receptor de una sola conexión, puede definir una dirección IP exclusiva o bien utilizar una dirección IP local existente en el servidor iSeries. Esta pasará a ser la dirección que va a identificar el extremo de la conexión PPP que corresponde al servidor iSeries. En el caso de los perfiles de receptor definidos para dar soporte a múltiples conexiones al mismo tiempo, deberá emplear una dirección IP local existente, que se puede visualizar mediante la flecha de la lista desplegable. Si no están disponibles direcciones IP locales ya existentes, podrá crear una dirección IP virtual con esta finalidad.

Dirección IP remota

Están disponibles numerosas opciones para asignar la dirección IP remota de distintas maneras. Si utiliza una dirección IP local existente que sirva para conectar el servidor iSeries a una LAN, la dirección IP remota que seleccione puede ayudar a determinar si va a permitir al usuario remoto formar parte en apariencia de esa LAN y compartir sus recursos. Para lograrlo, se utiliza una dirección IP remota que esté en el mismo rango de direcciones que los sistemas conectados a la LAN. También deberá habilitar el

reenvío de IP para el perfil de conexión de receptor, así como hacer que esté habilitado para todo el sistema servidor iSeries con el fin de garantizar que el servidor iSeries pueda funcionar como pasarela.

En la siguiente lista figuran las opciones de asignación de dirección IP remota:

- **Dirección IP fija**

  Se define la dirección IP única que se ha de dar a los usuarios remotos cuando se conectan por línea telefónica. Es una dirección IP solo de sistema principal (la máscara de subred es 255.255.255.255) y solamente está disponible para los perfiles de receptor de una sola conexión.
- **Agrupación de direcciones**

  Se define la dirección IP inicial y luego un rango que indica cuántas direcciones IP adicionales se definen. A cada usuario que se conecte se le dará una dirección exclusiva que esté comprendida dentro del rango definido. Es una dirección IP solo de sistema principal (la máscara de subred es 255.255.255.255) y solamente está disponible para los perfiles de receptor de múltiples conexiones.
- **RADIUS**

  La dirección IP remota y su máscara de subred vendrán determinadas por el servidor Radius. Esta opción solo está disponible si se definen los siguientes elementos:
  - El soporte de Radius para autenticación y sistema de direcciones IP se ha habilitado en la configuración de los servicios del servidor de acceso remoto.
  - La autenticación está habilitada para el perfil de conexión de receptor y definida para que la lleve a cabo remotamente el servidor Radius.
- **DHCP**

  La dirección IP remota viene determinada por el servidor DHCP. Esta opción solo está disponible si el soporte de DHCP se ha habilitado en la configuración de los servicios del servidor de acceso remoto. Es una dirección IP solo de sistema principal (la máscara de subred es 255.255.255.255).
- **Basada en el ID de usuario del sistema remoto**

  La dirección IP remota viene determinada por el ID de usuario definido para el sistema remoto al autenticarse. Ello permite al administrador asignar distintas direcciones IP remotas (y las máscaras de subred asociadas) al usuario que accede por línea telefónica. Permite asimismo que se definan rutas adicionales para cada uno de esos ID de usuario, lo que hace posible que el entorno se pueda adaptar al usuario remoto conocido. Para que esta función se lleve a cabo como es debido, es preciso habilitar la autenticación.

En la siguiente lista figuran las opciones adicionales para las direcciones IP remotas:

- **Definir direcciones IP adicionales basándose en el ID de usuario del sistema remoto**

  Esta opción le permite definir direcciones tomando como base el ID de usuario del sistema remoto. Esta opción se selecciona (y se debe usar) automáticamente si el método de asignación de la dirección IP remota se define como **Basada en ID de usuario de sistema remoto**. Esta opción también está permitida para los métodos de asignación de direcciones Dirección IP fija y Agrupación de direcciones. Cuando un usuario remoto se conecta al servidor iSeries, se hará una búsqueda para averiguar si se ha definido una dirección IP remota de manera específica para este usuario. Si está definida, se utilizará esa dirección, la máscara y un conjunto de posibles rutas para esa conexión. Si el usuario no está definido, la dirección tomará por omisión la dirección IP fija definida o la próxima dirección IP disponible de la agrupación de direcciones.
- **Permitir al sistema remoto definir su propia dirección IP**

  Esta opción permite a un usuario remoto definir su propia dirección IP si así lo negocia. Si el usuario no negocia utilizar su propia dirección IP, la dirección IP remota vendrá determinada por el método definido para la asignación de dirección IP remota. Esta opción está inhabilitada inicialmente y hay que ser muy precavido a la hora de habilitarla.

Autenticación del sistema

El protocolo PPP define dos tipos de autenticación que los sistemas similares pueden utilizar para identificarse mutuamente:

La autenticación de sistema local especifica el protocolo de autenticación y el nombre de usuario y la contraseña asociados a un perfil de conexión PPP. Cuando se establece una conexión con el sistema remoto y este solicita la autenticación, para la petición de identificación pertinente se utiliza el nombre de usuario, la contraseña y el protocolo especificados para la autenticación del sistema local.

La autenticación del sistema remoto especifica el protocolo de autenticación y la lista de validación que deben usarse para autenticar los nombres de usuarios remotos y las contraseñas asociados a un perfil de conexión PPP.

Las opciones para la autenticación del sistema son:

- El protocolo de autenticación de reconocimiento de identificación (CHAP)
- El protocolo de autenticación de contraseñas (PAP)
- El protocolo de autenticación extensible (EAP)
- Métodos de validación de sistema remoto
  - RADIUS (Remote Authentication Dial In User Service)
  - Lista de validación

CHAP

El **protocolo de autenticación de reconocimiento de identificación (CHAP)** emplea un algoritmo (MD-5) para calcular un valor que solo conocen el sistema que autentica y el dispositivo remoto. Con CHAP, el ID de usuario y la contraseña siempre están cifrados, lo que lo convierte en un protocolo más seguro que PAP. Este protocolo es eficaz contra los intentos de acceder mediante técnicas de reproducción o de ensayo y error. La autenticación CHAP puede realizar más de una petición de identificación durante una misma conexión.

El sistema que autentica envía una petición de identificación al dispositivo remoto que intenta conectarse a la red. El dispositivo remoto responde enviando un valor calculado mediante un algoritmo (MD-5) que conocen ambos dispositivos. El sistema que autentica compara la respuesta con la que ha calculado él. Se reconoce la autenticidad si los valores coinciden; en caso contrario, se finaliza la conexión.

PAP

El **protocolo de autenticación de contraseñas (PAP)** utiliza un reconocimiento de dos vías que ofrece al sistema similar un método simple de establecer su identidad. El reconocimiento se realiza al establecer un enlace. Después de establecer el enlace, el dispositivo remoto envía el ID de usuario y la contraseña al sistema que autentica. En función de si los valores son correctos o no, el sistema que autentica continúa o finaliza la conexión.

Para la autenticación por PAP, hay que enviar el nombre de usuario y la contraseña al sistema remoto en forma de texto sin cifrar. Con PAP, el ID de usuario y la contraseña nunca se cifran, lo que permite capturarlos si se rastrean y los hace vulnerables al ataque de piratas informáticos. Por esta razón, conviene utilizar el protocolo CHAP siempre que sea posible.

EAP

El **protocolo de autenticación extensible (EAP)** permite a los módulos de autenticación de terceros interaccionar con la implementación de PPP. EAP amplía PPP proporcionando un mecanismo de soporte estándar para esquemas de autenticación como las tarjetas testigo (inteligentes), Kerberos, clave pública y S/Key. EAP surge como respuesta a la demanda incesante de incrementar la autenticación RAS con

dispositivos de seguridad de terceros. EAP protege las VPN seguras contra los piratas que realizan ataques mediante diccionario y adivinan contraseñas. EAP mejora los protocolos PAP y CHAP.

Con EAP, los datos de autenticación no se incluyen en la información, sino junto con ella. Esto permite a los servidores remotos negociar la autenticación necesaria antes de recibir o pasar información.

Actualmente, el servidor iSeries solo da soporte a una versión de EAP que equivale básicamente a CHAP-MD5. Sin embargo, se puede utilizar la autenticación remota si se emplea un servidor RADIUS que dé soporte a algunos de los esquemas de autenticación adicionales descritos más arriba.

RADIUS

RADIUS (Remote Authentication Dial In User Service) es un protocolo de autenticación abierto y de fácil integración. Las peticiones de autenticación de los usuarios remotos, iniciadas desde un servidor iSeries y enviadas a un servidor RADIUS centralizado, se aceptan o deniegan. Toda información de seguridad perteneciente al usuario autenticado se puede ubicar en una sola base de datos central, en vez de estar dispersa en la red en distintos dispositivos.

El servidor RADIUS devuelve al servidor iSeries los servicios que el usuario autenticado esté autorizado a utilizar, como podría ser una dirección IP.

Si no es posible establecer contacto con un servidor RADIUS, el servidor iSeries puede direccionar las peticiones de autenticación a un servidor alternativo. Ello permite a las empresas globales prestar a los correspondientes usuarios un servicio de marcación de entrada con un ID de usuario de inicio de sesión exclusivo para el acceso corporativo amplio, con independencia del punto de acceso que se utilice.

Cuando un servidor RADIUS recibe una petición de autenticación, esta se valida y luego el servidor RADIUS descifra el paquete de datos para acceder a la información de nombre de usuario y contraseña. La información se pasa al sistema de seguridad apropiado que esté soportado. El sistema de seguridad podría ser de archivos de contraseñas UNIX, Kerberos, un sistema de seguridad disponible comercialmente o incluso uno que hubiera sido desarrollado de manera personalizada.

Lista de validación

Las listas de validación sirven para almacenar información de ID de usuario y contraseña perteneciente a los usuarios remotos. Podrá utilizar las listas de validación existentes o crear la suya propia en la página de autenticación de perfil de conexión de receptor. Para las entradas de las listas de validación, tendrá que identificar un tipo de protocolo de autenticación para asociarlo al ID de usuario y a la contraseña. Puede ser **cifrado - CHAP-MD5/EAP** o **no cifrado - PAP**.

Hallará más información en la ayuda en línea.

Alternativas de conexión

El protocolo punto a punto (PPP) puede transmitir datagramas a través de enlaces punto a punto serie. PPP permite interconectar equipo de múltiples proveedores y múltiples protocolos al estandarizar las comunicaciones punto a punto. La capa de enlace de datos de PPP emplea tramas al estilo de HDLC para encapsular los datagramas a través de enlaces de telecomunicaciones punto a punto tanto asíncronos como síncronos.

Si bien PPP da soporte a una amplia gama de tipos de enlaces, el protocolo SLIP solo da soporte a los tipos de enlaces asíncronos. En general, SLIP solo se emplea para los enlaces analógicos. Las compañías telefónicas locales prestan los servicios de telecomunicaciones tradicionales en una escala ascendente de posibilidades y costes. Estos servicios utilizan, entre el cliente y la oficina central, los recursos de red de voz de las compañías telefónicas existentes.

Los enlaces PPP establecen una conexión física entre un sistema principal local y uno remoto. Los enlaces conectados proporcionan ancho de banda dedicado. También los hay con una gran variedad de velocidades de datos y protocolos. Con los enlaces PPP, podrá elegir de entre estas alternativas de conexión:

- Líneas telefónicas analógicas
- Servicios digitales y DDS
- Conmutada-56
- RDSI
- T1/E1 y T1 fraccionaria
- Frame Relay

La tabla que sigue muestra una comparación de los servicios de comunicaciones y sus costes relativos. Los costes no reflejan los precios actuales. Por el contrario, muestran la diferencia relativa que hay entre los servicios. Las tarifas de coste en las líneas alquiladas se suelen calcular en función de la distancia, mientras que en las líneas conmutadas también interviene el tiempo.

Tabla 1. Comparación de los servicios de comunicaciones y sus costes relativos

Nota: esta tabla solo se muestra a efectos de ilustración. No incluye todas las configuraciones soportadas del servidor iSeries. Los costes no reflejan los precios actuales.				
Línea conmutada	**Velocidad** de línea	**Equipo necesario**	**Interfaz estándar y tipo de protocolo**	**Coste aproximado de la línea por mes**
Analógica	Entre 33,6 Kbps y 56 Kbps	Módem	RS232 / Asíncrono	Entre 4.000 y 30.000 ptas.
Conmutada 56	56 Kbps	Marcación CSU/DSU V.25bis	V.35/RS449 Síncrono	Entre 10.000 y 50.000 ptas.
RDSI	56/128 Kbps	Adaptador de terminal	RS232/V.35 Asíncrono/Síncrono	Entre 10.000 y 50.000 ptas.

Línea dedicada	**Velocidad de línea**	**Equipo necesario**	**Interfaz estándar y tipo de protocolo**	Coste aproximado de la línea por mes
Servicios digitales y DDS	56 Kbps	CSU/DSU	V.35/RS449 Síncrono	Entre 10.000 y 100.000 ptas.
T1 fraccionaria	De 64 Kbps a 1,54 Mbps	CSU/DSU o T1 mux	V.35/RS449 Síncrono	Entre 20.000 y 400.000 ptas.
T1	1,54 Mbps	CSU/DSU	V.35/RS449 Síncrono	Entre 70.000 y 400.000 ptas.
Frame Relay	De 64 Kbps a 1,54 Mbps	CSU/DSU o T1 mux	V.35/RS449	De 70.000 ptas. para arriba

Líneas telefónicas analógicas

La conexión analógica, que emplea módems para transportar datos a través de líneas alquiladas o conmutadas, se sitúa en la parte inferior de la escala punto a punto. Las líneas alquiladas son conexiones a todo tiempo entre dos ubicaciones especificadas, mientras que las líneas conmutadas son líneas telefónicas de voz a intervalos regulares. Los módems actuales más rápidos funcionan a la velocidad de 56 Kbps con datos sin comprimir. Sin embargo, dada la proporción de señal a ruido en los circuitos telefónicos de grado de voz no condicionados, esta velocidad es con frecuencia inalcanzable.

Los fabricantes de módems, cuando proclaman velocidades superiores en bits por segundo (bps), suelen basarse en el algoritmo de compresión de datos (CCITT V.42bis) utilizado por los módems. Aunque V.42bis puede llegar a reducir el volumen de datos hasta la cuarta parte, la compresión depende de los datos y muy pocas veces ni siquiera llega al 50%. Los datos ya comprimidos o los cifrados pueden

incluso aumentar cuando se aplica V.42bis. X2 o 56Flex amplía la velocidad en bps hasta los 56 K para las líneas telefónicas analógicas. Esta es una tecnología híbrida, en la que un extremo del enlace PPP debe ser digital, mientras que el otro extremo debe ser analógico. Además, la velocidad de 56 Kbps solo es aplicable cuando se mueven datos desde el extremo digital al extremo analógico del enlace. Esta tecnología está especialmente indicada para las conexiones con los ISP, estando el extremo digital del enlace y el hardware en la ubicación de los ISP. Por lo general, podrá conectarse a un módem analógico V.24 a través de una interfaz serie RS232 con un protocolo asíncrono a velocidades de hasta 115,2 Kbps.

El estándar V.90 puso final al problema de compatibilidad de K56flex/x2. El estándar V.90 es el resultado de un compromiso entre los partidarios de x2 y K56flex en el sector del módem.

Viendo la red telefónica pública conmutada como red digital, la tecnología V.90 puede acelerar los datos que van de Internet a una máquina hasta alcanzar velocidades de 56 Kbps. La tecnología V.90 se distingue de los otros estándares en que codifica los datos digitalmente, en vez de modularlos como lo hacen los módems analógicos. La transferencia de datos es un método asimétrico, por lo que las transmisiones en sentido ascendente (en su mayoría, mandatos emitidos al pulsar una tecla o el ratón desde una máquina a una ubicación central, para los que se necesita menos ancho de banda) siguen fluyendo a las velocidades convencionales de hasta 33,6 Kbps. Los datos enviados desde un módem lo hacen como transmisión analógica que refleja el estándar V.34. Solo las transferencias de datos en sentido descendente se aprovechan de las altas velocidades de V.90.

Servicios digitales y DDS

Servicio digital

Con el servicio digital, los datos, al viajar de la máquina del emisor a la oficina central de la compañía telefónica, al suministrador de larga distancia, a la oficina central, y luego a la máquina del receptor, lo hacen todo el tiempo con formato digital. El sistema de señales digitales ofrece un ancho de banda y una fiabilidad superiores que el sistema de señales analógicas. Los sistemas de señales digitales eliminan muchos de los problemas con los que deben enfrentarse los módems analógicos, como son el ruido, la calidad de línea variable y la atenuación de la señal.

DDS

Los servicios de datos digitales (DDS) son los más básicos de todos los servicios digitales. Los enlaces DDS son conexiones alquiladas y permanentes, que se ejecutan a velocidades fijas de hasta 56 Kbps. A estos servicios también se les llama normalmente DS0.

Podrá conectarse a DDS utilizando un recuadro especial que se llama Unidad de servicios de canal/Unidad de servicios de datos (CSU/DSU), que viene a ocupar el lugar del módem en el escenario analógico. DDS tiene limitaciones físicas, relacionadas sobre todo con la distancia entre la CSU/DSU y la oficina central de la compañía telefónica. DDS funciona mejor cuando la distancia no supera los 9.144 metros (30.000 pies). Las compañías telefónicas pueden implementar distancias más largas con extensores de señal, pero el servicio aumenta de precio. DDS es un servicio que está más indicado para conectar dos ubicaciones servidas por una misma oficina central. En el caso de las conexiones situadas a larga distancia, que implican distintas oficinas centrales, se pueden sumar rápidamente gastos de kilometraje que harían inviables los servicios DDS. En tal caso, Conmutada-56 podría ser una solución más adecuada. En general, podrá conectarse a una CSU/DSU de DDS a través de una interfaz serie V.35, RS 449 o X.21 con protocolo síncrono a velocidades de hasta 56 Kbps.

Conmutada-56

Si no necesita una conexión a todo tiempo, podrá ahorrarse dinero si utiliza el servicio digital conmutado, que suele llamarse Conmutada-56 (SW56). Los enlaces SW56 se parecen a la configuración de DDS en que el DTE se conecta al servicio digital por medio de una CSU/DSU. Sin embargo, una CSU/DSU de SW56 incluye un área de marcación en la que se entra el número de teléfono del sistema principal remoto. SW56 permite hacer conexiones digitales de acceso telefónico con cualquier otro abonado a

SW56 en el país o más allá de las fronteras internacionales. Las llamadas SW56 se transportan a través de la red digital de gran distancia igual que las llamadas de voz digitalizadas. SW56 utiliza los mismos números de teléfono que el sistema telefónico local, y los gastos de utilización coinciden con los de las llamadas de voz de las empresas. SW56 solo está disponible en las redes norteamericanas y está limitado a canales individuales que solo pueden transportar datos. SW56 es una alternativa para las ubicaciones en las que no está disponible RDSI. En general, podrá conectarse a una CSU/DSU de SW56 a través de una interfaz serie V.35 o RS 449 con protocolo síncrono a velocidades de hasta 56 Kbps. Con una unidad de llamada/respuesta V.25bis, los datos y el control de llamada fluyen a través de una sola interfaz serie.

RDSI

Al igual que Conmutada-56, RDSI también proporciona una conectividad digital conmutada de extremo a extremo. Sin embargo, a diferencia de los otros servicios, RDSI puede transportar voz y datos a través de una misma conexión. Hay dos tipos distintos de servicios RDSI, siendo el más común el de la interfaz de velocidad básica (BRI). La BRI tiene dos canales B de 64 Kbps para transportar los datos de cliente, y un canal D para transportar los datos de señal. Los dos canales B se pueden enlazar entre sí para dar una velocidad combinada igual a 128 Kbps. En algunas zonas, la compañía telefónica puede limitar cada uno de los canales B a una combinación de 56 Kbps o 112 Kbps. También hay una restricción física en lo que se refiere a la ubicación del cliente, que debe estar a menos de 5486,4 metros (18.000 pies) del conmutador de la oficina central. Existe la posibilidad de ampliar esta distancia con repetidores. Podrá conectarse a RDSI con un dispositivo llamado adaptador de terminal. La mayoría de los adaptadores de terminal tienen una unidad integrada de terminación de red (NT1) que permite la conexión directa con una clavija del teléfono. Normalmente, los adaptadores de terminal se conectan a la máquina informática por medio de un enlace RS232 asíncrono y utilizan el conjunto de mandatos AT para la configuración y el control, de manera muy parecida a como lo hacen los módems analógicos convencionales. Cada marca tiene su propia extensión de mandato AT para configurar los parámetros que son exclusivos de RDSI. Antes, había numerosos problemas de interoperatividad entre las distintas marcas de adaptadores de terminal RDSI. Esos problemas se debían casi todos a la gran variedad de protocolos de adaptación de velocidad que estaban disponibles en V.110 y en V.120, así como a los esquemas de vinculación de los dos canales B.

Ahora, este sector de la industria se ha decantado por el protocolo PPP síncrono con multienlace PPP para enlazar los dos canales B. Algunos productos de adaptador de terminal integran la posibilidad V.34 (módem analógico) en los adaptadores de terminal. Esto permite a los clientes que tienen una sola línea RDSI manejar las llamadas RDSI o analógicas convencionales sacando partido de la posible simultaneidad de voz/datos de los servicios RDSI. La nueva tecnología permite asimismo que un adaptador de terminal funcione del lado del servidor digital para los clientes de 56 K (X2/56Flex).

Normalmente, le interesará conectarse a un adaptador de terminal RDSI a través de una interfaz serie RS232 mediante un protocolo asíncrono a velocidades de hasta 230,4 Kbps. Sin embargo, la velocidad máxima en baudios del servidor iSeries para asíncrono a través de RS232 es de 115,2 Kbps. Lamentablemente, esto hace que la velocidad máxima de transferencia de bytes quede restringida a 11,5 Kbytes/segundo, mientras que el adaptador de terminal con multienlace tiene capacidad para 14/16 Kbytes sin comprimir. Algunos adaptadores de terminal dan soporte a síncrono a través de RS232 a 128 Kbps, pero la velocidad máxima en baudios del servidor iSeries para síncrono a través de RS232 es de 64 Kbps.

El servidor iSeries tiene capacidad para ejecutar asíncrono a través de V.35 a velocidades de hasta 230,4 Kbps, pero los fabricantes de adaptadores de terminal no suelen ofrecer una configuración de ese tipo. Los convertidores de interfaz que convierten la interfaz RS232 a V.35 podrían ser una solución razonable del problema, pero este enfoque no ha sido evaluado para el servidor iSeries. Otra posibilidad consiste en usar adaptadores de terminal con el protocolo síncrono de la interfaz V.35 a una velocidad de 128 Kbps. Aunque ya existe esta clase de adaptadores de terminal, no parece que muchos ofrezcan PPP multienlace síncrono.

T1/E1 y T1 fraccionaria

T1/E1

Una conexión T1 es un paquete compuesto por veinticuatro canales de multiplexado por división de tiempo (TDM) de 64 Kbps (DS0) a través de circuito de cobre de cuatro hilos. Esto crea un ancho de banda total de 1,544 Mbps. En Europa y en otras partes del mundo, un circuito E1 es un paquete compuesto por treinta y dos canales de 64 Kbps, dando un total de 2,048 Mbps. TDM permite que múltiples usuarios compartan un medio de transmisión digital al utilizar ubicaciones en el tiempo preasignadas. Muchas centralitas privadas (PBX) digitales sacan partido del servicio T1 para importar múltiples circuitos de llamada a través de una sola línea T1, en vez de tener 24 pares de hilos direccionados entre la centralita privada (PBX) y la compañía telefónica. Es importante darse cuenta de que T1 se puede compartir entre voz y datos. Por ejemplo, un servicio telefónico puede venir a través de un subconjunto de 24 canales de un enlace T1, dejando disponibles los demás canales para la conectividad internet. Se necesita un dispositivo multiplexor T1 para gestionar los 24 canales DS0 cuando se comparte un tronco T1 entre múltiples servicios. En el caso de una conexión individual solo de datos, el circuito se puede ejecutar sin canalizar (no se realiza TDM en la señal). Por ello, se puede emplear un dispositivo CSU/DSU más simple. En general, podrá conectarse a una CSU/DSU de T1/E1 o a un multiplexor a través de una interfaz serie V.35 o RS 449 con protocolo síncrono a velocidades múltiplos de 64 Kbps hasta 1,544 Mbps o 2,048 Mbps. La CSU/DSU o el multiplexor proporciona el cronometraje de la red.

T1 fraccionaria

Con T1 fraccionaria (FT1), un cliente puede alquilar submúltiplos de 64 Kbps de una línea T1. FT1 es de utilidad siempre que el coste de una línea T1 dedicada resulte prohibitivo para el ancho de banda real que utiliza el cliente. Con FT1, solo se paga lo que se necesita. Además, FT1 tiene la siguiente característica que no está disponible con un circuito T1 completo: el multiplexado de canales DS0 en la oficina central de la compañía telefónica. El extremo remoto de un circuito FT1 está en un conmutador de conexión cruzada de acceso digital cuyo mantenimiento realiza la compañía telefónica. Los sistemas que comparten un mismo conmutador digital pueden pasar de uno a otro canal DS0. Este esquema es muy conocido para los ISP que emplean un solo tronco T1 desde su ubicación hasta el conmutador digital de una compañía telefónica. En estos casos, se puede servir a múltiples clientes con el servicio FT1. En general, podrá conectarse a una CSU/DSU de T1/E1 o a un multiplexor a través de la interfaz serie V.35 o RS 449 con protocolo síncrono a algunos múltiplos de 64 Kbps. Con FT1, se le preasignará un subconjunto de los 24 canales. El multiplexor de T1 se debe configurar para que cubra solo las ubicaciones en el tiempo asignadas para su servicio.

Frame Relay

Frame Relay es un protocolo destinado a direccionar tramas a través de la red tomando como base el campo dirección (identificador de conexión de enlace de datos) de la trama y a gestionar la ruta o la conexión virtual.

En los Estados Unidos, las redes Frame Relay soportan las velocidades de transferencia de datos propias de las líneas T-1 (1,544 Mbps) y T-3 (45 Mbps). Podríamos decir que Frame Relay es una manera de utilizar las líneas T-1 y T-3 existentes que son propiedad de un proveedor de servicios. La mayoría de las compañías telefónicas proporcionan ahora el servicio Frame Relay para los clientes que desean conexiones a velocidades comprendidas entre 56 Kbps y las propias de T-1. (En Europa, las velocidades de Frame Relay varían de 64 Kbps a 2 Mbps). En los Estados Unidos, Frame Relay se ha hecho muy popular porque es relativamente económico. Sin embargo, en algunas zonas se está sustituyendo por tecnologías más rápidas, como ATM.

Equipo de conexión

A continuación figuran las tres clases de equipo de comunicaciones que se pueden utilizar en el entorno PPP:

- Módems
- CSU/DSU
- Adaptadores de terminal RDSI

Módems

Para las conexiones PPP se pueden emplear tanto los módems externos como los internos. El juego de mandatos usado en un módem suele estar descrito en la documentación del módem. Los mandatos sirven para restablecer e inicializar el módem y para indicar al módem que marque el número de teléfono del sistema remoto. Para poder utilizar un módem con un perfil de conexión PPP, primero habrá que definir el modelo del módem, porque cada modelo tiene mandatos de inicialización cuyas series de caracteres son distintas. Si el módem es interno, las series de los mandatos ya están definidas para utilizarse.

El servidor iSeries tiene predefinidos numerosos modelos de módem, pero se pueden definir nuevos modelos con Operations Navigator. Una definición existente puede servir de base para el nuevo tipo que se vaya a definir. Si no está seguro de cuáles son los mandatos que utiliza el módem, o si no tiene acceso a la documentación del módem, empiece por la definición del módem Hayes genérico. Las definiciones predefinidas que se envían de origen no se pueden cambiar. Sin embargo, se pueden añadir mandatos adicionales al mandato de inicialización o a la serie de marcación que ya existen.

Puede emplear el módem de soporte electrónico al cliente (ECS) que se envía junto con el servidor iSeries para establecer conexiones PPP. En los sistemas más antiguos, el módem de ECS era un módem externo IBM 7852-400. En los sistemas más recientes, los módems internos 2771 ó 2772 se pueden emplear para el soporte electrónico al cliente (ECS).

CSU/DSU

Una unidad de servicio de canal (CSU) es un dispositivo que conecta un terminal a una línea digital. Una unidad de servicio de datos (DSU) es un dispositivo que lleva a cabo funciones de protección y de diagnóstico en una línea de telecomunicaciones. En general, los dos dispositivos se entregan formando una sola unidad, CSU/DSU.

Podríamos decir que una CSU/DSU es un módem muy potente y caro. Se requiere un dispositivo como este para cada extremo de una conexión T-1 o T-3; las unidades que están en los dos extremos deben ser del mismo fabricante.

Adaptadores de terminal RDSI

RDSI proporciona una conexión digital que le permite comunicarse mediante cualquier combinación de voz, datos y vídeo, entre otras aplicaciones multimedia.

Verifique que las características del adaptador de terminal son las adecuadas para utilizarlo en el servidor iSeries:

- En Recomendaciones sobre adaptadores de terminal RDSI figura una lista que permite determinar el mejor adaptador de terminal que se puede usar.
- En Restricciones de los adaptadores de terminal RDSI hallará información y evaluaciones breves sobre los diversos adaptadores de terminal RDSI que se han probado con el servidor iSeries.

Para configurar el adaptador de terminal, siga estos pasos:

1. En Operations Navigator, seleccione su servidor y expanda **Red –> Servicios de acceso remoto**.
2. Pulse **Módems** con el botón derecho del ratón y seleccione **Módem nuevo**.

3. En el recuadro de diálogo Propiedades de módem nuevo, entre los valores correctos en todos los campos de la pestaña General. Para el dispositivo de comunicaciones, debe especificar que es un adaptador de terminal RDSI.
4. Seleccione la pestaña **Parámetros de RDSI**.
5. En la pestaña **Parámetros de RDSI**, añada o cambie propiedades de RDSI para que coincidan con las propiedades que necesita el adaptador de terminal.

En el ejemplo Configurar un adaptador de terminal RDSI hallará procedimientos de ejemplo que utilizan Operations Navigator.

Recomendaciones sobre adaptadores de terminal RDSI

El adaptador de terminal RDSI externo recomendado es el módem **3Com/U.S. Robotics Courier I RDSI V.35**. Soporta conexiones de módem analógico V.34, V.90 (X2) y PPP multienlace a través de RDSI, en las modalidades de origen y respuesta en el servidor iSeries. También soporta automáticamente el protocolo de autenticación de reconocimiento de identificación (CHAP) a través de la conexión PPP de RDSI.

- **Conexiones con origen en el servidor iSeries.** Las peticiones de identificación de CHAP con origen en el lado receptor las responde el adaptador de terminal Courier I mientras negocia la autenticación del protocolo PAP (protocolo de autenticación de contraseñas) con el servidor iSeries. Las respuestas de PAP no aparecen en la conexión RDSI.
- **Conexiones a las que responde el servidor iSeries.** El adaptador de terminal Courier I exige la autenticación CHAP por parte del lado llamante si la configuración de respuesta del servidor iSeries hace que este abra la autenticación con una petición de identificación CHAP. Si el servidor iSeries abre la autenticación con PAP, el adaptador de terminal Courier I autentica con PAP.

Si está utilizando un módem Courier I anterior a 1999, para obtener el mejor rendimiento de la conexión RDSI, verifique que el módem Courier I está conectado al servidor iSeries mediante un cable V.35. Con el módem Courier I se entrega un cable de módem de RS-232 a V.35; sin embargo, las versiones más antiguas de este cable tenían una clase de conector V.35 incorrecta. Póngase en contacto con la oficina de atención al cliente de 3Com/US Robotics para obtener un recambio.

Nota: Según 3Com/US Robotics, la versión V.35 de este adaptador de terminal ha dejado de estar disponible, aunque tal vez pueda encontrar algunas en suministradores de terceros. La versión RS-232 aún está recomendada en el servidor iSeries, a expensas de una ligera reducción del rendimiento, ya que las conexiones de RS-232 están limitadas a 115,2 Kb.

Black Box Corporation también ofrece adaptadores de V.35 a RS-232. El número de pieza es FA-058.

Asegúrese de establecer en el servidor iSeries que la velocidad de línea de V.35 es 230,4 Kbps.

Restricciones de los adaptadores de terminal RDSI

A continuación figuran los adaptadores de terminal que se han evaluado. Estos adaptadores solo están recomendados para las conexiones RDSI remotas con origen en el servidor iSeries.

3Com Impact IQ RDSI:

Este adaptador de terminal no está recomendado para el servidor iSeries por las siguientes razones:

- El adaptador de terminal no da soporte a las conexiones de módem analógico V.34. Sin embargo, puede dar soporte a las conexiones de módem analógico V.34 si se emplea la conexión externa RJ-11.
- Actualmente el adaptador de terminal no da soporte a las conexiones V.90.
- El adaptador de terminal no puede conectarse al servidor iSeries a velocidades superiores a los 115.200 bps.

- El adaptador de terminal no da automáticamente soporte al protocolo de autenticación de reconocimiento de identificación (CHAP). Sin embargo, si se establece el valor S84=0 sí que se puede realizar la autenticación CHAP en el servidor iSeries.
- El servidor iSeries no puede determinar en qué momento termina la conexión cuando se supervisa la señal de equipo de datos preparado (DSR) del adaptador de terminal. Esto supone exponer el sistema a un riesgo de seguridad.

Motorola BitSurfr Pro RDSI:

Este adaptador de terminal no está recomendado para el servidor iSeries por las siguientes razones:

- El adaptador de terminal no da soporte a las conexiones de módem analógico V.34. Sin embargo, puede dar soporte a las conexiones de módem analógico V.34 si se emplea la conexión externa RJ-11.
- Actualmente el adaptador de terminal no da soporte a las conexiones V.90.
- El adaptador de terminal no puede conectarse al servidor iSeries a velocidades superiores a los 115.200 bps.
- El adaptador de terminal no da automáticamente soporte a la autenticación CHAP. Sin embargo, si se establece el valor @M2=C sí que se puede realizar la autenticación CHAP en el servidor iSeries.
- El adaptador de terminal no permite responder automáticamente a las llamadas PPP de un solo enlace ni a las llamadas PPP multienlace. El adaptador de terminal remoto de origen debe estar configurado con el mismo protocolo (un solo enlace o multienlace) que el adaptador de terminal que responde.
- El mecanismo de control de flujo por hardware del servidor iSeries no funciona bien con este adaptador de terminal. Se produciría una reducción del rendimiento cuando el servidor iSeries enviase datos a través de una conexión PPP multienlace.

Consideraciones sobre el ancho de banda - Multienlace

Puede ocurrir que en algunas ocasiones, pero no en todas, se necesite más ancho de banda para completar algunas tareas. En tales casos, puede no estar justificada la adquisición de hardware especializado y de líneas de comunicaciones de precio elevado. El protocolo multienlace (MP) PPP permite agrupar múltiples enlaces PPP para formar un solo enlace virtual o ″paquete compuesto″. El resultado de agrupar múltiples enlaces aumenta el ancho de banda efectivo total entre dos sistemas si se utilizan módems y líneas telefónicas estándar. Un factor que limita el número máximo de enlaces permitidos en un paquete compuesto MP es el número de módems y líneas telefónicas que están disponibles en los dos extremos del enlace PPP. Para establecer una conexión multienlace, los dos extremos del enlace PPP han de dar soporte al protocolo multienlace. El protocolo multienlace viene documentado como petición de comentarios estándar RFC 1990. Podrá hallar más información sobre las RFC en http://www.rfc-editor.org.

Ancho de banda a petición:

La capacidad de añadir y quitar enlaces físicos de manera dinámica permite configurar un sistema para que suministre ancho de banda en la medida de lo necesario. Este enfoque, al que se suele llamar ″ancho de banda a petición″, permite que solo se pague el ancho de banda adicional que realmente se utilice. Para beneficiarse de las ventajas del ″ancho de banda a petición″, debe haber al menos un similar con capacidad para supervisar la utilización del ancho de banda total disponible actualmente en un paquete compuesto MP. Luego, cuando la utilización del ancho de banda supere los valores definidos en la configuración, se podrán añadir o quitar enlaces en el paquete compuesto. El protocolo de asignación de ancho de banda (BAP) permite a los similares negociar las acciones de añadir o quitar enlaces en un paquete compuesto MP. En la RFC 2125 hallará documentación relacionada con el protocolo de asignación de ancho de banda (BAP) y con el protocolo de control de asignación de ancho de banda (BACP) de PPP.

Soporte L2TP (túneles) para conexiones PPP

El protocolo L2TP (Layer 2 Tunneling Protocol) es un protocolo de túneles que amplía el protocolo punto a punto (PPP) para que dé soporte a un túnel en la capa de enlace entre un cliente L2TP solicitante (concentrador de acceso L2TP o LAC) y, como punto final, un servidor L2TP destino (servidor de red L2TP o LNS). Con los túneles L2TP, es posible separar la ubicación en la que finaliza el protocolo de acceso telefónico y la ubicación en la que se proporciona el acceso a la red; esta es la razón por la que al protocolo L2TP también se le llama PPP virtual. El protocolo L2TP viene documentado como petición de comentarios estándar RFC 2661. Hallará más información sobre las RFC en http://www.rfc-editor.org. El túnel L2TP se puede ampliar para que abarque toda una sesión PPP o solo uno de los dos segmentos de que consta una sesión. Ello da lugar a cuatros modelos de túneles:

- Túnel voluntario
- Túnel forzoso - llamada entrante
- Túnel forzoso - marcación remota
- Conexión multisalto L2TP

Túnel voluntario

En el modelo de túnel voluntario, el usuario es el que crea un túnel y lo suele hacer con un cliente habilitado para L2TP. Como resultado, el usuario enviará paquetes L2TP al proveedor de servicios de Internet (ISP), que los reenviará al LNS. En los túneles voluntarios, el ISP no necesita dar soporte a L2TP, y el iniciador del túnel L2TP reside realmente en el mismo sistema que el cliente remoto. En este modelo, el túnel atraviesa toda la sesión PPP, desde el cliente L2TP al LNS.

Modelo de túnel forzoso - llamada entrante

En el modelo de túnel forzoso para llamadas entrantes, se crea un túnel sin ninguna acción por parte del usuario y sin que el usuario pueda escoger. Como resultado, el usuario enviará paquetes PPP al ISP (LAC), que los encapsulará en L2TP y los hará pasar por el túnel hasta el LNS. En los casos de túneles forzosos, el ISP debe tener capacidad para L2TP. En este modelo, el túnel solo atraviesa el segmento de la sesión PPP que hay entre el ISP y el LNS.

Modelo de túnel forzoso - marcación remota

En el modelo de túnel forzoso para marcación remota, la pasarela local (LNS) inicia un túnel hasta un ISP (LAC) e indica al ISP que haga una llamada local para el cliente de respuesta PPP. Este modelo está pensado para los casos en que el cliente de respuesta PPP remoto tiene establecido un número de teléfono permanente con un ISP. Este modelo es especialmente indicado cuando una empresa que tiene una presencia establecida en Internet necesita establecer una conexión con una oficina remota que requiere un enlace de acceso telefónico. En este modelo, el túnel solo atraviesa el segmento de la sesión PPP que hay entre el LNS y el ISP.

Conexión multisalto L2TP

La conexión multisalto L2TP es una manera de redirigir el tráfico L2TP en nombre de los LAC cliente y los LNS. Las conexiones multisalto se establecen con una pasarela multisalto L2TP (sistema que enlaza entre sí los perfiles de iniciador y terminador L2TP). Para establecer una conexión multisalto, la pasarela multisalto L2TP funcionará como LNS para un conjunto de concentradores de acceso L2TP (LAC) y a la vez como LAC para un LNS dado. Se establece un túnel desde un LAC cliente a la pasarela multisalto L2TP y luego se establece otro túnel entre la pasarela multisalto L2TP y un LNS destino. Después, la pasarela multisalto L2TP redirige el tráfico L2TP del LAC cliente al LNS destino, y el tráfico del LNS destino se redirige al LAC cliente.

Soporte de políticas de grupo

El soporte de políticas de grupo permite a los administradores de la red definir políticas de grupo basadas en usuarios como ayuda para gestionar los recursos, y permite asimismo asignar políticas de control de acceso a los usuarios individuales cuando se conectan a la red con una sesión PPP o L2TP. Lo que se pretende es identificar a los usuarios por su pertenencia a una determinada clase de usuario, donde cada clase tendría su propia política exclusiva. Cada una de las políticas de grupo exclusivas permite definir límites de recursos, como el número de enlaces permitidos en un paquete compuesto multienlace, atributos como el reenvío de IP y la identificación del conjunto de reglas de filtrado de paquetes IP que deberían aplicarse. Con el soporte de políticas de grupo, los administradores de la red podrían definir, por ejemplo, un grupo de Trabajo_en_casa que permitiría a los usuarios de esta clase acceder sin restricciones a la red, mientras que los usuarios de otro grupo formado por Trabajadores_de_proveedor tendrían un acceso que estuviera restringido a un conjunto de servicios más limitado.

Filtrado de paquetes IP

El filtrado de paquetes IP es el mecanismo que puede limitar los servicios disponibles para un usuario individual cuando haya iniciado la sesión en una red. El filtrado de paquetes puede ″permitir″ o ″denegar″ el acceso en función de las direcciones IP y/o puertos destino. Se pueden poner en vigor distintas políticas al definir múltiples conjuntos de reglas de filtrado de paquetes, teniendo cada uno de ellos su propio identificador de filtro PPP exclusivo. Las reglas de filtrado de paquetes se pueden asignar para un determinado perfil de conexión de receptor o bien se pueden asignar mediante una política de grupo que aplicaría las reglas a esa categoría de usuario. Las reglas de filtrado de paquetes propiamente dichas no se definen en PPP, sino que se definen bajo Políticas, en Operations Navigator.

Capítulo 5. Configurar PPP

Para poder utilizar PPP con el fin de configurar una conexión punto a punto, primero tendrá que configurar el entorno PPP. En estos apartados hallará información de configuración para los entornos PPP:

- Crear un perfil de conexión
- Configurar el módem
- Configurar un PC remoto
- Configurar el acceso a Internet por medio de AT&T Global Network
- Asistentes de conexión
- Configurar una política de acceso de grupo
- Aplicar reglas de filtrado de paquetes IP a una conexión PPP
- Habilitar servicios de RADIUS y DHCP para perfiles de conexión de receptor PPP

Crear un perfil de conexión

El primer paso para configurar una conexión PPP entre sistemas consiste en crear un perfil de conexión en el servidor iSeries. El perfil de conexión es la representación lógica de los siguientes detalles de la conexión:

- Tipo de línea y de perfil
- Valores de multienlace
- Números de teléfono remotos
- Autenticación
- Valores de TCP/IP: direcciones IP y direccionamiento
- Gestión de trabajos y personalización de la conexión
- Servidores de nombres de dominio

En **Servicios de acceso remoto**, bajo el directorio Red, se incluyen los siguientes objetos:

- **Perfiles de conexión de originador**, que son conexiones punto a punto salientes que se originan en el servidor iSeries (sistema local). Son las conexiones PPP que recibe un sistema remoto.
- **Perfiles de conexión de receptor**, que son conexiones punto a punto entrantes que se originan en un sistema remoto. Son las conexiones PPP que recibe el servidor iSeries (sistema local).
- **Módems**

Para crear un perfil de conexión, siga estos pasos:

1. En Operations Navigator, seleccione su sistema y expanda **Red –> Servicios de acceso remoto**.
2. Seleccione una de estas opciones:
   - Pulse **Perfiles de conexión de originador** con el botón derecho del ratón para establecer el servidor iSeries como servidor que accede telefónicamente para obtener conexiones.
   - Pulse **Perfiles de conexión de receptor** con el botón derecho del ratón para establecer el servidor iSeries como servidor que permite las conexiones entrantes de los sistemas y usuarios remotos.
3. Seleccione **Perfil nuevo**.
4. En la página **Configuración de perfil de conexión punto a punto nuevo**, seleccione el tipo de protocolo.
5. Especifique las selecciones de modalidad.
6. Seleccione la configuración de enlace.
7. Pulse **Aceptar**.

Aparece la página **Propiedades de perfil punto a punto nuevo**. Puede establecer los demás valores que sean específicos de su red. Hallará información concreta en la ayuda en línea.

Tipo de protocolo: PPP o SLIP

¿Qué tipo de protocolo deberá elegir para establecer una conexión punto a punto?

PPP es una conexión estándar de Internet. Permite la interoperatividad entre el software de acceso remoto de distintos fabricantes. También permite que múltiples protocolos de comunicaciones de red utilicen una misma línea de comunicaciones física.

PPP sustituye a SLIP como protocolo que conviene elegir para las conexiones punto a punto. La petición de comentarios (RFC) de SLIP nunca llegó a ser un estándar de Internet debido a las siguientes deficiencias:

- SLIP no tiene ningún procedimiento estándar para definir el sistema de direcciones IP entre los dos sistemas principales. Ello implica que no se puede emplear una red no numerada.
- SLIP no tiene soporte para la detección de errores ni para la compresión de errores. La detección o la compresión de errores se implementan en PPP.
- SLIP no tiene soporte para la autenticación del sistema, mientras que PPP tiene autenticación en los dos sentidos.

El protocolo SLIP se sigue usando hoy en día y aún está soportado en el servidor iSeries. Sin embargo, IBM le recomienda que utilice PPP cuando configure la conectividad punto a punto. SLIP no proporciona ningún soporte para las conexiones multienlace. En comparación con SLIP, es mejor la autenticación de PPP. El rendimiento de PPP es mayor debido a los recursos de compresión.

Nota: Los perfiles de conexión SLIP definidos con los tipos de línea ASYNC han dejado de estar soportados en este release. Si dispone de estos perfiles de conexión, tendrá que migrarlos a un perfil SLIP o a un perfil PPP que emplee un tipo de línea PPP.

Selecciones de modalidad

Las selecciones de modalidad para un perfil de conexión PPP consisten en seleccionar el **tipo de conexión** y la **modalidad de operación**. Las selecciones de modalidad especifican cómo emplea el servidor la nueva conexión PPP.

Para especificar las selecciones de modalidad, siga estos pasos:

1. Seleccione uno de estos tipos de conexión:
   - Línea conmutada
   - Línea alquilada
   - L2TP (línea virtual)
2. Seleccione la modalidad de operación apropiada para la nueva conexión PPP.
3. Anote el tipo de conexión y la modalidad de operación que ha seleccionado. Necesitará esta información cuando empiece a configurar las conexiones PPP.

Línea conmutada

Seleccione este tipo de conexión si va a utilizar uno de los siguientes dispositivos para conectarse a través de una línea telefónica:

- Módem (interno o externo)
- Adaptador interno de interfaz de velocidad básica (BRI) RDSI
- Adaptador externo de terminal RDSI

El tipo de conexión por línea conmutada tiene las siguientes modalidades de operación:

- **Respuesta**

Elija este tipo de modalidad de operación si desea permitir que un sistema remoto pueda acceder telefónicamente al servidor iSeries.

- **Marcación**

  Elija esta modalidad de operación si desea permitir que el servidor iSeries pueda acceder telefónicamente a un sistema remoto.

- **Marcación a petición (solo marcar)**

  Elija esta modalidad de operación si desea permitir que el servidor iSeries pueda acceder telefónicamente de forma automática a un sistema remoto al detectarse tráfico TCP/IP en el sistema. La conexión finaliza cuando se completa la transmisión de los datos y no se produce ningún tráfico TCP/IP durante un tiempo dado.

- **Marcación a petición (similar dedicado habilitado para respuesta)**

  Elija esta modalidad de operación si desea permitir que el servidor iSeries pueda responder a las llamadas de un sistema remoto dedicado. Esta modalidad de operación también permitirá que el servidor iSeries llame al sistema remoto cuando se detecte tráfico TCP/IP para el sistema remoto. Si los dos sistemas son servidores iSeries y los dos utilizan esta modalidad de operación, el tráfico TCP/IP circulará a petición entre los dos sistemas sin que sea necesaria una conexión física permanente. Para esta modalidad de operación se necesita un recurso dedicado. Para que la modalidad de operación funcione correctamente, el similar remoto debe acceder telefónicamente.

- **Marcación a petición (similar remoto habilitado)**

  Elija esta modalidad de operación si desea permitir que se pueda acceder telefónicamente a un sistema remoto o responder a sus llamadas. Para manejar las llamadas entrantes, tendrá que hacer referencia a un perfil de respuesta existente en un perfil de conexión PPP que especifique esta modalidad de operación. Esto habilita un solo perfil de respuesta para que maneje todas las llamadas entrantes procedentes de uno o de varios similares remotos y un perfil de marcación a petición aparte para cada llamada saliente. Para esta modalidad de operación no se necesita un recurso dedicado para manejar las llamadas entrantes procedentes de los similares remotos.

Línea alquilada

Seleccione este tipo de conexión si tiene una línea dedicada entre el servidor iSeries local y el sistema remoto. Si tiene una línea alquilada, no necesita un módem ni un adaptador de terminal RDSI para conectar los dos sistemas.

Se considera que la conexión por línea alquilada entre dos sistemas equivale a una línea permanente o dedicada. La línea siempre está abierta y disponible. Uno de los extremos de la conexión por línea alquilada se configura como iniciador y el otro, como terminador.

El tipo de conexión por línea alquilada tiene las siguientes modalidades de operación:

- **Terminador**

  Elija esta modalidad de operación si desea permitir que un sistema remoto pueda acceder al servidor iSeries a través de una línea dedicada. Esta modalidad de operación hace referencia a un perfil de respuesta de línea alquilada.

- **Iniciador**

  Elija esta modalidad de operación si desea permitir que el servidor iSeries pueda acceder a un sistema remoto a través de una línea dedicada. Esta modalidad de operación hace referencia a un perfil de marcación de línea alquilada.

L2TP (línea virtual)

Seleccione este tipo de conexión para proporcionar una conexión entre sistemas que emplean el protocolo L2TP (Layer Two Tunneling Protocol).

Una vez establecido un túnel L2TP, se hace una conexión PPP virtual entre el servidor iSeries y el sistema remoto. Si se combina la utilización de túneles L2TP con el sistema de seguridad de IP (IP-SEC), se pueden enviar, direccionar y recibir datos de forma segura a través de Internet.

El tipo de conexión por línea virtual (L2TP) tiene las siguientes modalidades de operación:

- **Terminador**

  Elija esta modalidad de operación si desea permitir que un sistema remoto pueda conectarse al servidor iSeries a través de un túnel L2TP.
- **Iniciador**

  Elija esta modalidad de operación si desea permitir que el servidor iSeries pueda conectarse a un sistema remoto a través de un túnel L2TP.
- **Marcación remota**

  Elija esta modalidad de operación si desea permitir que el servidor iSeries pueda conectarse a un ISP a través de un túnel L2TP e indicar al ISP que acceda telefónicamente a un cliente PPP remoto.
- **Iniciador a petición**

  Equivale a la modalidad de iniciador, salvo que el túnel no se establecerá hasta que haya tráfico TCP/IP para el sistema remoto.
- **Marcación remota a petición**

  Equivale a la modalidad de marcación remota, salvo que la llamada al ISP para crear el túnel L2TP no se establecerá hasta que haya tráfico TCP/IP para el sistema remoto.
- **Iniciador multisalto**

  Elija esta modalidad de operación si desea permitir que el servidor iSeries pueda establecer una conexión multisalto.

  Nota: El perfil de terminador L2TP al que está asociado este iniciador multisalto debe tener marcado el recuadro ″Permitir conexión multisalto″ y también debe tener una entrada de lista de validación PPP que enlace el nombre de usuario de PPP con el perfil de iniciador multisalto.

Protocolo L2TP (Layer 2 Tunneling Protocol): El protocolo L2TP amplía el protocolo punto a punto (PPP) para que dé soporte a un túnel en la capa de enlace entre un cliente L2TP solicitante y, como punto final, el servidor L2TP destino. Al utilizar túneles L2TP, es posible separar la ubicación en la que finaliza el protocolo de acceso telefónico de la ubicación en la que se proporciona acceso a la red.

Los proveedores de servicios de Internet (ISP) utilizan la modalidad de línea virtual para trabajar con redes privadas virtuales (VPN). Puede obtener más información sobre cómo funciona VPN con L2TP en Configurar una conexión L2TP protegida por VPN.

Estas figuras ilustran tres implementaciones de túneles de L2TP:

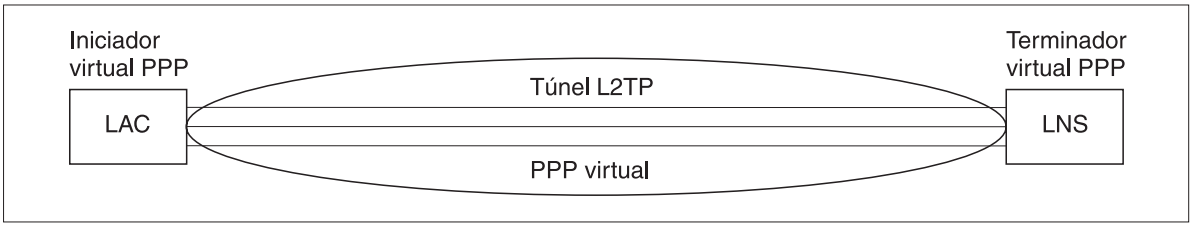


Figura 4. Iniciador virtual PPP o terminador virtual PPP

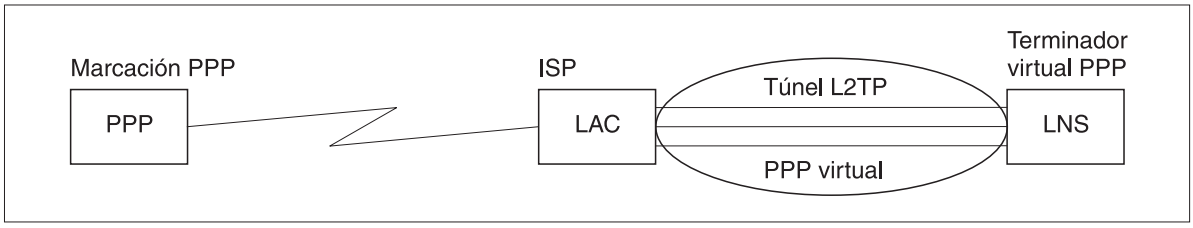


Figura 5. Iniciador de marcación PPP o terminador virtual PPP

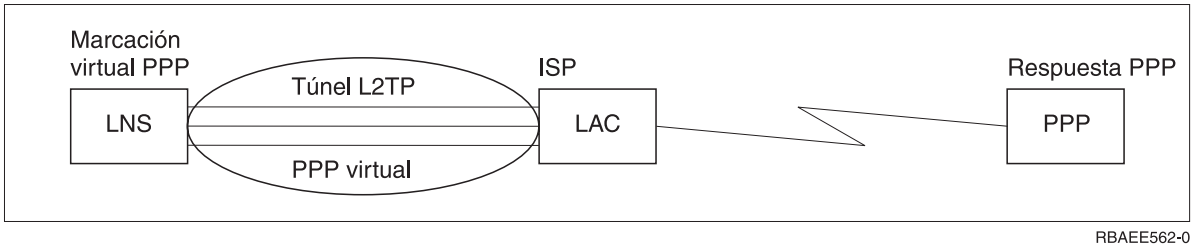


Figura 6. Marcación virtual PPP o respuesta virtual PPP

Configuración de enlace

La configuración de enlace define el tipo de servicio de línea que el perfil de conexión PPP utiliza para establecer una conexión. Los tipos de servicio de línea dependen del tipo de conexión que se especifique.

- Una sola línea
- Agrupación de líneas
- Línea RDSI integrada

Una sola línea

Seleccione este servicio de línea para definir una línea PPP asociada a un módem analógico. Esta opción también se utiliza para líneas alquiladas en las que no se necesita un módem. El perfil de conexión PPP siempre emplea el mismo recurso de puerto de comunicaciones del servidor iSeries.

El servicio de una sola línea también se emplea para los tipos de conexión L2TP (línea virtual). En el caso de los tipos de conexión L2TP (línea virtual), no hay ningún recurso de puerto de comunicaciones de hardware que se utilice con la línea única. Por el contrario, la línea única que se emplea con una conexión L2TP se considera *virtual* en el sentido de que no se necesita ninguna pieza física de hardware PPP para establecer el túnel.

Agrupación de líneas

Seleccione este servicio de línea para establecer que la conexión PPP utilice una línea de una agrupación de líneas. Al empezar la conexión PPP, el servidor iSeries selecciona en la agrupación de líneas una línea que no se esté utilizando. En el caso de los perfiles de marcación a petición, el servidor no elige la línea hasta que detecta tráfico TCP/IP para el sistema remoto.

En lugar de definir una descripción de línea para cada perfil de conexión, puede utilizar una agrupación de líneas. Es posible especificar una o varias descripciones de línea de una agrupación de líneas.

Una agrupación de líneas también permite que un solo perfil de conexión pueda manejar múltiples llamadas analógicas entrantes o una sola llamada analógica saliente. La línea regresa a la agrupación de líneas al finalizar la conexión PPP.

Si utiliza la agrupación de líneas para manejar simultáneamente múltiples llamadas analógicas entrantes, tendrá que indicar el número máximo de conexiones entrantes. Este número se puede establecer en la pestaña Conexiones del diálogo **Propiedades de perfil punto a punto nuevo** en el momento de configurar el perfil de conexión. Utilice el valor multienlace para usar agrupaciones de líneas de múltiples conexiones.

Ventajas de utilizar las agrupaciones de líneas:

- No tendrá que comprometer un recurso de línea en una conexión PPP hasta que esta se inicie.

  En el caso de las conexiones PPP que emplean una línea específica, la conexión finaliza si la línea no está disponible. En el caso de las conexiones que emplean una agrupación de líneas, solo es necesario que esté disponible una línea de la agrupación de líneas al iniciarse el perfil.
- Podrá utilizar perfiles de marcación a petición con agrupaciones de líneas para que el uso de los recursos resulte más eficaz.

  El servidor iSeries solo selecciona una línea de la agrupación de líneas cuando se utiliza una conexión de marcación a petición. Las otras conexiones pueden utilizar la misma línea en otras ocasiones.
- Podrá iniciar más conexiones PPP con menos recursos que les den soporte.

  Por ejemplo, si el entorno necesita cuatro tipos de conexión exclusivas, pero usted solo necesita dos líneas en todo momento, puede emplear una agrupación de líneas para hacer que funcione ese entorno. Puede crear cuatro perfiles de conexión de marcación a petición y hacer que cada uno de ellos haga referencia a una agrupación de líneas que contenga dos descripciones de línea. Cada una de las líneas estaría disponible para los cuatro perfiles de conexión, permitiendo así que hubiera dos conexiones activas en todo momento. Al utilizar una agrupación de líneas, no haría falta que tuviera cuatro líneas independientes.

Soporte de perfiles de múltiples conexiones

Los perfiles de conexión punto a punto que dan soporte a múltiples conexiones le permiten tener un solo perfil de conexión para manejar numerosas llamadas digitales, analógicas o L2TP. Esto le será de utilidad si desea que múltiples usuarios se conecten al servidor iSeries, pero no quiere especificar un perfil de conexión punto a punto aparte para manejar cada una de las líneas PPP. Esta característica es especialmente útil para el módem integrado 2761 de 8 puertos, en el que hay ocho líneas disponibles para utilizarse desde un solo adaptador, o para los adaptadores 2750 y 2751, que dan soporte a ocho conexiones de canal B RDSI independientes.

En el caso de las líneas analógicas con soporte para perfiles de múltiples conexiones, se utilizan todas las líneas de la agrupación de líneas especificada, hasta llegar al número máximo de conexiones. Básicamente, se inicia un trabajo de perfil de conexión aparte para cada línea definida en la agrupación de líneas. Todos los trabajos de perfil de conexión esperan llamadas entrantes a través de sus líneas respectivas.

Dirección IP local para perfiles de múltiples conexiones:

La dirección IP local se puede utilizar con los perfiles de múltiples conexiones, pero debe ser una dirección IP existente que esté definida en el servidor iSeries. Para seleccionar la dirección existente, podrá emplear la lista desplegable de direcciones IP locales. Los usuarios remotos pueden acceder a los recursos de la red local si usted elige la dirección IP local del servidor iSeries como dirección IP local para su perfil PPP. Además, deberá definir las direcciones IP que están en la agrupación de direcciones IP remotas para que estén en la misma red que la dirección IP local.

Si no tiene una dirección IP local del servidor iSeries o si no quiere que los usuarios remotos accedan a la LAN, deberá definir una dirección IP virtual para el servidor iSeries. A las direcciones IP virtuales también se las conoce como interfaces sin circuito. Los perfiles punto a punto pueden utilizar esta dirección IP como dirección IP local. Esta dirección, puesto que no está ligada a una red física, no reenviará automáticamente el tráfico a otras redes conectadas al servidor iSeries.

Para crear una dirección IP virtual, siga estos pasos:

1. En Operations Navigator, expanda su servidor y acceda a **Red –> Protocolos**.
2. Pulse TCP/IP con el botón derecho del ratón y seleccione Interfaz nueva—>IP virtual.
3. Siga las instrucciones facilitadas por el asistente de interfaz para crear la interfaz IP virtual. Los perfiles de conexión punto a punto podrán utilizar la dirección IP virtual nada más crearla. Para utilizar la dirección con el perfil, puede emplear la lista desplegable del campo Dirección IP local que aparece en la página Valores de TCP/IP.

   Nota: La dirección IP virtual debe estar activa antes de que inicie el perfil de múltiples conexiones; de lo contrario, el perfil no se iniciaría. Para activar la dirección después de crear la interfaz, seleccione la opción de iniciar la dirección cuando utilice el asistente de la interfaz. Además, debe establecer que el reenvío de IP es **No** para asegurarse de que la dirección no reenvía el tráfico a otras redes conectadas al servidor iSeries.

Agrupaciones de direcciones IP remotas para perfiles de múltiples conexiones:

También podrá utilizarse agrupaciones de direcciones IP remotas con perfiles de múltiples conexiones. Un perfil punto a punto de una sola conexión típico permite especificar solamente una dirección IP que se asigna al sistema llamante cuando se establece la conexión. Puesto que ahora pueden conectarse simultáneamente múltiples llamadores, se utiliza una agrupación de direcciones IP remotas para definir una dirección IP remota inicial, así como un rango de direcciones IP adicionales que se asignarán al sistema llamante.

Restricciones de las agrupaciones de líneas:

Cuando se utilizan agrupaciones de líneas para múltiples conexiones, se aplican las restricciones siguientes:

- Una línea concreta no puede existir a la vez en más de una agrupación de líneas. Si elimina una línea de una agrupación de líneas, la línea se podrá utilizar en otra agrupación de líneas.
- Al iniciar un perfil de múltiples conexiones que utiliza una agrupación de líneas, se utilizarán todas las líneas de la agrupación hasta alcanzar el valor del número máximo de conexiones del perfil. Cuando ya no haya líneas disponibles, no podrán establecerse nuevas conexiones. Además, si no hay líneas disponibles en la agrupación de líneas y se inicia otro perfil, este finalizará.
- Si inicia un perfil de una sola conexión que tiene una agrupación de líneas, el sistema utiliza solamente una línea de la agrupación. Si inicia un perfil de múltiples conexiones que utiliza la misma agrupación de líneas, las otras líneas de la agrupación estarán disponibles para utilizarse.

Agrupaciones de direcciones IP remotas: El sistema puede utilizar agrupaciones de direcciones IP remotas para un perfil de conexión punto a punto de respuesta o de terminación que se utilice con múltiples conexiones entrantes. Esto incluye L2TP, RDSI nativa y las agrupaciones de líneas cuyo número máximo de conexiones sea mayor que uno. Esta función permite al sistema asignar una dirección IP remota exclusiva a cada conexión entrante.

El primer sistema que se conecte recibirá la dirección IP definida en el campo Dirección IP inicial. Si esta dirección ya se está utilizando, se asignará la próxima dirección IP disponible dentro del rango del número de direcciones. Por ejemplo, supongamos que la dirección IP inicial es 10.1.1.1 y que el número de direcciones es 5. Las direcciones disponibles en la agrupación de direcciones IP remotas serán 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4 y 10.1.1.5. La máscara de subred definida para las direcciones de la agrupación de direcciones IP remotas será siempre 255.255.255.255.

Cuando se utilizan agrupaciones de direcciones IP remotas se aplican las restricciones siguientes:

- Puede haber más de un perfil de conexión que especifique una misma agrupación de direcciones. Sin embargo, una vez que se hayan utilizado todas las direcciones de la agrupación, se rechazarán las subsiguientes peticiones de conexión hasta que otra conexión finalice y libere una dirección.

- Para asignar direcciones concretas a determinados sistemas remotos al tiempo que se permite que otros sistemas entrantes utilicen una dirección de la agrupación, siga estos pasos:
  1. Habilite la autenticación de sistema remoto en la pestaña **Autenticación** para poder averiguar el nombre de usuario del sistema remoto.
  2. Defina una agrupación de direcciones IP remotas para todas las peticiones de conexión entrantes que no exijan una dirección IP concreta.
  3. Defina direcciones IP remotas para los usuarios concretos marcando el recuadro **Definir direcciones IP adicionales basadas en el ID de usuario del sistema remoto** y pulsando a continuación **Direcciones IP definidas por nombre de usuario**.

  Cuando el usuario remoto se conecta, el servidor iSeries determina si se ha definido una dirección IP específica para ese usuario. Si es así, al sistema remoto se le asignará esa dirección IP; en caso contrario, se le asignará una dirección de la agrupación de direcciones IP remotas.

RDSI
Seleccione este servicio de línea para definir una línea PPP asociada a una conexión de red RDSI.

Ventajas de utilizar RDSI:
- RDSI proporciona una comunicación clara a mayor velocidad.
- RDSI pretende ofrecer una conectividad universal utilizando una sola interfaz y una red digital de alta velocidad para transportar todo tipo de datos.
- RDSI tiene asimismo la posibilidad de establecer conexiones conmutadas en menos tiempo. Se puede tardar hasta 30 segundos o más en establecer conexión con un módem analógico, mientras que con RDSI solo se necesitan unos pocos segundos.

Configurar el módem para PPP

Para las conexiones PPP analógicas, puede utilizar un módem externo, un módem interno 2761 o un adaptador de terminal RDSI. Los módems permiten realizar conexiones analógicas (líneas alquiladas y conmutadas). En el servidor iSeries se han definido descripciones para la mayoría de los módems más conocidos.

Puede llevar a cabo estas tareas de configuración de módem:
- Configurar un módem nuevo
- Asociar un módem a una descripción de línea
- Establecer series para los mandatos del módem

Configurar un módem nuevo
1. En Operations Navigator, seleccione su servidor y expanda **Red –> Servicios de acceso remoto**.
2. Pulse **Módems** con el botón derecho del ratón y seleccione **Módem nuevo**.
3. En la pestaña General, entre los valores correctos en todos los campos.
4. **Opcional:** pulse la pestaña Parámetros adicionales para añadir los mandatos de inicialización que necesite para el módem.
5. Pulse **Aceptar** para guardar los valores que ha entrado y cerrar la página de propiedades del nuevo módem.

Para determinar si puede utilizar la descripción de un módem existente, siga estos pasos:
1. En Operations Navigator, seleccione su servidor y expanda **Red –> Servicios de acceso remoto**.
2. Seleccione **Módems**.
3. En la lista de módems, localice el nombre del fabricante, el modelo y la marca del módem.

   Nota: Si el módem figura en la lista por omisión, no es necesario que haga nada más.

4. Pulse con el botón derecho del ratón la descripción del módem que más se parezca al suyo y seleccione **Propiedades** para revisar las series de los mandatos.
5. Consulte la documentación del módem para determinar las series de los mandatos específicos del módem.

   Utilice las propiedades por omisión del módem si las series de los mandatos coinciden con los requisitos de su módem. En caso contrario, tendrá que crear una descripción para su módem y añadirla a la lista de módems.

Para crear una descripción de módem, siga estos pasos:

1. En Operations Navigator, seleccione su servidor y expanda **Red –> Servicios de acceso remoto**.
2. Seleccione **Módems**.
3. En la lista de módems, pulse **$generic hayes** con el botón derecho del ratón y seleccione **Módem nuevo basado en**.
4. En el diálogo **Módem nuevo**, cambie las series de los mandatos para que coincidan con la información necesaria para su módem.

Establecer series para los mandatos del módem

La tabla siguiente muestra el juego mínimo de series de mandatos que utilizan la mayoría de los módems definidos en el servidor iSeries. En el manual del usuario del módem podrá hallar la serie de mandato equivalente. Utilice el valor recomendado por el fabricante en la descripción del módem.

Propiedad del módem	**Serie de mandato correcta para la mayoría de los módems**
Restablecimiento del módem en los valores por omisión de fábrica	AT&F o AT&Z
Inicialización del módem:	
Mostrar códigos de resultado verbales	Q0 y V1
Modalidades CD y DTR normales	&C1 y &D2
Modalidad de eco desconectado	E0
Equipo de datos preparado (DSR) después de detectar la portadora	&S1
Habilitar el control de flujo por hardware (RTS/CTS)	
Habilitar la corrección de errores y, opcionalmente, la compresión (V.42/V.42 bis)	
Asegurarse de que la velocidad de línea DTE-DCE está fijada en 115,2 Kbps (o en la velocidad máxima que permite el módem)	
(Opcional) Habilitar el tiempo de inactividad, si el módem soporta esta función	
Modalidad de respuesta del módem:	
Responder después de *n* señales de llamada	S0=*n* donde n = 1 ó 2
Desconectar si no se detecta la portadora (conexión) después de *m* segundos	S7=*m*
Tipo de marcación del módem	ATDT realiza la marcación por tonos y ATDP por pulsos

Ejemplo: configurar un adaptador de terminal RDSI

1. En Operations Navigator, seleccione su servidor y expanda **Red –> Servicios de acceso remoto**.
2. Pulse **Módems** con el botón derecho del ratón y seleccione **Módem nuevo**.
3. En la pestaña General, entre los valores correctos en todos los campos.

4. **Opcional:** pulse la pestaña Parámetros RDSI para añadir los mandatos de inicialización que necesite para el módem.

   En el caso de los adaptadores de terminal RDSI, los mandatos y parámetros de esta lista solo se envían al adaptador de terminal cuando se dan estas situaciones:

   - Al añadir mandatos o parámetros a la lista o al modificarlos
   - Como resultado de ciertas acciones de recuperación que puede realizar el servidor iSeries en caso de errores

   En consecuencia, estos mandatos deben permitir y limitarse a:

   - Establecer el tipo y la versión del conmutador RDSI proporcionado por la compañía telefónica local
   - Establecer los números de directorio y los identificadores de perfil de servicio (SPID) proporcionados por la compañía telefónica local
   - Establecer los ID de entrada de terminal (TEI) que pueda proporcionar la compañía telefónica local
   - Establecer el protocolo del canal B (PPP asíncrono a síncrono)
   - Habilitar la asignación dinámica de ancho de banda para asignar automáticamente el canal de voz a los datos, si está disponible
   - Habilitar las conexiones PPP multienlace
   - Otros valores del módem que tengan parámetros de longitud variable que necesiten un retorno de carro para indicar la longitud del parámetro
   - Guardar y activar los valores nuevos para que se restauren cada vez que se restablezcan o que se apague el sistema
   - El mandato de prueba del estado activo de la interfaz *U* (ATD*x*), que permite al servidor iSeries determinar cuándo se ha logrado la sincronización con el conmutador de la oficina central de RDSI. La *x* puede ser cualquiera de los dígitos permitidos para un número de teléfono, incluidos los caracteres # y *.
5. Pulse **Añadir** para añadir más mandatos del módem. Los mandatos se pueden añadir a la lista de mandatos con o sin un parámetro asociado y una pequeña descripción. A los mandatos que especifique sin un parámetro asociado les podrá asignar uno cuando se asocie el módem a una descripción de línea.
6. Pulse **Aceptar** para guardar los valores que ha entrado y cerrar la página de propiedades del nuevo módem.

Asociar un módem a una descripción de línea

1. En Operations Navigator, seleccione su servidor y expanda **Red –> Servicios de acceso remotos –> Perfiles de conexión de originador** o **Perfiles de conexión de receptor**.
2. Seleccione una de estas opciones:
   - Para trabajar con un perfil de conexión existente, pulse un perfil de conexión con el botón derecho del ratón y seleccione **Propiedades**.
   - Para trabajar con un perfil de conexión nuevo, cree uno nuevo.
3. En la página de propiedades del nuevo perfil punto a punto, seleccione la pestaña **Conexión** y pulse **Nuevo**.
   - Entre un nombre para la configuración de enlace.
   - Pulse **Nuevo** para abrir el recuadro de diálogo Propiedades de línea nueva.
4. En el recuadro de diálogo de propiedades de la línea nueva, pulse la pestaña **Módem** y seleccione el módem en la lista. El módem seleccionado se asociará a esta descripción de línea. En el caso de los módems internos, ya debe estar seleccionada la debida definición de módem. Hallará más información en la ayuda en línea.

Configurar un PC remoto

Para conectarse a un servidor iSeries desde un PC que ejecute un sistema operativo Windows de 32 bits, verifique que el módem está debidamente instalado y configurado, y asegúrese de que ha instalado TCP/IP y el acceso telefónico a redes en el PC.

En la documentación de Microsoft Windows hallará información sobre cómo configurar el acceso telefónico a redes en el PC. Asegúrese de que especifica o entra la siguiente información:

- El tipo de conexión por línea telefónica debe ser **PPP**.
- Si va a emplear contraseñas cifradas, asegúrese de que utiliza MD-5 CHAP (el servidor iSeries NO da soporte a MS-CHAP). Algunas versiones de Windows no dan soporte directo a MD-5 CHAP, pero este protocolo se puede configurar con ayuda adicional de Microsoft.
- Si está empleando contraseñas no cifradas (o no protegidas), se utilizará automáticamente PAP. El servidor iSeries no da soporte a ningún otro tipo de protocolo no protegido.
- En general, el sistema de direcciones IP lo define el sistema remoto o, en este caso, el servidor iSeries. Si piensa utilizar métodos de direcciones IP alternativos (como el de definir sus propias direcciones IP), asegúrese de que el servidor iSeries también está configurado para aceptar su método de direcciones.
- Añada la dirección IP del DNS, si ello es apropiado para su entorno.

Configurar el acceso a Internet por medio de AT&T Global Network

IBM proporciona acceso a Internet mediante AT&T Global Network. Para acceder a este servicio, puede utilizar el asistente de conexión por línea telefónica de AT&T Global Network, que le ayudará a configurar un perfil de conexión PPP por línea telefónica conmutada para acceder telefónicamente a AT&T Global Network. El asistente le solicitará que rellene los datos de unos ocho paneles, lo que le llevará unos diez minutos. Puede cancelar el asistente en cualquier momento y no se guardarán los datos.

Los tipos de aplicaciones que pueden usar la conexión AT&T Global Network son estos dos:

- **Intercambio de correo**: permite recuperar periódicamente los mensajes de correo recibidos en una única cuenta de AT&T Global Network y enviarlos al servidor iSeries para distribuirlos entre los usuarios de Lotus Mail o del protocolo simple de transferencia de correo (SMTP).
- **Acceso telefónico a redes**: permite utilizar otras aplicaciones de acceso telefónico a redes con AT&T Global Network, como el acceso estándar a Internet.

El mantenimiento de los perfiles de conexión de AT&T Global Network es como el de cualquier otro perfil de conexión PPP.

Para utilizar el asistente de conexión por línea telefónica de AT&T Global Network, necesitará uno de estos adaptadores:

- 2699: adaptador de E/S (IOA) de WAN de dos líneas
- 2720: adaptador de E/S PCI de WAN/Twinaxial
- 2721: adaptador de E/S PCI de WAN de dos líneas
- 2745: adaptador de E/S PCI de WAN de dos líneas (sustituye al IOA 2721)
- 2761: adaptador de E/S de módem analógico de ocho puertos
- 2771: adaptador de E/S de WAN de dos puertos, con un módem integrado V.90 en el puerto 1 y una interfaz de comunicaciones estándar en el puerto 2 (para utilizar el puerto 2 del adaptador 2771, se necesita un módem externo o un adaptador de terminal RDSI con el cable apropiado)
- 2772: adaptador de E/S de WAN de dos puertos con módem integrado V.90

Antes de iniciar el asistente de conexión por línea telefónica de AT&T Global Network, tendrá que reunir toda esta información sobre su entorno:

- La información de cuenta de AT&T Global Network (número de cuenta, ID de usuario y contraseña) para la aplicación de intercambio de correo o para la aplicación de acceso telefónico a redes.
- Las direcciones IP del servidor de correo y el servidor de nombres de dominio para la aplicación de intercambio de correo.
- El nombre del módem utilizado para las conexiones de una sola línea.

Para iniciar el asistente de conexión por línea telefónica de AT&T Global Network, siga estos pasos:

1. En Operations Navigator, expanda su servidor y acceda a **Red –> Servicios de acceso remoto**.
2. Pulse **Perfiles de conexión de originador** y seleccione **Nueva conexión por línea telefónica de AT&T Global Network**.
3. Cuando se inicie el asistente de conexión por línea telefónica de AT&T Global Network, pulse **Ayuda** para obtener información sobre cómo rellenar los paneles.

Asistentes de conexión

Asistente de nueva conexión por línea telefónica

Este asistente le orientará paso a paso en el proceso de configurar un perfil de conexión por línea telefónica para acceder al proveedor de servicios de Internet (ISP) o a una intranet.

Para llegar hasta el final del asistente, tal vez tenga que pedir algunos datos informativos al administrador de la red o al proveedor de servicios de Internet (ISP).

En la ayuda en línea hallará más información sobre cómo completar este asistente.

Asistente de conexión universal

La selección de este asistente le orientará paso a paso en el proceso de configurar un perfil que el software de soporte electrónico al cliente puede emplear para conectarse a IBM. El soporte de servicio electrónico proporciona la supervisión del entorno de su sistema servidor iSeries exclusivo con el fin de recomendarle arreglos personalizados en función del sistema y de su situación.

En la ayuda en línea hallará más información sobre cómo completar este asistente.

Configurar una política de acceso de grupo

La carpeta **Políticas de acceso de grupo**, bajo **Perfiles de conexión de receptor**, proporciona opciones para configurar parámetros de conexión punto a punto que se aplican a un grupo de usuarios remotos. Solo es aplicable a aquellas conexiones punto a punto que se originan en un sistema remoto y se reciben en el sistema local.

Para configurar una nueva política de acceso de grupo:

1. En Operations Navigator, seleccione su servidor y expanda **Red –> Servicios de acceso remoto –> Perfiles de conexión de receptor**.
2. Pulse **Políticas de acceso de grupo** con el botón derecho del ratón y seleccione **Nueva política de acceso de grupo**.
3. En la pestaña **General**, entre un nombre y una descripción para la nueva política de acceso de grupo.
4. Pulse la pestaña **Multienlace** y defina la configuración multienlace.

   La configuración multienlace especifica que desea reunir múltiples líneas físicas para formar un paquete compuesto. El número máximo de enlaces por paquete compuesto puede oscilar entre 1 y 16. Puesto que no se conoce el valor del tipo de línea hasta que se establece una conexión, el valor por omisión siempre es 1. La política de grupo puede servir para ampliar o para limitar las posibilidades del protocolo multienlace de un usuario concreto.

- **Máximo de enlaces por paquete compuesto** especifica el número máximo de enlaces (o líneas) que desea reunir para formar una línea lógica. El número máximo de líneas no puede ser mayor que el número de líneas libres que están disponibles cuando se aplica esta política de grupo a una sesión para un perfil PPP.
- Marque **Exigir protocolo de asignación de ancho de banda** si desea especificar que solo se establece una conexión si el sistema remoto da soporte al protocolo de control de asignación de ancho de banda (BACP). Si no se puede negociar el protocolo BACP, se termina la conexión.

5. Pulse la pestaña **Valores de TCP/IP** para habilitar cualquiera de las siguientes posibilidades:
   - Permitir a sistema remoto acceder a otras redes (reenvío de IP)

     Esta opción especifica si desea que se produzca el reenvío de IP. Al seleccionar esta opción, lo que en realidad está haciendo es permitir que el servidor iSeries funcione como direccionador para esta conexión. Con esta opción, los datagramas del protocolo de Internet (IP) no destinados a este servidor iSeries pasan a través de este sistema hasta una red conectada. Si deja esta opción en blanco, el protocolo de Internet (IP) descarta aquellos datagramas del sistema remoto que no estén destinados a una dirección local de este servidor iSeries.

     Tal vez, por razones de seguridad, no le interese permitir el reenvío de IP. En cambio, los proveedores de servicios de Internet (ISP) suelen proporcionar siempre el reenvío de IP. Fíjese que esta opción solo entra en vigor si se habilita el reenvío de datagramas IP a escala del sistema; de lo contrario, esta opción, aunque esté marcada, se pasará por alto. El reenvío de datagramas IP a escala del sistema se puede visualizar en la pestaña Valores de la página Propiedades de TCP/IP.
   - Solicitar compresión de cabecera TCP/IP (VJ)

     Esta opción especifica si desea que el protocolo de Internet (IP) comprima la información de cabecera después de establecer una conexión. En general, la compresión aumenta el rendimiento, especialmente para el tráfico interactivo o para las líneas serie lentas. La compresión de la cabecera se realiza según el método de Van Jacobson (VJ) definido en la RFC 1332. Para PPP, la compresión se negocia en el momento de establecerse la conexión. Si el otro extremo de la conexión no da soporte a la compresión VJ, el servidor iSeries establece una conexión que no utiliza la compresión.
   - Utilizar reglas de paquetes IP para esta conexión

     Esta opción especifica si desea aplicar una regla de filtrado para esta política de grupo. Con las reglas de filtrado, podrá controlar qué tráfico IP va a permitir en la red. Este componente de filtrado de paquetes IP le podrá servir para proteger el sistema. El filtrado de paquetes IP, para proteger el sistema, filtra los paquetes según las reglas que usted especifique. Las reglas se basan en la información de cabecera de los paquetes.

     Hallará más información sobre las reglas de paquetes IP en el tema dedicado al filtrado de paquetes IP y a NAT, en Information Center.

Aplicar una política de grupo a un usuario de acceso remoto:

Puede aplicar una política de grupo a un usuario de acceso remoto cuando haya completado las propiedades punto a punto de un nuevo **Perfil de conexión de receptor**.

Para aplicar una política de grupo a un usuario de acceso remoto:

1. Pulse la página **Autenticación**.
2. Marque **Exigir que este AS/400 verifique la identidad del sistema remoto**.
3. Seleccione **Autenticar localmente utilizando una lista de validación**.
4. Si hay una lista de validación existente, selecciónela en la lista desplegable y pulse **Abrir**. Si la va a crear por primera vez, entre un nombre para la nueva lista de validación y pulse **Nueva**.
5. Pulse **Añadir** para añadir un usuario nuevo a la lista de validación.
6. En el recuadro de diálogo Añadir usuario, siga estos pasos:
   - Seleccione el protocolo de autenticación para el que está definido el nombre del usuario.

- Entre el nombre del usuario y su contraseña.

  Nota: Por razones de seguridad, le recomendamos que no utilice la misma contraseña cuando un usuario está definido para el protocolo de autenticación de reconocimiento de identificación (CHAP), para el protocolo de autenticación extensible (EAP) y para el protocolo de autenticación de contraseñas (PAP).
- Marque la opción **Aplicar una política de grupo al usuario**, seleccione una política de grupo en la lista desplegable y pulse **Abrir**.

  Puede modificar las propiedades de la política de grupo o trabajar con la configuración existente. Pulse **Aceptar** para completar la configuración y regresar a la página de propiedades punto a punto.

Aplicar reglas de filtrado de paquetes IP a una conexión PPP

En Information Center hallará un tema dedicado a las reglas de filtrado de paquetes IP y a las reglas NAT, en el que se explica cómo se crean reglas de paquetes IP a las que se pueda hacer referencia para un perfil de conexión PPP.

Hay dos maneras de hacer referencia a las reglas de filtrado de paquetes IP existentes:

- A nivel de perfil de conexión
  1. Cuando haya completado las **propiedades punto a punto** de un **perfil de conexión de receptor**, seleccione la página Valores de TCP/IP y pulse **Opciones avanzadas**.
  2. Marque **Utilizar reglas de paquetes IP para esta conexión** y seleccione un identificador de filtro PPP en la lista desplegable.
  3. Pulse **Aceptar** para aplicar el filtro PPP al perfil de conexión.
- A nivel de usuario
  1. Abra una política de acceso de grupo existente o cree una nueva política de acceso de grupo.
  2. Pulse la página Valores de TCP/IP.
  3. Marque **Utilizar reglas de paquetes IP para esta conexión** y seleccione un identificador de filtro PPP en la lista desplegable.
  4. Pulse **Aceptar** para aplicar el filtro PPP.

Habilitar servicios de RADIUS y DHCP para perfiles de conexión

Si desea habilitar los servicios de RADIUS y DHCP para los perfiles de conexión de receptor PPP, siga estos pasos:

1. En Operations Navigator, seleccione su servidor y expanda **Red –> Servicios de acceso remoto**.
2. Pulse **Servicios de acceso remoto** con el botón derecho del ratón y seleccione **Servicios**.
3. Para habilitar los servicios DHCP, marque la opción **Habilitar conexión de cliente WAN DHCP con un servidor DHCP o un agente de retransmisión**.
   a. Seleccione la dirección IP del sistema local en la lista desplegable y pulse **Aceptar**.
4. Para habilitar los servicios RADIUS, marque la opción **Habilitar conexión de servidor de acceso a red RADIUS**.
   a. Complete las propiedades NAS de RADIUS. En la ayuda en línea hallará información detallada sobre cómo completar las páginas de propiedades.
5. Pulse **Aceptar** para volver a Operations Navigator.

Capítulo 6. Gestionar PPP

Las tareas de gestión de PPP que puede realizar en el servidor iSeries son las siguientes:

- Establecer las propiedades de los perfiles de conexión PPP
- Supervisar la actividad de PPP

Establecer las propiedades de los perfiles de conexión PPP

Al crear un perfil de conexión, lo normal es que seleccione el protocolo, el tipo de conexión y la modalidad de operación del nuevo perfil de conexión en el recuadro de diálogo Configuración de perfil de conexión punto a punto. Una vez que haya entrado sus selecciones en ese recuadro de diálogo, aparece la hoja de propiedades del perfil de conexión. Las selecciones que especifique en el recuadro de diálogo Configuración de perfil de conexión punto a punto determinan el contenido de la página y el orden de las pestañas de la hoja de propiedades del perfil de conexión. La hoja de propiedades de los perfiles de conexión de originador es distinta de la de los perfiles de conexión de receptor.

Las siguientes directrices le orientarán en el proceso de completar las páginas del recuadro de diálogo **Propiedades de perfil punto a punto nuevo**. Los valores que seleccione en cada página dependerán del entorno y del tipo de conexión que vaya a configurar. La ayuda en línea de Operations Navigator describe todas las opciones que figuran en el recuadro de diálogo. También podrá hallar más información en los ejemplos y procedimientos de PPP.

Página General:

- En esta página se define un nombre y una descripción para el perfil de conexión.

Página Conexión:

- En el caso de los perfiles de marcación o de iniciador, en la página Conexión podrá teclear los números de teléfono de las máquinas remotas a las que se va a conectar.

  Podrá entrar 6 números como máximo y tendrá opciones para indicar lo que se debe hacer cuando se marca satisfactoriamente un número. También hay un nuevo botón avanzado que tiene opciones configurables para los intentos de rellamada.
- Para crear una descripción de línea nueva mientras esté configurando un perfil de conexión PPP, siga las instrucciones que se indican en Configurar una descripción de línea.
- En el caso de los perfiles de respuesta o de terminador, podrá definir el número máximo de conexiones soportadas por una agrupación de líneas.
- Seleccione **Habilitar protocolo multienlace**, si elige utilizar este protocolo, y teclee el número de conexiones soportadas por su sistema.
  - **Para los perfiles de respuesta o de terminador**, si selecciona **Habilitar protocolo multienlace**, puede seleccionar el número máximo de enlaces o conexiones permitidas por paquete compuesto multienlace. También puede especificar que es preciso negociar el protocolo de asignación de ancho de banda (BAP) para cada paquete compuesto multienlace.
  - **Para los perfiles de marcación**, si selecciona **Habilitar protocolo multienlace**, puede configurar valores de multienlace. El recuadro de diálogo de valores de multienlace le permite seleccionar el número máximo de enlaces permitidos por paquete compuesto multienlace. En este recuadro de diálogo, también puede seleccionar la opción de permitir que un sistema remoto pueda solicitar al sistema local que inicie una llamada al sistema remoto, así como la opción **Habilitar supervisión de utilización de ancho de banda** para supervisar el ancho de banda total de un paquete compuesto multienlace. En función del porcentaje de utilización de Añadir enlace/Eliminar enlace, los enlaces se añadirán al paquete compuesto multienlace o se eliminarán de él según se necesite.

Página Autenticación:

- En el caso de los **Perfiles de conexión de originador**, podrá habilitar en esta página la identificación del sistema local o la identificación del sistema remoto.
- En el caso de los **Perfiles de conexión de receptor**, podrá elegir entre autenticar localmente por medio de una lista de validación o autenticar remotamente con un servidor RADIUS.

  Nota: Debe habilitar las propiedades NAS de RADIUS configuradas desde Operations Navigator.
- Esta página le permite definir los usuarios que pueden conectarse al sistema. En el caso de las conexiones por línea telefónica, deberá especificar el nombre de usuario y la contraseña que se utilizarán para conectar con el sistema remoto.
- El protocolo de autenticación recomendado siempre es CHAP (protocolo de autenticación de reconocimiento de identificación). Los datos de autenticación de CHAP están cifrados y son exclusivos para cada petición de identificación.
- AT&T Global Network exige que los clientes utilicen el protocolo de autenticación de contraseñas (PAP) para la autenticación. Puede haber otros ISP que utilicen el protocolo de autenticación CHAP. Póngase en contacto con su ISP para averiguar los requisitos de nombre de usuario y contraseña.
- No utilice el mismo nombre de usuario y contraseña para ambos protocolos, CHAP y PAP. Alguien podría averiguar el nombre de usuario y la contraseña utilizados para el protocolo CHAP si leyera el nombre de usuario y la contraseña utilizados para PAP, que no están cifrados.
- El nombre de usuario y la contraseña funcionan con un protocolo determinado. La autenticación no será correcta si, durante la petición de identificación, el nombre de usuario y la contraseña no coinciden con los definidos para el protocolo.

Página Valores de TCP/IP:

- En esta página se pueden definir las direcciones IP local y remota que se utilizarán en las conexiones punto a punto. Asimismo, se pueden establecer otros atributos de TCP/IP como el reenvío de IP o el enmascaramiento de direcciones IP.
  - **Direcciones IP locales:**
    - Para los perfiles de respuesta, puede elegir entre utilizar una dirección IP local existente del servidor iSeries como dirección local punto a punto (opción recomendada) o crear una dirección IP exclusiva.

      Si utiliza una dirección local existente, la conexión punto a punto que se crea se conoce como red no numerada. Ello se debe a que esta opción equivale a ampliar la red existente, en vez de crear una nueva. Para los perfiles de respuesta de múltiples conexiones, tendrá que utilizar una dirección IP local existente.

      Para seleccionar una dirección local existente, utilice la lista desplegable del campo Dirección IP local. El tipo de línea asociado a la dirección IP local se especifica junto a la dirección IP con el fin de ayudar a localizar la dirección IP local adecuada que hay que utilizar.
    - Para los perfiles de marcación, la dirección IP local suele definirse como dinámica, especialmente si el perfil se conecta con un proveedor de servicios de Internet (ISP).
  - **Direcciones IP remotas:**
    - La dirección IP remota es la dirección IP definida para el sistema remoto. En el caso de los perfiles de respuesta, si usted lo desea, el usuario remoto puede acceder a la red conectada a la dirección IP local. Para ello, utilice una dirección existente para la dirección IP local, y una dirección IP remota que esté en la misma red que la dirección local. Si prefiere restringir el acceso de un usuario remoto, impidiéndole que acceda a la red conectada a la dirección IP local, utilice una dirección IP remota que no esté en la misma red que la dirección local o asegúrese de inhabilitar el reenvío de IP.
    - En el caso de los perfiles de marcación, la dirección IP remota suele definirse como dinámica, especialmente si el perfil se utiliza para conectar con un ISP.
- Para la modalidad Similar remoto habilitado, puede especificar el perfil de conexión Respuesta de similar con las direcciones IP local y remota.

- Para los perfiles de originador, puede elegir entre no tener rutas adicionales, añadir el sistema remoto como ruta por omisión o definir rutas estáticas adicionales. Pulse **Opciones avanzadas** para especificar otros valores.

  El diálogo de valores de **Opciones avanzadas** permite seleccionar la compresión de cabecera, el direccionamiento dinámico y si las reglas de filtrado de paquetes IP se deben aplicar a la conexión PPP. Para los perfiles de receptor, puede definir las direcciones IP que hay que asignar tomando como base el ID de usuario del sistema remoto. Para cada ID de usuario, podrá definir rutas estáticas adicionales.

Página Otros:

- Esta página le permite identificar el nombre del subsistema que ejecutará todos los trabajos de un perfil de conexión concreto. El subsistema solo es configurable para los perfiles L2TP, RDSI o de líneas analógicas de múltiples conexiones.
- En esta página puede especificar el script de conexión SLIP. Para PPP no se necesitan scripts de conexión. SLIP utiliza un script de conexión para la autenticación y para pasar información de dirección IP.

Página DNS:

- En esta página se define el servidor de nombres de dominio de la conexión.
- Esta página solo se visualiza para los perfiles de conexión de originador.

Supervisar la actividad de PPP

Esta página explica cómo se puede ver un perfil de conexión y las anotaciones de sesión utilizando Operations Navigator.

Acerca de los trabajos de conexión PPP:

- Hay dos trabajos de control de PPP que se emplean para gestionar los trabajos de las conexiones PPP individuales. Estos trabajos se ejecutan en el subsistema QSYSWRK:
  - QTPPPCTL - Trabajo de control de PPP principal. Este trabajo gestiona cada uno de los trabajos de conexión PPP.
  - QTPPPL2TP - Servidor L2TP. Este trabajo gestiona el establecimiento de túneles L2TP y solo se ejecuta si en ese momento está funcionando un perfil L2TP.
- Los trabajos de conexión PPP se ejecutan bajo el perfil de usuario QTCP y sirven para manejar cada una de las conexiones PPP individuales. Estos trabajos se ejecutan por omisión en el subsistema QUSRWRK, pero se pueden configurar para que se ejecuten en otros subsistemas. Se emplean dos nombres de trabajos de conexión PPP:
  - QTPPPSSN - Este trabajo se utiliza para manejar todas las conexiones PPP que no son L2TP.
  - QTPPPL2SSN - Este trabajo se utiliza para manejar los datos de PPP virtual después de que los trabajos QTPPPL2TP hayan negociado satisfactoriamente un túnel L2TP.
- Los trabajos de conexión SLIP se ejecutan en el subsistema QSYSWRK bajo el nombre de usuario QTCP. Hay dos tipos de nombres de trabajos SLIP:
  - QTPPDIAL*nn*, que son trabajos de marcación de salida, siendo *nn* cualquier número comprendido entre 1 y 99.
  - QTPPANS*nn*, que son trabajos de marcación de entrada, siendo *nn* cualquier número comprendido entre 1 y 99.

Trabajar con perfiles de conexión:

1. En Operations Navigator, expanda su servidor y acceda a **Red –> Servicios de acceso remoto**. Seleccione **Perfil de conexión de originador** o **Perfil de conexión de receptor**.
2. En la columna Perfil, pulse con el botón derecho del ratón el nombre de perfil de una conexión y seleccione una de las opciones siguientes:

- **Trabajos**, que abre las anotaciones de los trabajos QTPP*xxx*.
- **Conexiones**, que abre un recuadro de diálogo para visualizar información sobre todas las conexiones asociadas al perfil. La información puede incluir los datos de una conexión actual, de las conexiones anteriores o las dos cosas. Existen opciones para ver la salida de los trabajos o los detalles de cada una de las conexiones.
- **Propiedades**, que abre la página Propiedades, en la que se visualizan las propiedades actuales de una conexión.

Ver información de conexiones:

1. En Operations Navigator, expanda su servidor y acceda a **Red –> Servicios de acceso remoto**. Seleccione **Perfil de conexión de originador** o **Perfil de conexión de receptor**.
2. En la columna Perfil, pulse con el botón derecho del ratón el nombre de perfil de una conexión cuyo estado no sea Inactivo y seleccione **Conexiones** para ver información sobre las conexiones.

   Se mostrará cada una de las conexiones de este perfil (actual y anterior). El campo de estado indica el estado actual de la conexión. En función del estado de cada uno de los trabajos PPP, puede aparecer información adicional como el ID del usuario conectado, las direcciones IP local y remota y el nombre del trabajo PPP.
3. Si desea ver la salida del trabajo o los detalles de una conexión, pulse una conexión con el botón derecho del ratón y se habilitarán los botones.
4. Para ver la salida del trabajo, pulse **Trabajos**. En las anotaciones de trabajo, pulse el nombre del trabajo con el botón derecho del ratón y seleccione **Salida de impresora**. Entonces se puede visualizar el contenido de las anotaciones de sesión y las anotaciones de trabajo (en el caso de las sesiones finalizadas) de la conexión.
5. Para ver los detalles de la conexión, pulse **Detalles**. Solo se pueden visualizar los detalles de las conexiones que estén activas en ese momento. El diálogo de detalles le permitirá ver información adicional sobre esta conexión en concreto.

Trabajar con salida PPP desde el servidor iSeries:

Para trabajar con la salida PPP, teclee WRKTCPPTP en la línea de mandatos del servidor iSeries:

- Para trabajar con TODOS los trabajos PPP activos (incluidos los trabajos QTPPPCTL y QTPPPL2TP), pulse la tecla **F14** (Trabajar con trabajos activos).
- Para trabajar con toda la salida de un determinado perfil de conexión, seleccione la **opción 8** (trabajar con salida) para ese perfil.
- Para imprimir la configuración del perfil PPP, seleccione la **opción 6** (imprimir) para ese perfil.

Estado de conexión:

El estado del perfil de conexión se visualiza en el campo **Estado** correspondiente a cada perfil de la lista de perfiles de conexión. El estado de una conexión individual se visualiza mediante el diálogo Conexiones.

Descripción del estado	Explicación
En espera de peticiones de conexión	El perfil de receptor está preparado para una conexión
En espera de llamada entrante	El servidor está preparado para una conexión
Conectándose	En proceso de conectarse al sistema remoto
Activa/Conexiones activas	Se ha establecido la conexión y el trabajo se está ejecutando satisfactoriamente
Inactiva	Actualmente no se está ejecutando ningún trabajo para este perfil de conexión
Finalizada	Información disponible

Capítulo 7. Resolución de problemas de PPP

La información actual relacionada con los arreglos temporales de programa (PTF) y la resolución de problemas se facilita en la página de presentación de TCP/IP del servidor iSeries . Este enlace proporciona la información más reciente que complementa y prevalece sobre la información que figura en el presente tema.

Si surgieran problemas de conexión PPP, puede utilizar esta lista de comprobación para reunir información sobre los errores. Esta lista de comprobación pretende ayudarle a identificar los síntomas del error y resolver los problemas de conexión PPP.

1. Material de soporte obligatorio:
   - Sistema operativo, nivel y tipo del sistema principal remoto
   - Nivel del sistema operativo del sistema principal servidor iSeries
   - Anotaciones de trabajo de la sesión anómala y archivo de diálogo de conexión

     En V5R1, las anotaciones de trabajo y la salida del diálogo de conexión se guardan en una cola de salida (OUTQ) que tiene el mismo nombre que el perfil.
   - Script de la conexión, si se utiliza en el entorno
   - Estado del perfil de conexión antes y después de que fallara la conexión
2. Material de soporte recomendado:
   - Descripción de línea
   - Perfil de conexión

     La opción 6 de WRKTCPPTP imprime los valores del perfil.
   - Tipo y modelo del módem
   - Series de los mandatos del módem
   - Rastreo de comunicaciones

El libro rojo ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190) explica detenidamente los siguientes problemas de PPP. Además, facilita información detallada sobre la resolución de problemas.

Problema	Solución
Configuración de hardware del módem Configuración errónea de conmutadores dip y otros valores de hardware	Asegúrese de que el módem está configurado para el tipo correcto de tramas. El tipo puede ser *Asíncrono* o *Síncrono*. Hallará más información en el manual del módem.
Mandatos AT del módem El módem que está intentando utilizar no figura en la lista predefinida de módems de Operations Navigator.	Cree un nuevo módem.
Usuarios y contraseñas de PPP Se producen errores relacionados con el nombre de usuario y la contraseña al intentar una conexión PPP.	• Fíjese en cómo ha entrado el ID de usuario y la contraseña, pues son sensibles a las mayúsculas/minúsculas. • Asegúrese de que coincide el protocolo de autenticación utilizado por los similares. • No utilice PAP en un similar si el otro similar está configurado para CHAP.

Problema	Solución
Líneas PPP para iniciar un perfil de conexión Las líneas PPP identificadas las utiliza el mismo recurso de hardware.	No olvide desactivar las otras líneas que utilizan el mismo recurso de hardware.
Protocolo PPP Pueden producirse errores de conexión debido a una configuración equivocada del protocolo PPP.	Puede ser necesario investigar los niveles inferiores del protocolo PPP cuando se dan situaciones en las que los similares no se pueden comunicar entre sí debido a un error de configuración. Si en las anotaciones de PPP o en las anotaciones del trabajo PPP no aparece ninguna indicación del problema, puede investigarlo utilizando la función de rastreo de comunicaciones.

Capítulo 8. Más información sobre PPP

Otras fuentes de información sobre PPP:

- Localice los últimos arreglos temporales de programa (PTF) y la información de configuración más reciente sobre PPP y L2TP mediante el enlace PPP que hay en la página de presentación de TCP/IP para servidor iSeries  . Este enlace proporciona la información más reciente que complementa y prevalece sobre la información incluida en el tema **Servicios de acceso remoto: conexiones PPP**.

- Lea el capítulo que trata sobre PPP en *OS/400 TCP/IP Configuration and Reference*  . Esta información describe escenarios adicionales de PPP, como el acceso por LAN remota al direccionamiento dinámico.

- El libro rojo ITSO TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  explica detenidamente los servicios y las aplicaciones de TCP/IP.

Impreso en España