System i

Servicios de acceso remoto a redes: conexiones PPP

Versión 6 Release 1

System i

Servicios de acceso remoto a redes: conexiones PPP

Versión 6 Release 1

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información del apartado “Avisos”, en la página 73.

Esta edición es aplicable a la versión 6, release 1, modificación 0 de IBM i5/OS (producto número 5761–SS1) y a todos los releases y modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones. Esta versión no se ejecuta en todos los modelos RISC (Reduced Instruction Set Computer) ni en los modelos CISC.

Contenido

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.

PPP es el protocolo de conexión que más se utiliza entre los proveedores de servicios de Internet (ISP). PPP permite que los sistemas individuales puedan acceder a las redes. Las redes, por su parte, proporcionan acceso a Internet. El producto System i 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 a la plataforma System i. Mediante PPP, los sistemas remotos conectados al sistema pueden acceder a los recursos o a las otras máquinas que pertenecen a la misma red que el sistema. También podrá configurar el sistema para que se conecte a Internet utilizando PPP. El asistente de conexión por línea telefónica de System i Navigator le podrá orientar durante el proceso de conectar el sistema a Internet o a una red interna.

Archivo PDF para Servicios de acceso remoto

Puede ver e imprimir un archivo PDF de esta información.

Para ver o descargar la versión PDF de este documento, seleccione Servicios de acceso remoto: conexiones PPP (940 KB, aproximadamente).

Cómo guardar los archivos PDF

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

1. Pulse con el botón derecho el enlace PDF en el navegador.
2. Pulse la opción que guarda el archivo PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el archivo PDF.
4. Pulse **Guardar**.

Cómo descargar Adobe Reader

Necesita tener instalado Adobe Reader en el sistema para poder ver o imprimir estos archivos PDF. Puede descargar una copia gratuita desde el sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Referencia relacionada

"Información relacionada con los Servicios de acceso remoto" en la página 70
Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas Servicios de acceso remoto. Puede ver o imprimir los archivos PDF que desee.

Conceptos de PPP

Puede utilizar PPP para conectar una plataforma System i a redes remotas, a máquinas PC cliente, a otra plataforma System i o a un proveedor de servicios de Internet (ISP). Para poder utilizar plenamente este protocolo, conviene que conozca las prestaciones y el soporte de i5/OS para este protocolo.

Referencia relacionada

"Información relacionada con los Servicios de acceso remoto" en la página 70
Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas Servicios de acceso remoto. Puede ver o imprimir los archivos PDF que desee.

Qué es PPP

El protocolo punto a punto (PPP) es un protocolo TCP/IP que se emplea para conectar un sistema informático a otro. Las máquinas emplean PPP para comunicarse por la red telefónica o por Internet.

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 a través de la red.

El protocolo punto a punto (PPP) permite que haya 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 las peticiones de comentarios (RFC) estándar que describen el protocolo PPP.

Hallará más información sobre las RFC en la página Web de RFC Editor.

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

Perfiles de conexión

Los perfiles de conexión punto a punto definen un conjunto de parámetros y recursos para las conexiones de protocolo punto a punto (PPP) específicas. Puede iniciar perfiles que utilizan estos valores de parámetro para acceder por llamada telefónica a las conexiones PPP (originar) o bien para estar a la escucha de ellas (recibir).

Utilice los dos tipos de perfiles siguientes para definir una serie de características para una conexión o un conjunto de conexiones PPP:

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

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

- ¿Qué tipo de protocolo de conexión utiliza? (PPP o Protocolo Internet de línea serie (SLIP))
- ¿Hace el sistema una llamada por línea telefónica para contactar con la otra máquina (originador)? ¿Espera el sistema recibir una llamada del otro sistema (receptor)?
- ¿Qué línea de comunicaciones utiliza la conexión?
- ¿Cómo debe determinar el sistema la dirección IP que va a utilizar?
- ¿Cómo debe autenticar el sistema a otro sistema? ¿Dónde ha de almacenar el sistema 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 y opciones de marcación
- Autenticación
- Valores de TCP/IP: direcciones IP, direccionamiento y filtrado de IP
- Gestión de trabajos y personalización de la conexión
- Servidores de nombres de dominio

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

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

  Tipo de conexión. Especifica el tipo de línea en el que se basan las conexiones y si estas son de marcación (originador) o de respuesta (receptor). Puede elegir de entre estos tipos de conexión:

  – Línea conmutada
  – Línea alquilada (dedicada)
  – L2TP (Layer Two Tunneling Protocol) (línea virtual)
  – Protocolo punto a punto por Ethernet (PPPoE) (línea virtual)

  PPPoE solo está soportado para los perfiles de conexión de originador.
- La **modalidad de operación**. La modalidad de operación disponible depende del tipo de conexión.

Tabla 1. Modalidades operativas disponibles para los perfiles de conexión de originador

Tipo de conexión	Modalidades operativas disponibles
Línea conmutada	• Marcación • Marcación a petición (solo marcar) • Marcación a petición (similar dedicado habilitado para respuesta) • Marcación a petición (similar remoto habilitado)
Línea alquilada	Iniciador
L2TP	• Iniciador • Iniciador multisalto • Marcación remota
PPP por Ethernet	Iniciador

Tabla 2. Modalidades operativas disponibles para los perfiles de conexión de receptor

Tipo de conexión	Modalidades operativas disponibles
Línea conmutada	Respuesta
Línea alquilada	Terminador
L2TP	Terminador (servidor de red)

- 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

  Para los demás tipos de conexión (alquilada, L2TP, PPPoE), la selección del servicio de línea es únicamente una sola línea.

Referencia relacionada

"Requisitos de software y de hardware" en la página 33
En un entorno de protocolo punto a punto (PPP) se necesitan dos o más máquinas que den soporte a PPP. Una de esas máquinas, la plataforma System i, puede ser el originador o el receptor.

Soporte de políticas de grupo

Con el soporte de políticas de grupo, los administradores de red pueden definir políticas de grupo basadas en usuarios para gestionar recursos. Pueden asignarse políticas de control de acceso a usuarios individuales cuando inician una sesión de protocolo punto a punto (PPP) o una sesión L2TP (Layer Two Tunneling Protocol).

Los usuarios se pueden identificar por su pertenencia a una determinada clase de usuario. Cada clase tiene su propia política exclusiva que define los límites de recursos (por ejemplo, el número de enlaces permitidos en un paquete compuesto multienlace), los atributos (por ejemplo, el reenvío de IP) y la identificación del conjunto de reglas de filtrado de paquetes IP que deberían aplicarse. Por ejemplo, con el soporte de políticas de grupo, los administradores de red pueden definir un grupo de Trabajo_en_casa que permita acceso completo a la red, o un grupo de Trabajadores_de_proveedor que esté restringido a un conjunto de servicios.

Referencia relacionada

"Caso práctico: conexión del sistema a un concentrador de acceso PPPoE" en la página 10
Muchos proveedores de servicios de Internet (ISP) ofrecen acceso a Internet de alta velocidad a través de una Línea de abonado digital (DSL) utilizando el protocolo punto a punto por Ethernet (PPPoE). Puede conectar el sistema a estos ISP para proporcionar conexiones con un amplio ancho de banda que conserven las ventajas del protocolo punto a punto (PPP).

"Caso práctico: gestión del acceso de usuarios remotos a los recursos mediante las políticas de grupo y el filtrado de IP" en la página 24
Las políticas de acceso de grupo identifican los distintos grupos de usuarios de una conexión y permiten aplicar atributos de conexión comunes y valores de seguridad a todo el grupo. Puede utilizar políticas de grupo, junto con el filtrado de IP, para permitir y restringir el acceso a direcciones IP específicas de la red.

Casos prácticos: acceso remoto utilizando conexiones PPP

Estos casos prácticos describen cómo funciona el protocolo punto a punto (PPP) y cómo implementar un entorno PPP en una red. Los casos prácticos también 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.

Referencia relacionada

"Información relacionada con los Servicios de acceso remoto" en la página 70
Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas Servicios de acceso remoto. Puede ver o imprimir los archivos PDF que desee.

Ejemplo: PPP y DHCP en un solo System i

En este ejemplo se explica cómo configurar un modelo de System i como servidor de Protocolo de configuración dinámica de hosts (DHCP) para una LAN y un cliente de acceso telefónico remoto.

Los clientes remotos, como los clientes de acceso telefónico, necesitan acceder con frecuencia a la red de una empresa. Los clientes de acceso telefónico pueden obtener acceso a un modelo de System i con el protocolo punto a punto (PPP). Para acceder a la red, el cliente de acceso telefónico necesita información IP como cualquier cliente de red conectado directamente. Un servidor DHCP System i puede distribuir información de direcciones IP a un cliente de acceso telefónico PPP como a cualquier otro cliente conectado directamente. En la siguiente figura se muestra un cliente remoto que necesita establecer una conexión telefónica con la red de la empresa para realizar un trabajo.

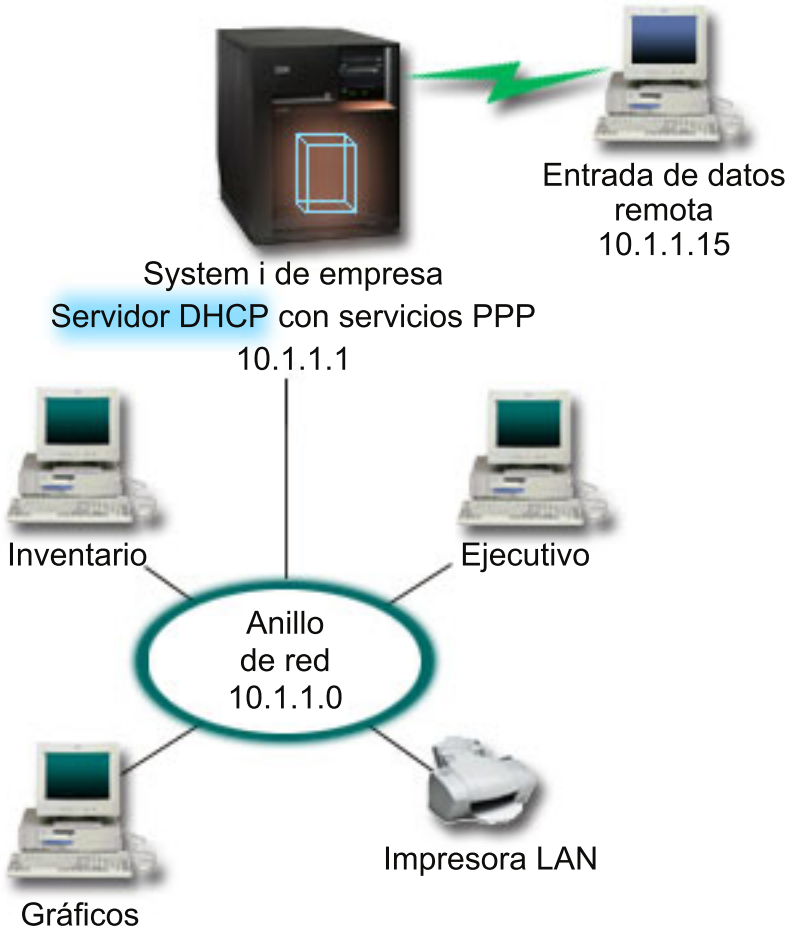


Figura 1. PPP y DHCP en un solo modelo de System i

Para que el empleado remoto pueda formar parte de la red de la empresa, el modelo de System i debe utilizar una combinación de Servicios de acceso remoto y DHCP. La función de Servicios de acceso remoto ofrece la posibilidad de acceso telefónico para el modelo de System i. Si se configura correctamente, cuando el cliente establece la conexión telefónica, el servidor PPP solicita al servidor DHCP que distribuya la información TCP/IP al cliente remoto.

En este ejemplo, una sola política de subred DHCP cubre los clientes de red in situ y los clientes de acceso telefónico.

Si desea que el perfil PPP relegue la distribución IP a DHCP, debe hacerlo en el perfil PPP. En los valores de TCP/IP del perfil de conexión del receptor, establezca el método de asignación de direcciones IP remotas de Fijo a DHCP. Para que los clientes de acceso telefónico puedan comunicarse con otros clientes de red como la impresora LAN, debe permitir también el reenvío de IP en los valores de TCP/IP del perfil y las propiedades de la configuración TCP/IP (pila). Si solo establece el reenvío de IP en el perfil PPP, el modelo de System i no pasará los paquetes IP. Debe establecer el reenvío de IP en el perfil y la pila.

Asimismo, la dirección IP de la interfaz local en el perfil PPP debe ser una dirección IP que cumpla la definición de subred en el servidor DHCP. En este ejemplo, la dirección IP de la interfaz local del perfil PPP debe ser 10.1.1.1. Esta dirección también se debe excluir de la agrupación de direcciones del servidor DHCP, para que no se le asigne a ningún cliente DHCP.

Planificación de la configuración de DHCP para clientes in situ y PPP

Tabla 3. Opciones de configuración global (se aplica a todos los clientes que utilizan el servidor DHCP)

Objeto		**Valor**
Opciones de configuración	Opción 1: máscara de subred	255.255.255.0
	Opción 6: servidor de nombres de dominio	10.1.1.1
	Opción 15: nombre de dominio	mycompany.com
¿El sistema está realizando actualizaciones de DNS?		No
¿El sistema está dando soporte a clientes BOOTP?		No

Tabla 4. Subred de clientes in situ y de acceso telefónico

Objeto		**Valor**
Nombre de subred		MainNetwork
Direcciones a gestionar		10.1.1.3 - 10.1.1.150
Tiempo de cesión		24 horas (valor predeterminado)
Opciones de configuración	Opciones heredadas	Opciones de la configuración global
Direcciones de subred no asignadas por el servidor		10.1.1.1 (dirección de interfaz local especificada en los Valores de TCP/IP de las propiedades del perfil de conexión de receptor en System i Navigator)

Otra configuración

- Establezca el método de dirección IP remota como DHCP en el perfil de conexión de receptor PPP.
  1. Habilite la conexión de cliente WAN DHCP con un servidor DHCP o una conexión de retransmisión utilizando el elemento de menú **Servicios** de Servicios de acceso remoto en System i Navigator.
  2. Seleccione utilizar DHCP para el método de asignación de direcciones IP en las Propiedades de los valores de TCP/IP del Perfil de conexión de receptor en System i Navigator.
- Permita que el sistema remoto acceda a otras redes (reenvío de IP) en las Propiedades de los valores de TCP/IP del Perfil de conexión de receptor en System i Navigator.
- Habilite el reenvío de datagramas IP en Propiedades de los valores de la Configuración TCP/IP en System i Navigator.

Ejemplo: perfil DHCP y PPP en distintos modelos de System i

En este ejemplo se explica cómo configurar dos modelos de System i como el servidor de Protocolo de configuración dinámica de hosts (DHCP) de red y el agente de retransmisión BOOTP/DHCP para dos LAN y clientes de acceso telefónico remoto.

En el ejemplo sobre PPP y DHCP en un solo modelo de System i, se muestra cómo utilizar PPP y DHCP en un solo sistema para permitir el acceso de clientes de acceso telefónico a una red. Ya sea debido al diseño físico de la red o por motivos de seguridad, es preferible tener los servidores PPP y DHCP separados o tener un servidor PPP dedicado sin servicios DHCP. La figura siguiente representa una red que tiene clientes de acceso telefónico, con las políticas PPP y DHCP en servidores diferentes.

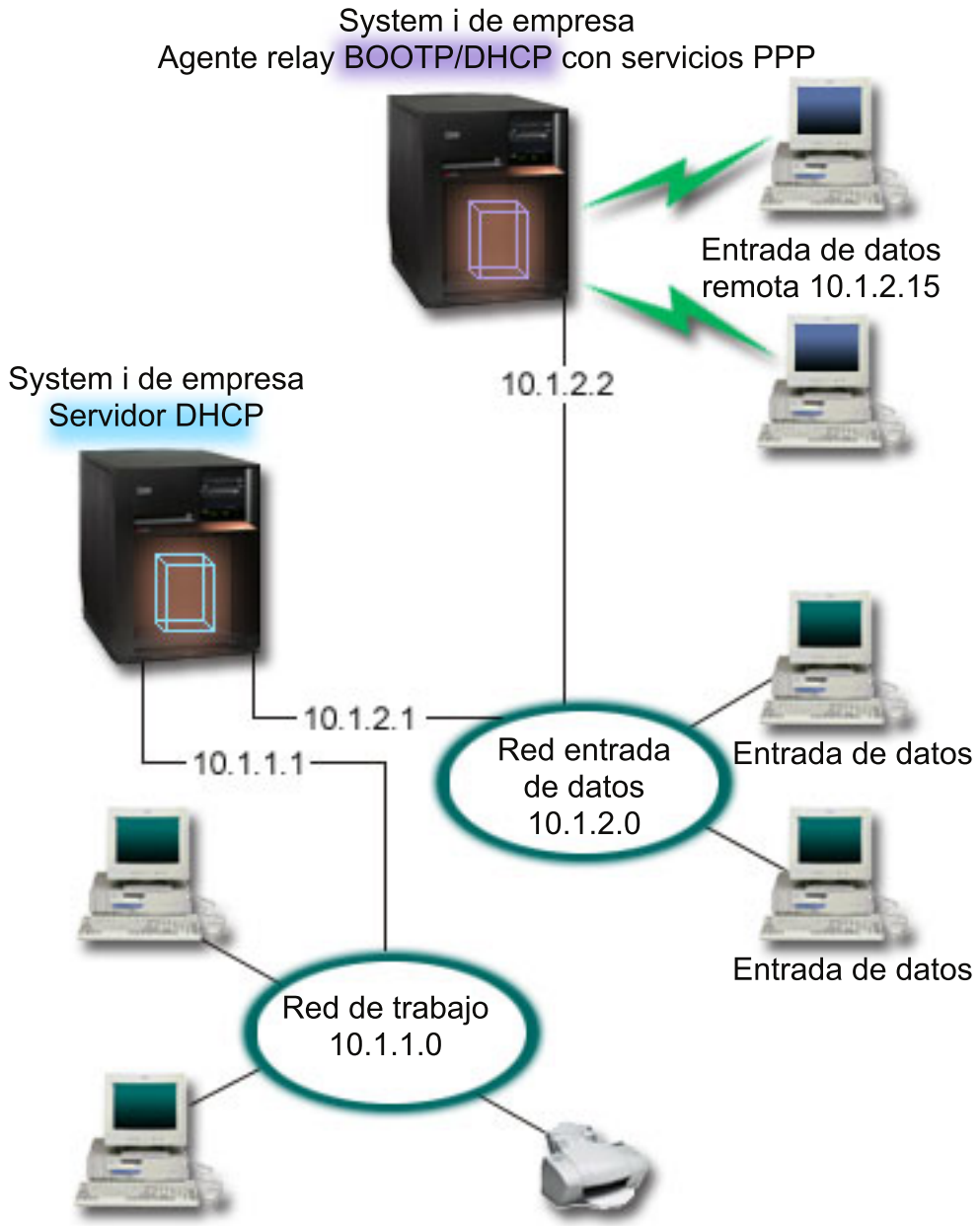


Figura 2. Perfil DHCP y PPP en distintos modelos de System i

Los clientes de entrada de datos remota realizan una conexión telefónica con el servidor PPP de System i. El perfil PPP en ese servidor debe tener un método de dirección IP remota DHCP, como el que se utiliza en el ejemplo de PPP y DHCP en un solo modelo de System i. El perfil PPP y las propiedades de la pila TCP/IP en el servidor PP deben permitir el reenvío de IP. Asimismo, como este servidor actúa como un agente de retransmisión DHCP, el agente de retransmisión BOOTP/DHCP debe estar activado. Esto permite al servidor de acceso remoto System i pasar paquetes DHCPDISCOVER DISCOVER al servidor DHCP. Posteriormente, el servidor DHCP responde y distribuye información TCP/IP a los clientes de acceso telefónico a través del servidor PPP.

El servidor DHCP es el responsable de distribuir direcciones IP a las redes 10.1.1.0 y 10.1.2.0. En la red de entrada de datos, el servidor DHCP proporciona direcciones IP de 10.1.2.10 a 10.1.2.40 a clientes de acceso telefónico o de red conectada directamente. Los clientes de entrada de datos también necesitan una

dirección de direccionador (opción 3) 10.1.2.1 para comunicarse con la red de trabajo y el servidor DHCP System i también debe tener el reenvío de IP habilitado.

Asimismo, la dirección IP de la interfaz local en el perfil PPP debe ser una dirección IP que cumpla la definición de subred en el servidor DHCP. En este ejemplo, la dirección de la interfaz local del perfil PPP debe ser 10.1.2.2. Esta dirección también se debe excluir de la agrupación de direcciones del servidor DHCP, para que no se le asigne a ningún cliente DHCP. La dirección IP de la interfaz local debe ser una dirección a la que el servidor DHCP pueda enviar paquetes de respuesta.

Planificación de la configuración de DHCP para DHCP con un agente de retransmisión DHCP

Tabla 5. Opciones de configuración global (se aplica a todos los clientes que utilizan el servidor DHCP)

Objeto		**Valor**
Opciones de configuración	Opción 1: máscara de subred	255.255.255.0
	Opción 6: servidor de nombres de dominio	10.1.1.1
	Opción 15: Nombre de dominio	mycompany.com
¿El sistema está realizando actualizaciones de DNS?		No
¿El sistema está dando soporte a clientes BOOTP?		No

Tabla 6. Subred de red de trabajo

Objeto		**Valor**
Nombre de subred		WorkNetwork
Direcciones a gestionar		10.1.1.3 - 10.1.1.150
Tiempo de cesión		24 horas (valor predeterminado)
Opciones de configuración	Opciones heredadas	Opciones de la configuración global
Direcciones de subred no asignadas por el servidor		ninguna

Tabla 7. Subred de red de entrada de datos

Objeto		**Valor**
Nombre de subred		DataEntry
Direcciones a gestionar		10.1.2.10 - 10.1.2.40
Tiempo de cesión		24 horas (valor predeterminado)
Opciones de configuración	Opción 3: direccionador	10.1.2.1
	Opciones heredadas	Opciones de la configuración global
Direcciones de subred no asignadas por el servidor		10.1.2.1 (direccionador) 10.1.2.15 (dirección IP de interfaz local del cliente de entrada de datos remota) 10.1.2.14 (dirección IP de interfaz local del cliente de entrada de datos remota)

Otra configuración en una plataforma System i que ejecuta PPP

- Configure el servidor TCP/IP del agente de retransmisión BOOTP/DHCP

Objeto	Valor
Dirección de la interfaz	10.1.2.2
Retransmitir paquetes a la dirección IP del servidor	10.1.2.1

- Establezca el método de dirección IP remota como DHCP en el perfil de conexión de receptor PPP
  1. Habilite la conexión de cliente WAN DHCP con un servidor DHCP o una conexión de retransmisión utilizando el elemento de menú Servicios de Servicios de acceso remoto en System i Navigator
  2. Seleccione Utilizar DHCP para el método de asignación de direcciones IP en las Propiedades de los valores de TCP/IP del Perfil de conexión de receptor en System i Navigator
- Permita que el sistema remoto acceda a otras redes (reenvío de IP) en las Propiedades de los valores de TCP/IP del Perfil de conexión de receptor en System i Navigator (para que los clientes remotos puedan comunicarse con la Red de entrada de datos)
- Habilite el reenvío de datagramas IP en Propiedades de los valores de la Configuración TCP/IP en System i Navigator (para que los clientes remotos puedan comunicarse con la red de entrada de datos)

Caso práctico: protección de un túnel voluntario L2TP con IPSec

En este caso práctico, aprenderá a configurar una conexión entre un host de una sucursal y una oficina central que utiliza L2TP protegido por IPSec. La sucursal tiene una dirección IP asignada de forma dinámica, mientras que la oficina central tiene una dirección IP estática, direccionable de forma global.

Situación

Supongamos que su empresa tiene una pequeña sucursal en otro país. En un día laborable cualquiera, la sucursal puede necesitar acceder a información confidencial sobre un modelo System i dentro de la intranet corporativa. Su empresa utiliza actualmente una línea alquilada de precio elevado para proporcionar a la sucursal acceso a la red corporativa. Aunque la empresa desea continuar proporcionando un acceso seguro a la intranet, en última instancia, también desea reducir el gasto asociado con la línea alquilada. Esto se puede hacer creando un túnel voluntario L2TP (Layer 2 Tunnel Protocol) que amplía la red 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.

Con un túnel voluntario L2TP, la sucursal remota establece un túnel directamente con el servidor de red L2TP (LNS) de la red corporativa. La funcionalidad del concentrador de acceso L2TP (LAC) reside en el cliente. El túnel es transparente para el proveedor de servicios de Internet (ISP) del cliente remoto, por lo que el ISP no es necesario que dé soporte a L2TP. Si desea obtener más información sobre los conceptos de L2TP, consulte Layer 2 Tunnel Protocol (L2TP).

Importante: Este caso práctico muestra las pasarelas de seguridad conectadas directamente a Internet. No se ha incluido un cortafuegos para simplificar el caso práctico. Esto no implica que el uso de un cortafuegos no sea necesario. Tenga en cuenta los riesgos de seguridad implicados siempre que se conecte a Internet.

Objetivos

En este caso práctico, un sistema de la sucursal se conecta a la red corporativa a través de un sistema de pasarela con un túnel L2TP protegido por VPN.

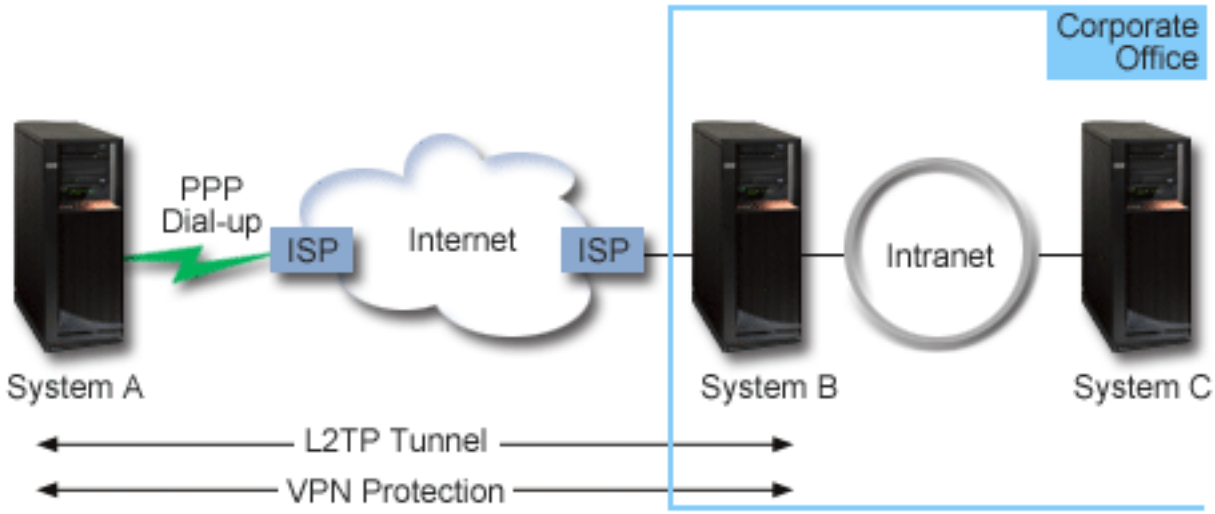
Los objetivos principales de este caso práctico son:

- El sistema de la sucursal siempre inicia la conexión con la oficina central.
- El sistema de la sucursal es el único sistema de la red de la sucursal que necesita acceder a la red corporativa. Es decir, su rol es el de host, no el de pasarela, en la red de la sucursal.

- El sistema corporativo es un host en la red corporativa.

Detalles

En la siguiente figura se ilustran las características de la red para este caso práctico:



Sistema A

- Debe tener acceso a aplicaciones TCP/IP en todos los sistemas de la red corporativa.
- Recibe direcciones IP asignadas de forma dinámica desde el ISP.
- Debe estar configurado para proporcionar soporte L2TP.

Sistema B

- Debe tener acceso a aplicaciones TCP/IP en el sistema A.
- La subred es 10.6.0.0 con la máscara 255.255.0.0. Esta subred representa el punto final de los datos del túnel VPN en el sitio corporativo.
- Se conecta a Internet con la dirección IP 205.13.237.6. Este es el punto final de la conexión. Es decir, el sistema B realiza la gestión de claves y aplica IPSec a los datagramas IP entrantes y salientes. El sistema B se conecta a su subred con la dirección IP 10.6.11.1.

En términos de L2TP, el *Sistema A* actúa como el iniciador L2TP, mientras que el *Sistema B* actúa como el terminador L2TP.

Tareas de configuración

Suponiendo que la configuración TCP/IP ya existe y funciona correctamente, debe completar las siguientes tareas:

Caso práctico: conexión del sistema a un concentrador de acceso PPPoE

Muchos proveedores de servicios de Internet (ISP) ofrecen acceso a Internet de alta velocidad a través de una Línea de abonado digital (DSL) utilizando el protocolo punto a punto por Ethernet (PPPoE). Puede conectar el sistema a estos ISP para proporcionar conexiones con un amplio ancho de banda que conserven las ventajas del protocolo punto a punto (PPP).

Situación

Su empresa necesita una conexión más rápida a Internet, por lo que a usted le interesa obtener un servicio de Línea de abonado Digital (DSL) con un ISP local. Tras una investigación inicial, averigua que el ISP emplea PPPoE para conectar las máquinas cliente. Debe utilizar esta conexión PPPoE para proporcionar conexiones a Internet con un amplio ancho de banda a través del sistema.

Figura 3. Conexión del sistema a un ISP con PPPoE

Solución

Puede dar soporte a una conexión PPPoE con el ISP mediante el sistema. El sistema utiliza un nuevo tipo de línea virtual PPPoE que está enlazada a una línea Ethernet física configurada para utilizar un adaptador Ethernet de tipo 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A o 576A. La línea virtual da soporte a protocolos de sesión PPP por una red de área local (LAN) Ethernet, que está conectada a un módem DSL que proporciona la pasarela al ISP remoto. Esta pasarela permite a los usuarios conectados a la LAN tener un acceso a Internet de alta velocidad mediante la conexión PPPoE. Una vez iniciada la conexión entre el sistema y el ISP, los usuarios individuales de la LAN pueden acceder al ISP a través de PPPoE, utilizando la dirección IP asignada al sistema. Para proporcionar medidas de seguridad adicionales, pueden aplicarse reglas de filtrado a la línea virtual PPPoE con objeto de restringir la parte que convenga del tráfico entrante de Internet.

Configuración de ejemplo

Para crear una configuración PPP de ejemplo de System i Navigator, efectúe los siguientes pasos:

1. Configure el dispositivo de conexión que utilizará con el ISP.
2. Configure un perfil de conexiones de originador en el sistema.
   Asegúrese de que entra esta información:
   - **Tipo de protocolo**: `PPP`
   - **Tipo de conexión**: `PPP por Ethernet`
   - **Modalidad de operación**: `iniciador`

- **Configuración de enlace**: una sola línea

3. En la página General de las propiedades del nuevo perfil punto a punto, entre un nombre y una descripción para el perfil de originador. El nombre hace referencia al perfil de conexión y a la línea virtual PPPoE.
4. Pulse **Conexión** para abrir la página Conexión. Elija el **nombre de línea virtual PPPoE** que se corresponde con el nombre de este perfil de conexión. Tras seleccionar la línea, System i Navigator visualiza el diálogo de **propiedades de la línea**.
   a. En la página General, entre una descripción útil de la línea virtual PPPoE.
   b. Pulse **Enlace** para abrir la página Enlace. En la lista de selección de nombres de líneas físicas, seleccione la línea Ethernet que esta conexión va a emplear y pulse **Abrir**. Por el contrario, si tiene que definir una línea Ethernet nueva, teclee el nombre de la línea y pulse **Nuevo**. System i Navigator muestra el diálogo **Propiedades de la línea Ethernet**.

      Nota: PPPoE requiere un adaptador Ethernet de tipo 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A o 576A.

      1) En la página General, entre una descripción útil de la línea Ethernet y verifique que la definición de la línea está utilizando los recursos de hardware necesarios.
      2) Pulse **Enlace** para abrir la página Enlace. Escriba las propiedades de la línea Ethernet física. Hallará más información en la documentación del adaptador Ethernet y en la ayuda en línea.
      3) Pulse **Otros** para abrir la página Otros. Especifique el nivel de acceso y autorización que los otros usuarios pueden tener sobre esta línea.
      4) Pulse **Aceptar** para regresar a la página de propiedades de la línea virtual PPPoE.
   c. Pulse **Límites** para definir las propiedades de la autenticación LCP o bien pulse **Aceptar** si desea regresar a la página Conexión del nuevo perfil punto a punto.
   d. Cuando regrese a la página Conexión, especifique el direccionamiento del servidor PPPoE basándose en la información que le ha proporcionado el ISP.
5. Si el ISP exige que el sistema se autentique o bien si usted quiere que el sistema autentique el sistema remoto, pulse **Autenticación** para abrir la página Autenticación y entre la información solicitada.
6. Pulse **Valores de TCP/IP** para abrir la página Valores de TCP/IP y especifique los parámetros de manejo de direcciones IP correspondientes a este perfil de conexión. El valor que debe utilizarse lo proporciona el ISP. Para permitir que los usuarios conectados a la LAN se conecten con el ISP utilizando las direcciones IP asignadas al sistema, seleccione **Ocultar direcciones (enmascaramiento total)**.
7. Pulse **DNS** para abrir la página DNS y entre la dirección IP del servidor DNS proporcionada por el ISP.
8. Pulse **Aceptar** para completar el perfil.

Conceptos relacionados

"Soporte de políticas de grupo" en la página 4
Con el soporte de políticas de grupo, los administradores de red pueden definir políticas de grupo basadas en usuarios para gestionar recursos. Pueden asignarse políticas de control de acceso a usuarios individuales cuando inician una sesión de protocolo punto a punto (PPP) o una sesión L2TP (Layer Two Tunneling Protocol).

Tareas relacionadas

"Creación de un perfil de conexión" en la página 50
El primer paso para configurar una conexión PPP entre sistemas consiste en crear un perfil de conexión en el sistema.

Referencia relacionada

"Configuración de enlace" en la página 54
La configuración de enlace define el tipo de servicio de línea que el perfil de conexión del protocolo punto a punto (PPP) utiliza para establecer una conexión.

"Autenticación del sistema" en la página 46
Las conexiones PPP con una plataforma System i dan soporte a varias opciones para autenticar los clientes remotos que acceden telefónicamente al sistema y las conexiones que se establecen con un ISP u otro sistema al que esté accediendo telefónicamente el sistema.

"Manejo de las direcciones IP" en la página 44
Las conexiones del protocolo punto a punto (PPP) permiten utilizar varios juegos de opciones para gestionar direcciones IP en función del tipo de perfil de conexión.

"Filtrado de paquetes IP" en la página 44
El filtrado de paquetes IP limita los servicios que se prestan a usuarios individuales cuando inician una sesión en una red.

Caso práctico: conexión de clientes de acceso telefónico remoto al sistema

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 sistema con protocolo punto a punto (PPP).

Situación

Como administrador de la red de su empresa, debe mantener el sistema y los clientes de la red. En vez de venir a trabajar para resolver y arreglar problemas, necesita la posibilidad de trabajar desde una ubicación remota, por ejemplo, desde su casa. Puesto que su empresa no tiene una conexión de red enlazada a Internet, puede establecer una conexión por línea telefónica con el sistema utilizando una conexión PPP. Además, el único módem que tiene actualmente es el módem de soporte electrónico al cliente 7852-400 y necesita utilizarlo para la conexión.

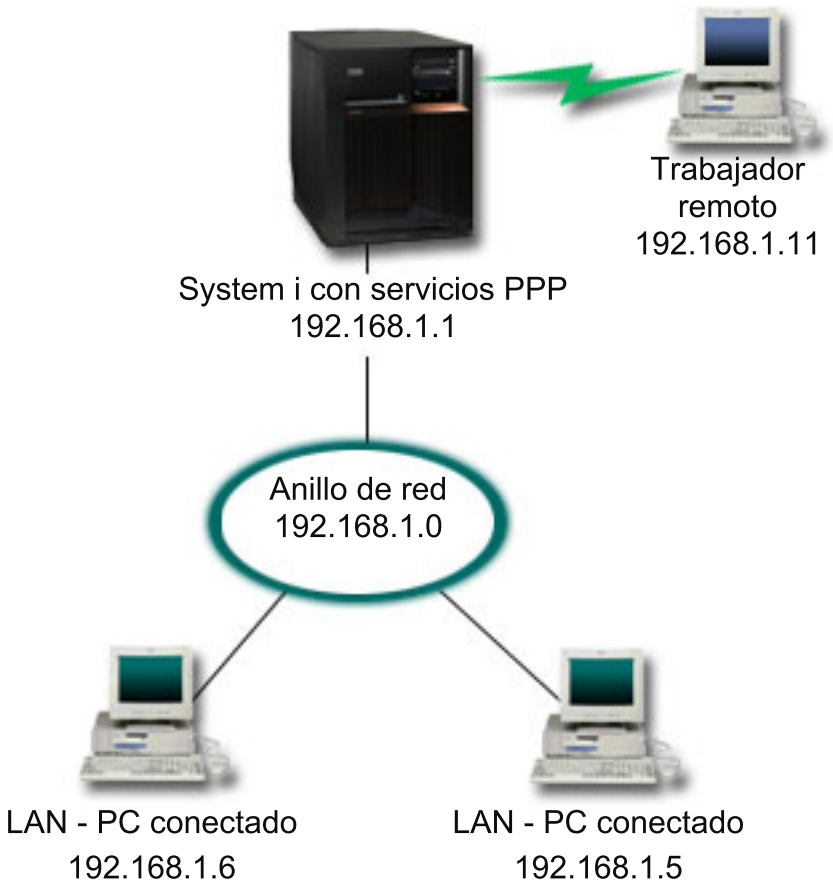


Figura 4. Conexión de clientes remotos al sistema

Solución

Puede emplear PPP para conectar el PC de su casa al sistema utilizando el módem que tiene. Puesto que va a emplear el módem de soporte electrónico al cliente para este tipo de conexión PPP, deberá asegurarse de que el módem está configurado para las dos modalidades, la síncrona y la asíncrona. La figura muestra un sistema con servicios PPP que está conectado a una LAN con dos PC. A continuación, el trabajador remoto establece conexión telefónica con el sistema. El sistema 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 el protocolo de autenticación de reconocimiento de identificación (CHAP-MD5) para autenticarse con el sistema. El sistema no puede utilizar MS_CHAP, por lo que será necesario asegurarse de que el cliente PPP utiliza 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 y, además, el direccionamiento IP debe estar debidamente configurado. 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 figura anterior sólo tiene un cliente de acceso telefónico remoto, porque el módem de soporte electrónico al cliente únicamente puede manejar las conexiones de una en una.

Configuración de ejemplo

Para crear una configuración PPP de ejemplo de System i Navigator, efectúe los siguientes pasos:

1. Configure el acceso telefónico a redes y cree una conexión por línea telefónica en el PC remoto.
2. Configure un perfil de conexiones de receptor en el sistema.

   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 o una agrupación de líneas, 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 **Conexión** para abrir 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 en el que se ha conectado el adaptador 7852–400 y establezca la trama en **Asíncrona**.
   b. Pulse **Módem** para abrir la página Módem. En la lista de selección de nombres, elija el módem **IBM 7852–400**.
   c. Pulse **Aceptar** para regresar a la página de propiedades del nuevo perfil punto a punto.
5. Pulse **Autenticación** para abrir la página Autenticación.
   a. Seleccione **Exigir que este servidor iSeries 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 **Valores de TCP/IP** para abrir la página TCP/IP.
   a. Seleccione la dirección IP local 192.168.1.1.
   b. Para la dirección IP remota, seleccione **Dirección IP fija** con la dirección IP inicial 192.168.1.11.
   c. Seleccione **Permitir a sistema remoto acceder a otras redes**.
7. Pulse **Aceptar** para completar el perfil.

Conceptos relacionados

"Planificación de PPP" en la página 33
La planificación del Protocolo punto a punto (PPP) incluye la creación y la administración de conexiones PPP.

Tareas relacionadas

"Creación de un perfil de conexión" en la página 50
El primer paso para configurar una conexión PPP entre sistemas consiste en crear un perfil de conexión en el sistema.

Referencia relacionada

"Protocolo de autenticación de reconocimiento de identificación con MD5" en la página 47
El Protocolo de autenticación de reconocimiento de identificación (CHAP-MD5) emplea un algoritmo (MD-5) para calcular un valor que solo conocen el sistema que autentica y el dispositivo remoto.

"Configuración de enlace" en la página 54
La configuración de enlace define el tipo de servicio de línea que el perfil de conexión del protocolo punto a punto (PPP) utiliza para establecer una conexión.

"Agrupación de líneas" en la página 55
Para establecer que la conexión PPP utilice una línea de una agrupación de líneas, seleccione este servicio de línea. Al empezar la conexión PPP, el sistema selecciona en la agrupación de líneas una

línea que no se esté utilizando. En el caso de los perfiles de marcación a petición, el sistema no elige la línea hasta que detecta tráfico TCP/IP para el sistema remoto.

Caso práctico: conexión de la LAN de oficina a Internet con un módem

Normalmente, los administradores configuran redes de oficina que permiten a los empleados acceder a Internet. Los administradores pueden utilizar un módem para conectar el sistema a un proveedor de servicios de Internet (ISP). Los clientes PC conectados a la LAN pueden comunicarse con Internet utilizando el sistema operativo i5/OS como pasarela.

Situación

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, debe poder utilizar un módem para conectar a Internet el sistema y los clientes PC conectados a la LAN. La siguiente figura describe un ejemplo en el que se da esta situación.

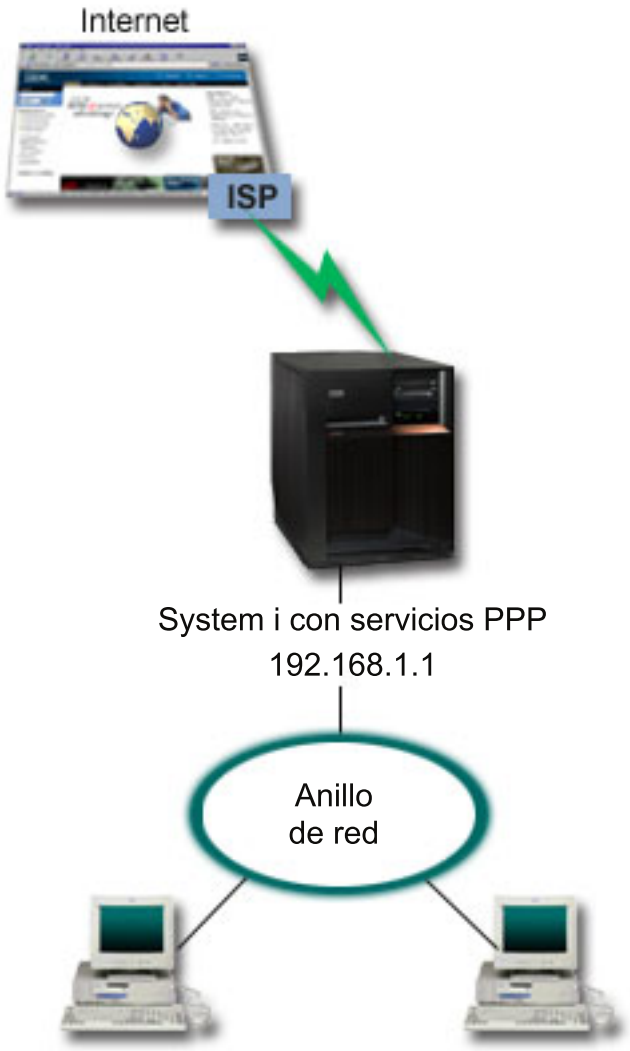


Figura 5. Conexión de la LAN de oficina a Internet con un módem

Solución

Puede emplear el módem integrado (u otro que sea compatible) para conectar el sistema al ISP. Tendrá que crear un perfil de originador de protocolo punto a punto (PPP) en el sistema para establecer la conexión PPP con el ISP.

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

Ahora que el sistema y la red están conectados a Internet, deberá comprender los riesgos que ello supone para la seguridad. En colaboración con el ISP, intente comprender cómo son las políticas de seguridad del ISP y tome medidas adicionales para proteger el sistema y la red.

En función del uso que haga de Internet, debería plantearse la posibilidad de aumentar el ancho de banda.

Configuración de ejemplo

Para crear una configuración de ejemplo de System i Navigator, efectúe los siguientes pasos:

1. Configure un perfil de conexiones de originador en el sistema.

   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 o una agrupación de líneas, 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 **Conexión** para abrir 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. Si selecciona un recurso de módem interno, los valores del tipo de módem y tipo de trama se seleccionarán automáticamente.
   b. 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 **Autenticación** para abrir la página Autenticación y seleccione **Permitir al sistema remoto verificar la identidad de este servidor iSeries**. Seleccione el protocolo de autenticación y entre la información de nombre de usuario o contraseña que sea necesaria.
6. Pulse **Valores de TCP/IP** para abrir la página TCP/IP.
   a. Seleccione **Asignada por sistema remoto** para las direcciones IP local y remota.
   b. Seleccione **Añadir sistema remoto como ruta predeterminada**.
   c. Marque **Ocultar direcciones** para que las direcciones IP internas no se direccionen a Internet.
7. Pulse **DNS** para abrir la página Sistema de nombres de dominio (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 System i 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 a través del sistema.

Conceptos relacionados

"Planificación de PPP" en la página 33
La planificación del Protocolo punto a punto (PPP) incluye la creación y la administración de conexiones PPP.

Tareas relacionadas

"Creación de un perfil de conexión" en la página 50
El primer paso para configurar una conexión PPP entre sistemas consiste en crear un perfil de conexión en el sistema.

Referencia relacionada

"Agrupación de líneas" en la página 55
Para establecer que la conexión PPP utilice una línea de una agrupación de líneas, seleccione este servicio de línea. Al empezar la conexión PPP, el sistema selecciona en la agrupación de líneas una línea que no se esté utilizando. En el caso de los perfiles de marcación a petición, el sistema no elige la línea hasta que detecta tráfico TCP/IP para el sistema remoto.

"Configuración de enlace" en la página 54
La configuración de enlace define el tipo de servicio de línea que el perfil de conexión del protocolo punto a punto (PPP) utiliza para establecer una conexión.

Caso práctico: conexión de 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. El protocolo punto a punto (PPP) puede conectar dos LAN entre sí estableciendo una conexión entre un sistema en la oficina central y otro en la sucursal.

Situación

Supongamos 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 central 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.

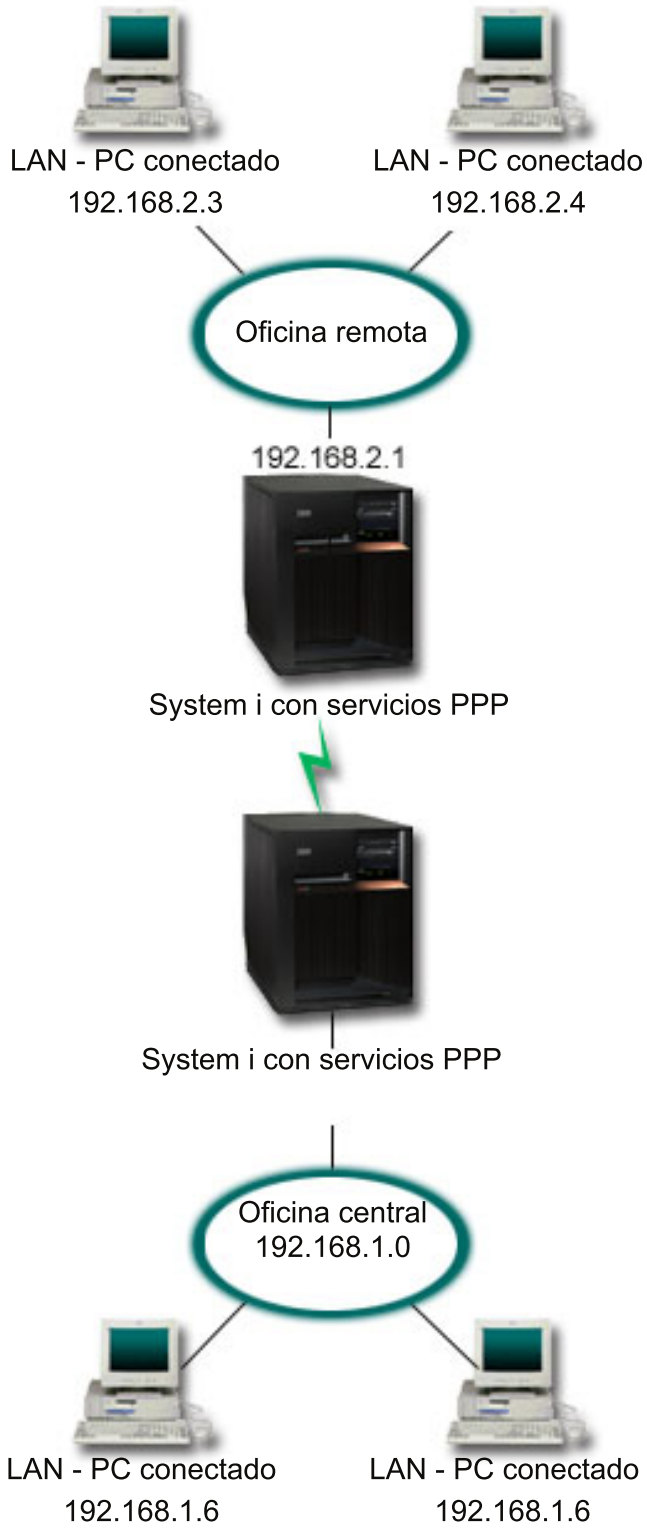


Figura 6. Conexión de las redes corporativa y remota con un módem

Solución

PPP puede conectar dos LAN entre sí estableciendo una conexión entre los sistemas como se indica en la figura. En este caso, imagine que la oficina remota es la que inicia la conexión con la oficina central. Debe configurar un perfil de originador en el sistema remoto y un perfil de receptor en el sistema de la oficina central.

Si los PC de la oficina remota tienen que acceder a la LAN corporativa (192.168.1.0), deberá activar el reenvío de IP en el perfil de receptor de la oficina central y habilitar el direccionamiento de direcciones IP para los PC (192.168.2, 192.168.3, 192.168.1.6 y 192.168.1.5, en este ejemplo). También habría que activar el reenvío de IP de la pila de TCP/IP. Esta configuración habilita la comunicación TCP/IP básica entre las LAN. Debería tomar en consideración factores de seguridad y un DNS para resolver los nombres de host entre las LAN.

Configuración de ejemplo

Para crear una configuración de ejemplo de System i Navigator, efectúe los siguientes pasos:

1. Configure un perfil de conexiones de originador en el sistema de oficina remoto.

   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 o una agrupación de líneas, 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 **Conexión** para abrir 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 **Módem** para abrir la página Módem. En la lista de selección de nombres, 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 para establecer conexión con el sistema de oficina central. No olvide incluir los prefijos que se necesiten.
5. Pulse **Autenticación** para abrir la página Autenticación y seleccione **Permitir al sistema remoto verificar la identidad de este servidor iSeries**. Seleccione **Exigir contraseña cifrada (CHAP-MD5)** y entre la información de nombre de usuario y contraseña necesaria.
6. Pulse **Valores de TCP/IP** para abrir 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 predeterminada**.
   d. Pulse **Aceptar** para completar el perfil de originador.
7. Configure un perfil de conexiones de receptor en el sistema de 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 o una agrupación de líneas, 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 **Conexión** para abrir 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 **Módem** para abrir la página Módem. En la lista de selección de nombres, 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 **Autenticación** para abrir la página Autenticación.
    a. Marque el recuadro **Exigir que este servidor iSeries 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 **Valores de TCP/IP** para abrir 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 caso práctico, los valores apropiados serán:
       - 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 este sistema como pasarela.
12. Pulse **Aceptar** para completar el perfil de receptor.

Tareas relacionadas

"Creación de un perfil de conexión" en la página 50
El primer paso para configurar una conexión PPP entre sistemas consiste en crear un perfil de conexión en el sistema.

Referencia relacionada

"Configuración de enlace" en la página 54
La configuración de enlace define el tipo de servicio de línea que el perfil de conexión del protocolo punto a punto (PPP) utiliza para establecer una conexión.

"Agrupación de líneas" en la página 55
Para establecer que la conexión PPP utilice una línea de una agrupación de líneas, seleccione este servicio de línea. Al empezar la conexión PPP, el sistema selecciona en la agrupación de líneas una línea que no se esté utilizando. En el caso de los perfiles de marcación a petición, el sistema no elige la línea hasta que detecta tráfico TCP/IP para el sistema remoto.

Caso práctico: autenticación de conexiones por línea telefónica con NAS de RADIUS

Un servidor de acceso a red (NAS) que se esté ejecutando en el sistema puede direccionar las peticiones de autenticación desde los clientes de acceso telefónico a un servidor RADIUS (Remote Authentication Dial In User Service) aparte. Si la autenticación es satisfactoria, el servidor RADIUS también puede controlar las direcciones IP asignadas al usuario.

Situación

La red corporativa tiene usuarios remotos que acceden telefónicamente a dos sistemas de una red de acceso telefónico distribuida. Debe centralizar la autenticación, el servicio y la contabilidad, dejando que un solo sistema maneje las peticiones para validar los ID de usuario y las contraseñas y determinar qué direcciones IP están asignadas a ellos.

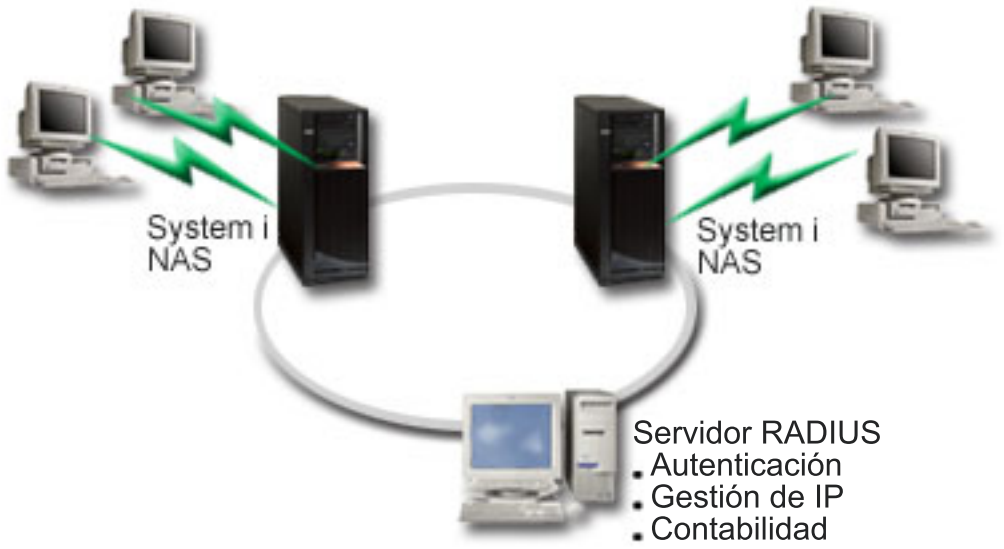


Figura 7. Autenticación de conexiones por línea telefónica con un servidor RADIUS

Solución

Cuando los usuarios intentan conectarse, el NAS que se está ejecutando en los sistemas reenvía la información de autenticación a un servidor RADIUS situado en la red. El servidor RADIUS, que mantiene toda las información de autenticación de la red, procesa la petición de autenticación y responde. Si el usuario queda validado, el servidor RADIUS, si se le configura para ello, también puede asignar la dirección IP de los similares y activar la contabilidad para hacer un seguimiento de la actividad y la utilización del usuario. Para dar soporte a RADIUS, hay que definir el servidor de acceso a red (NAS) de RADIUS en el sistema.

Configuración de ejemplo

Para crear una configuración de ejemplo de System i Navigator, efectúe los siguientes pasos:

1. En System i Navigator, expanda **Red**, pulse **Servicios de acceso remoto** con el botón derecho del ratón y seleccione **Servicios**.
2. En la pestaña **RADIUS**, seleccione **Habilitar conexión de servidor de acceso a red de RADIUS** y **Habilitar RADIUS para autenticación**. Según cual sea su solución RADIUS, también puede optar por hacer que RADIUS maneje la contabilidad de las conexiones y la configuración de las direcciones TCP/IP.
3. Pulse el botón **Valores de NAS de RADIUS**.
4. En la página General, entre una descripción de este servidor.
5. En las páginas Servidor de autenticación (y, opcionalmente, Servidor de contabilidad), pulse **Añadir** y entre esta información:

a. En el recuadro **Dirección IP local**, entre la dirección IP de la interfaz empleada para conectar con el servidor RADIUS.
b. En el recuadro **Dirección IP de servidor**, entre la dirección IP del servidor RADIUS.
c. En el recuadro **Contraseña**, entre la contraseña que sirve para identificar el sistema ante el servidor RADIUS.
d. En el recuadro **Puerto**, entre el puerto del sistema que se utiliza para comunicar con el servidor RADIUS. Los valores predeterminados son el puerto 1812 para el servidor de autenticación o el puerto 1813 para el servidor de contabilidad.

6. Pulse **Aceptar**.
7. En System i Navigator, expanda **Red** → **Servicios de acceso remoto**.
8. Seleccione el perfil de conexión que utilizará el servidor RADIUS para la autenticación. Los servicios RADIUS solo son aplicables para los perfiles de conexión de receptor.
9. En la página Autenticación, marque el recuadro **Exigir que este servidor iSeries verifique la identidad del sistema remoto**.
10. Seleccione **Autenticar remotamente utilizando un servidor RADIUS**.
11. Seleccione el protocolo de autenticación. (Puede ser PAP o CHAP-MD5). El servidor RADIUS también debe utilizar este protocolo.
12. Seleccione **Utilizar RADIUS para edición y contabilidad de conexión**.
13. Pulse **Aceptar** para guardar los cambios en el perfil de conexión.

También debe configurar el servidor RADIUS incluyendo soporte para el protocolo de autenticación, datos de usuario, contraseñas e información de contabilidad. El distribuidor de RADIUS le facilitará más información.

Cuando los usuarios acceden telefónicamente mediante este perfil de conexión, el sistema reenvía la información de autenticación al servidor RADIUS especificado. Si el usuario queda validado, la conexión estará permitida y se emplearán las restricciones de conexión que estén especificadas en la información del usuario sobre el servidor RADIUS.

Tareas relacionadas

"Habilitación de servicios de RADIUS y DHCP para perfiles de conexión" en la página 66
A continuación, se muestran los pasos necesarios para habilitar servicios RADIUS o DHCP (Protocolo de configuración dinámica de hosts) para los perfiles de conexión de receptor PPP.

Referencia relacionada

"Autenticación del sistema" en la página 46
Las conexiones PPP con una plataforma System i dan soporte a varias opciones para autenticar los clientes remotos que acceden telefónicamente al sistema y las conexiones que se establecen con un ISP u otro sistema al que esté accediendo telefónicamente el sistema.

"Visión general de RADIUS (Remote Authentication Dial In User Service)" en la página 48
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.

Caso práctico: gestión del acceso de usuarios remotos a los recursos mediante las políticas de grupo y el filtrado de IP

Las políticas de acceso de grupo identifican los distintos grupos de usuarios de una conexión y permiten aplicar atributos de conexión comunes y valores de seguridad a todo el grupo. Puede utilizar políticas de grupo, junto con el filtrado de IP, para permitir y restringir el acceso a direcciones IP específicas de la red.

Situación

La red tiene varios grupos de usuarios distribuidos, cada uno de los cuales necesita acceso a distintos recursos de la LAN corporativa. Un grupo de usuarios de entrada de datos necesita acceso a la base de datos y a otras aplicaciones. Un grupo de personas de otras empresas necesita acceso telefónico a los servicios HTTP, FTP (Protocolo de transferencia de archivos) y Telnet, pero, por cuestión de seguridad, no debe tener autorización para acceder a otros servicios TCP/IP ni al tráfico TCP/IP. Si define atributos y permisos de conexión detallados para cada usuario, el trabajo será el doble, y si proporciona restricciones de red para todos los usuarios de este perfil de conexión, no garantiza un control suficiente. Usted busca una manera de definir los valores y los permisos de conexión para varios grupos diferenciados de usuarios que rutinariamente acceden por teléfono a este sistema.

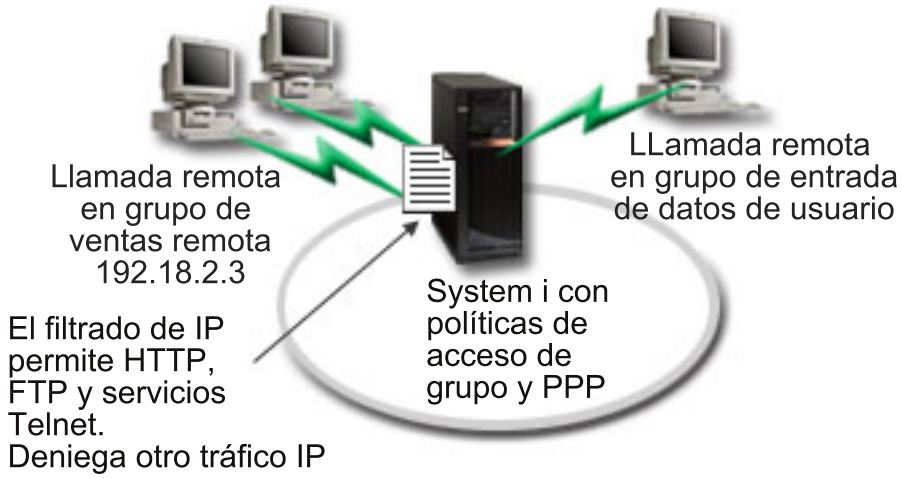


Figura 8. Aplicación de valores de conexión a las conexiones por línea telefónica tomando como base los valores de política de grupos

Solución

Necesita aplicar restricciones de filtrado de IP exclusivas a dos grupos distintos de usuarios. Para lograrlo, debe crear políticas de acceso de grupo y reglas de filtro de IP. Las políticas de acceso de grupo hacen referencia a las reglas de filtro de IP, por lo que primero tendrá que crear las reglas de filtro. En este ejemplo, tiene que crear un filtro PPP que incluya reglas de filtro de IP para la política de acceso de grupo Socio comercial de IBM. Las reglas de filtro permitirán el acceso a los servicios HTTP, FTP y Telnet, pero restringirán el acceso a todo otro servicio y tráfico de TCP/IP mediante el sistema. Este caso práctico solo muestra las reglas de filtro que se necesitan para el grupo de ventas; sin embargo, también puede configurar filtros semejantes para el grupo Entrada de datos.

Finalmente, tendrá que crear las políticas de acceso de grupo (una por grupo) para definir el grupo. Una política de acceso de grupo permite definir atributos de conexión comunes para un grupo de usuarios. Al añadir una política de acceso de grupo a una lista de validación en el sistema, podrá aplicar los valores de conexión durante el proceso de autenticación. La política de acceso de grupo especifica varios valores para la sesión del usuario, entre ellos, la capacidad de aplicar reglas de filtrado de IP que restrinjan las direcciones IP y los servicios TCP/IP disponibles para un usuario durante la sesión.

Configuración de ejemplo

Para crear una configuración de ejemplo de System i Navigator, efectúe los siguientes pasos:

1. Cree el identificador de filtro de protocolo punto a punto (PPP) y las reglas de filtrado de paquetes IP que especifiquen los permisos y las restricciones de esta política de acceso de grupo.

a. En System i Navigator, expanda **Red** → **Servicios de acceso remoto**.
b. Pulse **Perfiles de conexión de receptor** y seleccione Políticas de acceso de grupo.
c. Pulse con el botón derecho del ratón en uno de los grupos predefinidos que figuran en el panel de la derecha y seleccione **Propiedades**.

   Nota: si desea crear una política de acceso de grupo nueva, con el botón derecho del ratón pulse **Políticas de acceso de grupo** y seleccione **Nueva política de acceso de grupo**. Complete la pestaña **General**. A continuación, seleccione la pestaña **Valores TCP/IP** y continúe con el paso e a continuación.
d. Seleccione la pestaña **Valores de TCP/IP** y pulse **Avanzadas**.
e. Seleccione **Utilizar reglas de paquetes IP para esta conexión** y pulse **Editar archivo de reglas**. Se iniciará el editor de reglas de paquetes IP y se abrirá el archivo de reglas de paquetes de los filtros PPP.
f. Abra el menú **Insertar** y seleccione **Filtros** para añadir conjuntos de filtros (FILTER SET). Utilice la pestaña **General** para definir los conjuntos de filtros y la pestaña **Servicios** para definir el servicio que va a permitir, como puede ser HTTP. El siguiente conjunto de filtros, "services_rules", permitirá acceder a los servicios HTTP, FTP y Telnet. Las reglas de filtro incluye una sentencia de denegación predeterminada implícita que restringe los servicios TCP/IP o el tráfico IP que no se haya permitido de forma específica.

   Nota: las direcciones IP del siguiente ejemplo son globalmente direccionables y solo están destinadas para ponerlas como ejemplo.

```
###Los 2 filtros siguientes permitirán el tráfico HTTP (navegador Web) de
entrada y salida del sistema.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
                = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 80 SRCPORT  %
                = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
                = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
                80 FRAGMENTS = NONE JRN = OFF

###Los 4 filtros siguientes permitirán el tráfico FTP de entrada y salida del
sistema.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
                = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 21 SRCPORT  %
                = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
                = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
                21 FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
                = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 20 SRCPORT  %
                = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
                = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
                20 FRAGMENTS = NONE JRN = OFF
###Los 2 filtros siguientes permitirán el tráfico Telnet de entrada y salida
del sistema.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
                = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
                = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
                = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
                = 23 FRAGMENTS = NONE JRN = OFF
```

g. Abra el menú **Insertar** y seleccione **Interfaz de filtro**. La interfaz de filtro le permite crear un identificador de filtro PPP e incluir los conjuntos de filtros que ha definido.
   1) En la pestaña **General**, entre `permitted_services` para el identificador del filtro PPP.
   2) En la pestaña **Conjuntos de filtros**, seleccione el conjunto de filtros **services_rules** y pulse **Añadir**.
   3) Pulse Aceptar. Se añadirá la siguiente línea al archivo de reglas:

```
###Esta sentencia enlaza (asocia) el conjunto de filtros 'services_rules' al
ID de filtro PPP "permitted_services". Después, este ID de filtro PPP
se puede aplicar a la interfaz física asociada a un perfil de conexión PPP
o a una política de acceso de grupo.

FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
```

h. Guarde los cambios y salga. Si más adelante necesita deshacer los cambios, utilice la interfaz basada en caracteres para entrar el mandato `RMVTCPTBL *ALL`. Este mandato elimina todas las reglas de filtro y NAT que hay en el sistema.

i. En el diálogo **Valores avanzados de TCP/IP**, deje en blanco el recuadro **Identificador de filtro PPP** y pulse **Aceptar** para salir. Más adelante, deberá aplicar a una política de acceso de grupo el identificador de filtro que acaba de crear, no este perfil de conexión.

2. Defina una política de acceso de grupo nueva para este grupo de usuarios.
   a. En System i Navigator, expanda **Red** → **Servicios de acceso remoto** → **Perfiles de conexión de receptor**.
   b. Pulse el icono **Política de acceso de grupo** con el botón derecho del ratón y seleccione **Nueva política de acceso de grupo**. System i Navigator muestra el diálogo **Definición de la nueva política de acceso de grupo**.
   c. En la página General, entre un nombre y una descripción para la política de acceso de grupo.
   d. En la página Valores de TCP/IP:
      - Seleccione **Utilizar reglas de paquetes IP para esta conexión** y después el identificador de filtro PPP **permitted_services**.
   e. Seleccione **Aceptar** para guardar la política de acceso de grupo.
3. Aplique la política de acceso de grupo a los usuarios asociados a este grupo.
   a. Abra el perfil de conexión de receptor que controla estas conexiones por línea telefónica.
   b. En la página Autenticación del perfil de conexión de receptor, seleccione la lista de validación que contiene la información de autenticación del usuario y pulse **Abrir**.
   c. En el grupo de ventas, seleccione un usuario al que desee aplicar la política de acceso de grupo y pulse **Abrir**.
   d. Pulse **Aplicar una política de grupo al usuario** y seleccione la política de acceso de grupo definida en el paso 2.
   e. Repita este procedimiento para cada usuario del grupo de ventas.

Conceptos relacionados

"Configuración de una política de acceso de grupo" en la página 64
La carpeta **Políticas de acceso de grupo**, en 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.

"Soporte de políticas de grupo" en la página 4
Con el soporte de políticas de grupo, los administradores de red pueden definir políticas de grupo basadas en usuarios para gestionar recursos. Pueden asignarse políticas de control de acceso a usuarios individuales cuando inician una sesión de protocolo punto a punto (PPP) o una sesión L2TP (Layer Two Tunneling Protocol).

Tareas relacionadas

"Creación de un perfil de conexión" en la página 50
El primer paso para configurar una conexión PPP entre sistemas consiste en crear un perfil de conexión en el sistema.

"Aplicación de reglas de filtrado de paquetes IP a una conexión PPP" en la página 65
Puede utilizar un archivo de reglas de paquete para restringir el acceso de un usuario o un grupo a las direcciones IP de la red.

Referencia relacionada

"Lista de validación" en la página 49
Las listas de validación sirven para almacenar información de ID de usuario y contraseña perteneciente a los usuarios remotos.

"Autenticación del sistema" en la página 46
Las conexiones PPP con una plataforma System i dan soporte a varias opciones para autenticar los clientes remotos que acceden telefónicamente al sistema y las conexiones que se establecen con un ISP u otro sistema al que esté accediendo telefónicamente el sistema.

Información relacionada

Filtrado de IP y conversión de direcciones de red

Caso práctico: compartimiento de un módem entre particiones lógicas utilizando L2TP

Tiene configurado Ethernet virtual en cuatro particiones lógicas. Desea que las particiones lógicas seleccionadas compartan un módem para acceder a una LAN externa.

Situación

Usted es el administrador del sistema en una empresa de tamaño medio. Es hora de actualizar el equipo informático, pero le gustaría hacer mucho más que esto; desea agilizar el hardware. Empieza el proceso consolidando el trabajo de tres sistemas antiguos en un sistema nuevo. Crea tres particiones lógicas en el sistema. El sistema nuevo se proporciona con un módem interno 2793. Es el único procesador de entrada/salida (IOP) que tiene que soporta el protocolo punto a punto (PPP). También tiene un módem de soporte electrónico al cliente 7852–400 antiguo.

Solución

Múltiples sistemas y particiones pueden compartir los mismos módems para las conexiones por línea telefónica, eliminando la necesidad de que cada sistema o partición tenga su propio módem. Esto es posible si utiliza túneles L2TP y configura perfiles L2TP que permitan llamadas salientes. En la red, los túneles se crearán a través de una red Ethernet virtual y una red física. La línea física está conectada a otro sistema que comparte los módems en la red.

Detalles

En la siguiente figura se ilustran las características de la red para este caso práctico:

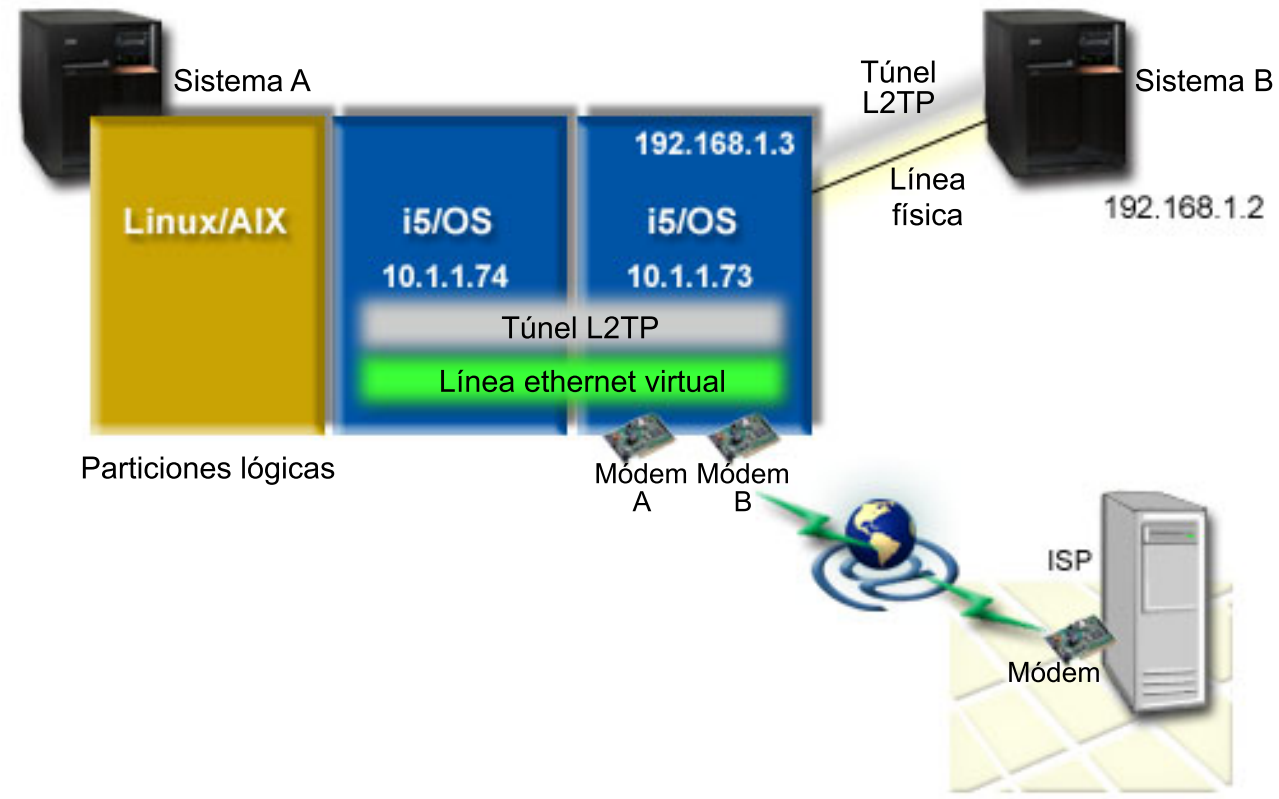


Figura 9. Múltiples sistemas que comparten el mismo módem para las conexiones por línea telefónica

Prerrequisitos y supuestos

El Sistema A debe cumplir los siguientes requisitos de configuración:

- i5/OS Versión 5 Release 3 o posterior, instalado en la partición que posee los módems con capacidad ASYNC
- Hardware que permita crear particiones.
- System i Access para Windows y System i Navigator (componente Configuración y servicio de System i Navigator), Versión 5 Release 3, o posterior,
- Ha creado como mínimo dos particiones lógicas (LPAR) en el sistema. La partición que posee el módem debe tener instalado i5/OS V5R3, o posterior. Las demás particiones pueden tener instalado OS/400 V5R2, i5/OS V5R3, Linux o AIX. En este caso práctico, las particiones utilizan el sistema operativo i5/OS o Linux.
- Ha creado una Ethernet virtual para comunicarse entre las particiones.

El Sistema B debe tener instalados el programa bajo licencia y los componentes relevantes de System i Navigator: System i Access para Windows y System i Navigator (componente Configuración y servicio de System i Navigator) V5R2, o posterior.

Información relacionada

Particiones lógicas

Detalles del caso práctico: compartimiento de un módem entre particiones lógicas utilizando L2TP

Una vez haya completado los prerrequisitos, ya puede empezar la configuración de perfiles L2TP (Layer Two Tunneling Protocol).

Paso 1: configuración del perfil de terminador L2TP para cada una de las interfaces de la partición que posee los módems:

Siga estos pasos para crear un perfil de terminador para cada interfaz:

1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servicios de acceso remoto**.
2. Pulse con el botón derecho del ratón en **Perfiles de conexión de receptor** y seleccione **Perfil nuevo**.
3. Seleccione las siguientes opciones en la página Configuración y pulse **Aceptar**:
   - **Tipo de protocolo**: PPP
   - **Tipo de conexión**: L2TP (línea virtual)
   - **Modalidad de operación**: Terminador (servidor de red)
   - **Tipo de servicio de línea**: una sola línea
4. En la pestaña **Perfil nuevo - General**, complete los siguientes campos:
   - **Nombre**: toExternal
   - **Descripción**: conexión de receptor para efectuar llamadas
   - Seleccione **Iniciar perfil con TCP/IP**.
5. En la pestaña **Perfil nuevo - Conexión**, complete los siguientes campos.
   - **Dirección IP del punto final del túnel local**: ANY
   - **Nombre de línea virtual**: toExternal. Esta línea no tiene interfaces físicas asociadas. La línea virtual describe varias características de este perfil PPP. Cuando se abra la ventana Propiedades de línea L2TP, pulse la pestaña **Autenticación** y especifique el nombre de host del sistema. Pulse **Aceptar** para regresar a la pestaña **Conexión** de la ventana Propiedades de perfil PPP nuevo.
6. Pulse **Permitir establecimiento de llamadas de salida**. Aparece el diálogo **Propiedades de llamadas salientes**.
7. En la página Propiedades de llamadas salientes, seleccione un tipo de servicio de línea.
   - **Tipo de servicio de línea**: agrupación de líneas
   - **Nombre**: dialOut
   - Pulse **Nueva**. Aparece el diálogo **Propiedades de agrupación de líneas nueva**.
8. En la ventana Propiedades de agrupación de líneas nueva, seleccione las líneas y módems en los que permitirá las llamadas salientes y pulse **Añadir**. Si necesita definir estas líneas, seleccione **Línea nueva**. Las interfaces de la partición que posee los módems intentarán utilizar cualquier línea que esté abierta de esta agrupación de líneas. Se abre la ventana Propiedades de línea nueva.
9. En la pestaña **Propiedades de línea nueva - General**, especifique información en los siguientes campos:
   - **Nombre**: line1
   - **Descripción**: primera línea y primer módem de la agrupación de líneas (módem interno 2793)
   - **Recurso de hardware**: cmn03 (puerto de comunicaciones)
10. Acepte los valores predeterminados en las demás pestañas y pulse **Aceptar** para regresar a la ventana Propiedades de agrupación de líneas nueva.
11. En la ventana Propiedades de agrupación de líneas nueva, seleccione las líneas y módems en los que permitirá las llamadas salientes y pulse **Añadir**. Verifique que se ha seleccionado el módem 2793 para la agrupación.
12. Vuelva a seleccionar **Línea nueva** para añadir el módem de soporte electrónico al cliente 7852–400. Se abre la ventana Propiedades de línea nueva.
13. En la pestaña **Propiedades de línea nueva - General**, especifique información en los siguientes campos:
    - **Nombre**: line2
    - **Descripción**: segunda línea y segundo módem de la agrupación de líneas (módem de soporte electrónico al cliente externo 7852-400)

- **Recurso de hardware**: cmn04 (puerto V.24)
- **Tramas**: Asíncrono

14. En la pestaña **Propiedades de línea nueva - Módem**, seleccione el módem externo (7852–400) y pulse **Aceptar** para regresar a la ventana Propiedades de agrupación de líneas nueva.
15. Seleccione cualquiera de las demás líneas disponibles que desea añadir a la agrupación de líneas y pulse **Añadir**. En este ejemplo, verifique que los dos módems nuevos que ha añadido antes figuran en el campo **Líneas seleccionadas para la agrupación** y pulse **Aceptar** para regresar a la ventana Propiedades de llamada de salida.
16. En la ventana Propiedades de llamada de salida, especifique los `Números de llamada predeterminados` y pulse **Aceptar** para regresar a la ventana Propiedades del perfil PPP nuevo.

    Nota: estos números pueden ser como una especie de proveedor de servicios de Internet (ISP), a los que los demás sistemas llamarán frecuentemente utilizando estos módems. Si los demás sistemas especifican un número de teléfono *PRIMARY o *BACKUP, los números que realmente se marcarán serán los que aquí se especifiquen. Si los demás sistemas especifican un número de teléfono real, se utilizará dicho número de teléfono.
17. En la pestaña **Valores de TCP/IP**, seleccione los siguientes valores:
    - **Dirección IP local**: Ninguna
    - **Dirección IP remota**: Ninguna

    Nota: Si desea utilizar el perfil para finalizar las sesiones L2TP, deberá elegir la dirección IP local que representa el sistema. En el caso de la dirección IP remota, puede seleccionar una agrupación de direcciones que se encuentre en la misma subred que el sistema. Todas las sesiones L2TP obtienen sus direcciones IP de esta agrupación.
18. En la pestaña **Autenticación**, acepte todos los valores predeterminados.

De este modo finaliza la configuración de un perfil de terminador L2TP en la partición con módems. El siguiente paso consiste en configurar un perfil originador de llamada remota L2TP para 10.1.1.74.

Referencia relacionada

"Soporte para perfiles de múltiples conexiones" en la página 57
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.

Paso 2: configuración de un perfil de originador L2TP en 10.1.1.74:

Estos pasos le ayudarán a crear un perfil de originador L2TP (Layer Two Tunneling Protocol):

1. En System i Navigator, expanda **10.1.1.74** → **Red** → **Servicios de acceso remoto**.
2. Pulse con el botón derecho del ratón en **Perfiles de conexión de originador** y seleccione **Perfil nuevo**.
3. Seleccione las siguientes opciones en la página Configuración y pulse **Aceptar**:
   - **Tipo de protocolo**: PPP
   - **Tipo de conexión**: L2TP (línea virtual)
   - **Modalidad de operación**: llamada remota
   - **Tipo de servicio de línea**: una sola línea
4. En la pestaña **General**, complete los siguientes campos:
   - **Nombre**: toModem
   - **Descripción**: conexión de originador con la partición que tiene el módem
5. En la pestaña **Conexión**, complete los siguientes campos:

   Nombre de línea virtual: toModem. Esta línea no tiene ninguna interfaz física asociada. La línea virtual describe varias características de este perfil PPP. Se abre la ventana Propiedades de línea L2TP.

6. En la pestaña **General**, entre una descripción para la línea virtual.
7. En la pestaña **Autenticación**, especifique el nombre de host de la partición y pulse **Aceptar** para regresar a la página Conexión.
8. En el campo **Números de teléfono remotos**, añada `*PRIMARY` y `*BACKUP`. Esto permite al perfil utilizar los mismos números de teléfono que el perfil de terminador existente en la partición que posee los módems.
9. En el campo **Nombre o dirección IP del host de punto final del túnel remoto**, especifique la dirección IP del punto final del túnel remoto (`10.1.1.73`).
10. En la pestaña **Autenticación**, seleccione **Permitir al sistema remoto verificar la identidad de este servidor iSeries**.
11. En el Protocolo de autenticación que debe utilizarse, seleccione **Se necesita contraseña cifrada (CHAP-MD5)**. De forma predeterminada también se selecciona **Permitir protocolo de autenticación extensible**.

    Nota: el protocolo debe coincidir con el que utiliza el sistema al que llamará.
12. Entre el nombre del usuario y su contraseña.

    Nota: el nombre de usuario y la contraseña deben coincidir con el nombre de usuario y la contraseña válidos en el sistema al que llamará.
13. Vaya a la pestaña **Valores TCP/IP** y verifique los campos necesarios:
    - **Dirección IP local**: asignada por el sistema remoto
    - **Dirección IP remota**: asignada por el sistema remoto
    - **Direccionamiento**: no se necesita ningún direccionamiento adicional
14. Pulse **Aceptar** para guardar el perfil PPP.

Paso 3: configuración de un perfil de llamada remota L2TP para 192.168.1.2:

Para configurar un perfil de llamada remota L2TP (Layer Two Tunneling Protocol) para 192.168.1.2, repita el Paso 2 y cambie el punto final del túnel remoto por 192.168.1.3 (la interfaz física a la que se conecta el sistema B).

Nota: estas direcciones IP son ficticias y solo se utilizan a efectos ilustrativos.

Paso 4: prueba de la conexión:

Una vez se han configurado los dos sistemas, debe probar la conectividad para asegurarse de que los sistemas comparten el módem para alcanzar redes externas.

1. Compruebe que el perfil de terminador de L2TP (Layer Two Tunneling Protocol) esté activo.
   a. En System i Navigator, expanda **10.1.1.73 → Red → Servicios de acceso remoto → Perfiles de conexión de receptor**.
   b. En el panel derecho, busque el perfil que necesite (toExternal) y verifique que el campo **Estado** es Activo. En caso contrario, con el botón derecho del ratón pulse en el perfil y seleccione **Iniciar**.
2. Inicie el perfil de llamada remota de 10.1.1.74.
   a. En System i Navigator, expanda **10.1.1.74 → Red → Servicios de acceso remoto → Perfiles de conexión de originador**.
   b. En el panel derecho, busque el perfil que necesite (toModem) y verifique que el campo **Estado** es Activo. En caso contrario, con el botón derecho del ratón pulse en el perfil y seleccione **Iniciar**.
3. Inicie el perfil de llamada remota de System B.
   a. En System i Navigator, expanda **192.168.1.2 → Red → Servicios de acceso remoto → Perfiles de conexión de originador**.

b. En el panel derecho, busque el perfil que ha creado y verifique que el campo **Estado** es Activo. En caso contrario, con el botón derecho del ratón pulse en el perfil y seleccione **Iniciar**.

4. Si es posible, efectúe un PING con el proveedor de servicios de Internet (ISP) u otro destino al que haya llamado para verificar que ambos perfiles están activos. Efectuará el mandato PING tanto desde 10.1.1.74 como desde 192.168.1.2.
5. Como alternativa, también puede comprobar el estado de la conexión.
   a. En System i Navigator, expanda **el sistema** → **Red** → **Servicios de acceso remoto** → **Perfiles de conexión de originador**.
   b. En el panel derecho, con el botón derecho del ratón pulse el perfil que ha creado y seleccione **Conexiones**. En la ventana Estado de la conexión puede ver los perfiles que están activos, inactivos, conectándose, etc.

Planificación de PPP

La planificación del Protocolo punto a punto (PPP) incluye la creación y la administración de conexiones PPP.

Referencia relacionada

"Caso práctico: conexión de clientes de acceso telefónico remoto al sistema" en la página 13
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 sistema con protocolo punto a punto (PPP).

"Caso práctico: conexión de la LAN de oficina a Internet con un módem" en la página 16
Normalmente, los administradores configuran redes de oficina que permiten a los empleados acceder a Internet. Los administradores pueden utilizar un módem para conectar el sistema a un proveedor de servicios de Internet (ISP). Los clientes PC conectados a la LAN pueden comunicarse con Internet utilizando el sistema operativo i5/OS como pasarela.

"Información relacionada con los Servicios de acceso remoto" en la página 70
Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas Servicios de acceso remoto. Puede ver o imprimir los archivos PDF que desee.

Requisitos de software y de hardware

En un entorno de protocolo punto a punto (PPP) se necesitan dos o más máquinas que den soporte a PPP. Una de esas máquinas, la plataforma System i, puede ser el originador o el receptor.

El sistema debe satisfacer los siguientes prerrequisitos para que los sistemas remotos puedan acceder a él:

- System i Navigator 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 System i Access para Windows 95 o posterior con System i 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).
  - 2742*: adaptador de E/S de dos líneas (sustituye al IOA 2745).

- 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.
- 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A/576A: adaptador Ethernet para conexiones PPPoE.
- 2793/576C: adaptador de E/S de WAN de dos puertos, con un módem integrado V.92 en el puerto 1 y una interfaz de comunicaciones estándar en el puerto 2. Para utilizar el puerto 2, se necesita un módem externo o un adaptador de terminal RDSI con el cable apropiado.
- 2805: adaptador de E/S de WAN de cuatro puertos, con un módem analógico V.92 integrado. Sustituye a los modelos 2761 y 2772.

* Para estos adaptadores se necesita un módem externo V.90 (o superior), o un adaptador de terminal de red digital de servicios integrados (RDSI), y un cable RS-232 (EIA 232) o compatible.

- 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.

Referencia relacionada

"Perfiles de conexión" en la página 2
Los perfiles de conexión punto a punto definen un conjunto de parámetros y recursos para las conexiones de protocolo punto a punto (PPP) específicas. Puede iniciar perfiles que utilizan estos valores de parámetro para acceder por llamada telefónica a las conexiones PPP (originar) o bien para estar a la escucha de ellas (recibir).

"Módems" en la página 41
Para las conexiones de protocolo punto a punto (PPP) se pueden emplear tanto los módems externos como los internos.

"CSU/DSU" en la página 41
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.

"Adaptadores de terminal RDSI" en la página 42
La Red digital de servicios integrados (RDSI) proporciona una conexión digital que le permite comunicarse mediante cualquier combinación de voz, datos y vídeo, entre otras aplicaciones multimedia.

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 (Control de enlace de datos de alto nivel) para encapsular los datagramas a través de enlaces de telecomunicaciones punto a punto tanto asíncronos como síncronos.

PPP da soporte a una amplia gama de tipos de enlaces, mientras que el protocolo Internet de línea serie (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 host 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

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), se basan normalmente 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 hasta los 56 kbps 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 RS-232 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.

Una de las ventajas que tiene el estándar V.92 sobre el estándar V.90 es que permite velocidades en sentido ascendente que alcanzan los 48 kbps. Además, los tiempos de conexión pueden verse reducidos a causa de las mejoras realizadas en el proceso de establecimiento de enlace y los módems que tienen la función de retención de llamada pueden ahora permanecer conectados mientras la línea telefónica acepta una llamada entrante o utiliza el estado de llamada en espera.

Servicios digitales y Servicios de datos digitales

Puede utilizar servicios digitales y Servicios de datos digitales (DDS) con el protocolo punto a punto (PPP).

Servicio digital

Con el servicio digital, los datos viajan todo el tiempo con formato digital cuando van desde 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. 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.

Servicios de datos digitales

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 caso práctico 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 9.000 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, se recomienda Conmutada-56. 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.

Referencia relacionada

"CSU/DSU" en la página 41
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.

"Conmutado-56"
Si no necesita una conexión a todo tiempo, podrá ahorrarse dinero si utiliza el servicio digital conmutado, que suele llamarse *Conmutada-56 (SW56)*.

Conmutado-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 servicios de datos digitales (DDS) en que el equipo terminal de datos (DTE) se conecta al servicio digital por medio de una unidad de servicios de canal/unidad de servicios de datos de CSU/DSU. Sin embargo, una CSU/DSU de SW56 incluye un área de marcación en la que se entra el número de teléfono del host remoto. Puede utilizar SW56 para hacer conexiones digitales de acceso telefónico con cualquier otro abonado a SW56 en la región 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 existe únicamente 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.

Referencia relacionada

"Servicios digitales y Servicios de datos digitales" en la página 35
Puede utilizar servicios digitales y Servicios de datos digitales (DDS) con el protocolo punto a punto (PPP).

"Red digital de servicios integrados"
La Red digital de servicios integrados (RDSI) proporciona una conectividad digital conmutada de extremo a extremo. RDSI puede transportar voz y datos a través de una misma conexión.

Red digital de servicios integrados

La Red digital de servicios integrados (RDSI) proporciona una conectividad digital conmutada de extremo a extremo. 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 5.400 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 RS-232 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 había 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. Esta posibilidad 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. Con esta tecnología, un adaptador de terminal también puede operar como el lado del sistema digital de los clientes V.92.

Normalmente, deberá conectarse a un adaptador de terminal RDSI a través de una interfaz serie RS-232 mediante un protocolo asíncrono a velocidades de hasta 230,4 kbps. Sin embargo, la velocidad máxima en baudios del sistema para el protocolo asíncrono a través de RS-232 es de 115,2 kbps. Lamentablemente, esto hace que la velocidad máxima de transferencia de bytes quede restringida a 11,5 kbps, mientras que el adaptador de terminal con multienlace tiene capacidad para 14 o 16 KB sin comprimir. Algunos adaptadores de terminal dan soporte al protocolo síncrono a través de RS-232 a 128 kbps, pero la velocidad máxima en baudios del sistema para el protocolo síncrono a través de RS-232 es de 64 kbps.

El sistema tiene capacidad para ejecutar el protocolo 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 una interfaz RS-232 en una interfaz V.35 pueden ser una solución razonable del problema, pero este enfoque no ha sido evaluado para el sistema. 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.

Referencia relacionada

"Conmutado-56" en la página 36
Si no necesita una conexión a todo tiempo, podrá ahorrarse dinero si utiliza el servicio digital conmutado, que suele llamarse *Conmutada-56 (SW56)*.

"Adaptadores de terminal RDSI" en la página 42
La Red digital de servicios integrados (RDSI) proporciona una conexión digital que le permite comunicarse mediante cualquier combinación de voz, datos y vídeo, entre otras aplicaciones multimedia.

Conexiones T1/E1 y T1 fraccionaria

T1/E1 y T1 fraccionaria son dos tipos de alternativas de conexión válidas.

T1/E1

Una conexión T1 es un paquete compuesto por 24 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 32 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 los demás canales para la conectividad de 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 de unidad de servicios de canal/unidad de servicios de datos (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 que llegan a alcanzar 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 proveedores de servicios de Internet (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 una 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 IP (identificador de conexión de enlace de datos) de la trama y a gestionar la ruta o la conexión virtual.

En Estados Unidos, las redes frame relay soportan las velocidades de transferencia de datos propias de las líneas T1 (1,544 mbps) y T3 (45 mbps). Podríamos decir que frame relay es una manera de utilizar las líneas T1 y T3 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 T1. (En Europa, las velocidades de frame relay varían de 64 kbps a 2 mbps. En 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 la modalidad de transferencia asíncrona (ATM).

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).

Layer Two Tunneling Protocol

Al utilizar túneles L2TP (Layer Two Tunneling Protocol), es posible separar la ubicación en la que finaliza el protocolo de acceso telefónico y donde se proporciona el acceso a la red. Es por ello por lo que L2TP también se conoce como *PPP virtual*.

Estas figuras ilustran tres implementaciones de túneles de L2TP.

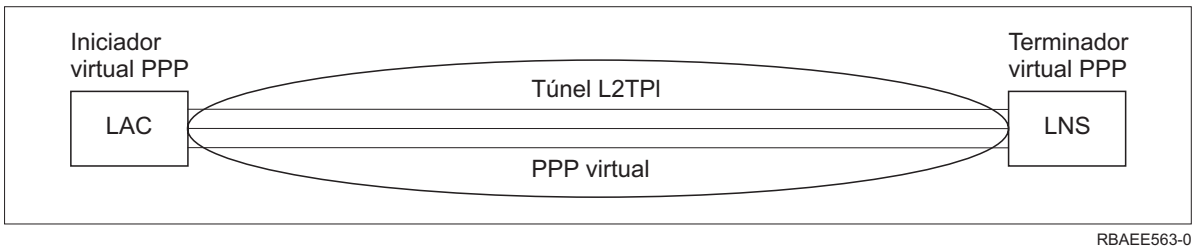


Figura 10. Iniciador de marcación PPP o terminador virtual PPP

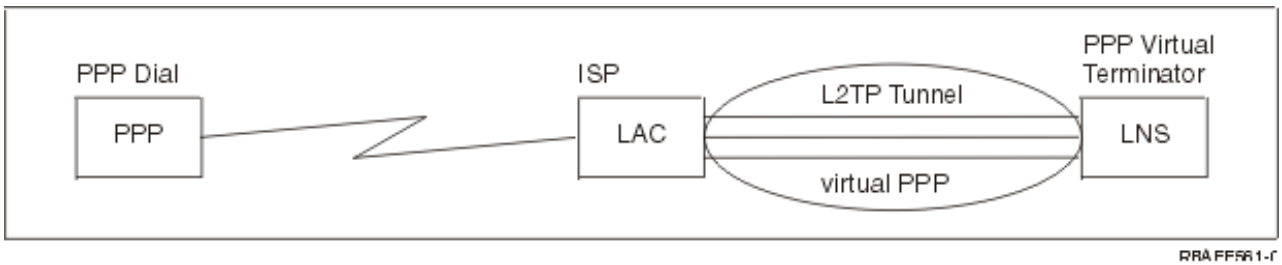


Figura 11. Iniciador de marcación PPP o terminador virtual PPP

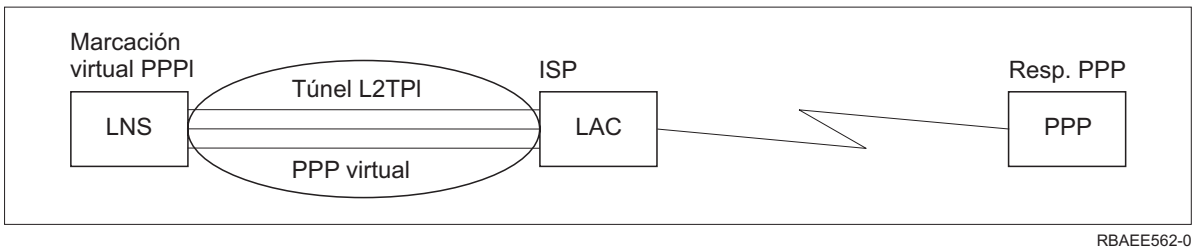


Figura 12. Marcación virtual PPP o respuesta virtual PPP

El protocolo L2TP viene documentado como petición de comentarios estándar RFC-2661. El túnel L2TP puede extenderse para que abarque toda una sesión PPP o solo uno de los dos segmentos de que consta una sesión. Ello da lugar a cuatro modelos de túneles.

Información relacionada

Caso práctico: protección de un túnel voluntario L2TP con IPSec

RFC Editor

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 (Layer Two Tunneling Protocol).

Como resultado, el usuario envía paquetes L2TP al proveedor de servicios de Internet (ISP), que los reenvía al servidor de red L2TP (LNS). En los túneles voluntarios, el ISP no necesita dar soporte a L2TP, y el iniciador del túnel L2TP está en el mismo sistema que el cliente remoto. En este modelo, el túnel atraviesa toda la sesión de protocolo punto a punto (PPP), desde el cliente L2TP al LNS.

Modelo de túnel forzoso - llamada entrante:

En el modelo de túnel forzoso (llamada entrante), se crea un túnel sin ninguna acción por parte del usuario y sin que el usuario pueda escoger.

Como resultado, el usuario envía paquetes de protocolo punto a punto a LAC (Concentrador de acceso L2TP (Layer Two Tunneling Protocol)) del proveedor de servicios de Internet (ISP). ISP encapsula los paquetes en L2TP y los envía en un túnel al servidor de red L2TP (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 (marcación remota), la pasarela local (servidor de red L2TP (LNS)) inicia un túnel hasta un proveedor de servicios de Internet (ISP) (LAC) e indica al ISP que haga una llamada local para el cliente de respuesta de protocolo punto a punto (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 (Layer Two Tunneling Protocol) es una manera de redirigir el tráfico L2TP en nombre de los concentradores de acceso L2TP (LAC) cliente y los servidores de red L2TP (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 funciona 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 PPPoE (DSL) para conexiones PPP

La *Línea de abonado digital (DSL)* hace referencia a una clase de tecnología empleada para obtener más ancho de banda a través del cableado telefónico de cobre que hay entre el local de un cliente y un proveedor de servicios de Internet (ISP).

DSL permite servicios simultáneos de voz y datos de alta velocidad a través de un único par de hilos telefónicos de cobre. Las velocidades del módem han aumentado gradualmente por medio de diversas técnicas, entre ellas las de compresión, pero las velocidades más altas de hoy en día (56 kbps) están alcanzando el límite teórico que admite esta tecnología. La tecnología DSL permite velocidades mucho más altas a través de líneas de par trenzado entre la oficina central y las casas particulares, la escuela o la empresa. En algunas zonas pueden alcanzarse velocidades de hasta 2 Mbps. El protocolo PPP se utiliza normalmente en las comunicaciones en serie como las de las conexiones telefónicas por módem. Ahora,

muchos proveedores de servicios de Internet que proporcionan DSL utilizan PPP por Ethernet (PPPoE) por sus funciones adicionales de seguridad y conexión.

Llamamos *módem DSL* a un dispositivo situado en cada extremo de una línea telefónica de cobre que permite a un sistema (o a una LAN) conectarse a Internet por medio de una conexión DSL. A diferencia de lo que ocurre en una conexión por línea telefónica, para DSL no se necesita normalmente una línea telefónica dedicada (hay un discriminador POTS que permite compartir la línea de manera simultánea). Si bien los módems DSL se parecen a los módems analógicos convencionales, su productividad es mucho mayor.

Equipo de conexión

El sistema utiliza módems, adaptadores de terminal de red digital de servicios integrados (RDSI), adaptadores Token-ring, adaptadores Ethernet o dispositivos de unidad de servicios de canal/unidad de servicios de datos (CSU/DSU) para manejar las conexiones de protocolo punto a punto (PPP).

Hay cuatro clases de equipo de comunicaciones que se pueden utilizar con el entorno PPP:

- Módems
- CSU/DSU
- Adaptadores de terminal RDSI
- Adaptadores Ethernet (para las conexiones PPPoE)

Módems

Para las conexiones de protocolo punto a punto (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 sistema tiene predefinidos numerosos modelos de módem, pero se pueden definir nuevos modelos con System i 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 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 que se incluye con el sistema para establecer conexiones PPP. En los sistemas más antiguos, el módem de soporte electrónico al cliente era un módem externo IBM 7852-400. Este módem se ha sustituido por el módem MultiTech MT5600BA-V92 V.92 Data/Fax World. En los sistemas más recientes, se pueden emplear el 2771, 2793 o cualquiera de los demás módems internos soportados como módem de soporte electrónico al cliente.

Referencia relacionada

"Requisitos de software y de hardware" en la página 33
En un entorno de protocolo punto a punto (PPP) se necesitan dos o más máquinas que den soporte a PPP. Una de esas máquinas, la plataforma System i, puede ser el originador o el receptor.

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.

Referencia relacionada

"Requisitos de software y de hardware" en la página 33
En un entorno de protocolo punto a punto (PPP) se necesitan dos o más máquinas que den soporte a PPP. Una de esas máquinas, la plataforma System i, puede ser el originador o el receptor.

"Servicios digitales y Servicios de datos digitales" en la página 35
Puede utilizar servicios digitales y Servicios de datos digitales (DDS) con el protocolo punto a punto (PPP).

Adaptadores de terminal RDSI

La Red digital de servicios integrados (RDSI) proporciona una conexión digital que le permite comunicarse mediante cualquier combinación de voz, datos y vídeo, entre otras aplicaciones multimedia.

Debe verificar que las características del adaptador de terminal son las adecuadas para utilizarlo en el sistema.

Para configurar el adaptador de terminal, siga estos pasos:

1. En System i Navigator, seleccione su sistema y expanda **Red → Servicios de acceso remoto**.
2. Pulse **Módems** con el botón derecho del ratón y seleccione **Módem nuevo**.
3. En el diálogo **Propiedades de módem nuevo**, entre los valores correctos en todos los recuadros de **campo** 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 las propiedades de RDSI para que coincidan con las propiedades que necesita el adaptador de terminal.

Tareas relacionadas

"Ejemplo: configuración de un adaptador de terminal RDSI" en la página 61
En el ejemplo se muestra cómo configurar un adaptador de terminal de red digital de servicios integrados (RDSI).

Referencia relacionada

"Requisitos de software y de hardware" en la página 33
En un entorno de protocolo punto a punto (PPP) se necesitan dos o más máquinas que den soporte a PPP. Una de esas máquinas, la plataforma System i, puede ser el originador o el receptor.

"Red digital de servicios integrados" en la página 37
La Red digital de servicios integrados (RDSI) proporciona una conectividad digital conmutada de extremo a extremo. RDSI puede transportar voz y datos a través de una misma conexión.

Sugerencias sobre adaptadores de terminal RDSI:

Puede utilizar varios adaptadores de terminal diferentes.

El adaptador de terminal de red digital de servicios integrados (RDSI) externo recomendado es el módem **3Com/U.S. Robotics Courier I RDSI V.x** (siendo x un número). Soporta conexiones de módem analógico V.34, V.90 (X2), V.92 y PPP multienlace a través de RDSI, en las modalidades de origen y respuesta en el sistema. También soporta automáticamente el protocolo de autenticación de reconocimiento de identificación (CHAP) a través de la conexión PPP de RDSI. Están disponibles asimismo los siguientes adaptadores de terminal RDSI: Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA y ADtran ISU 2x64 Puerto Dual.

- **Conexiones con origen en el sistema.** 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 sistema. Las respuestas de PAP no aparecen en la conexión RDSI.
- **Conexiones a las que responde el sistema.** El adaptador de terminal Courier I exige la autenticación CHAP por parte del lado llamante si la configuración de respuesta hace que el sistema abra la autenticación con una petición de identificación CHAP. Si el sistema 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 sistema 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 ser de suministradores de terceros, aunque tal vez pueda encontrar algunas versiones V.53 en suministradores de terceros. La versión RS-232 aún está recomendada en el sistema, a expensas de una ligera reducción del rendimiento, ya que las conexiones de RS-232 están limitadas a 115,2 KB.

Asegúrese de establecer en el sistema la velocidad de línea de V.35 en 230,4 kbps.

Restricciones de los adaptadores de terminal RDSI:

Los adaptadores de terminal de este tema se han evaluado. Estos adaptadores solo están recomendados para las conexiones de red digital de servicios integrados (RDSI) remotas con origen en el sistema.

3Com Impact IQ RDSI:

Este adaptador de terminal no está recomendado para la plataforma System i 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 estar conectado al sistema 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). Si establece S84 en 0, se ejecuta la autenticación CHAP.
- El sistema 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 la plataforma System i 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 estar conectado al sistema 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.

- 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 no funciona bien con este adaptador de terminal. Esto produce una reducción del rendimiento cuando el sistema envíe datos a través de una conexión PPP multienlace.

Manejo de las direcciones IP

Las conexiones del protocolo punto a punto (PPP) permiten utilizar varios juegos de opciones para gestionar direcciones IP en función del tipo de perfil de conexión.

- DHCP puede gestionar centralmente las asignaciones de dirección IP para la red. Este tema le enseñará a configurar y a gestionar los servicios DHCP en la red. Consulte Protocolo de configuración dinámica de hosts
- DNS puede ayudarle a gestionar los nombres de host y las direcciones IP asociadas. Este tema le enseñará a configurar y a gestionar los servicios DNS en la red. Consulte Sistema de nombres de dominio
- BOOTP permite asociar las estaciones de trabajo cliente al sistema, y asignarles direcciones IP. Este tema le enseñará a configurar y a gestionar los servicios BOOTP en la red. Consulte Protocolo de programa de arranque

Referencia relacionada

"Caso práctico: conexión del sistema a un concentrador de acceso PPPoE" en la página 10
Muchos proveedores de servicios de Internet (ISP) ofrecen acceso a Internet de alta velocidad a través de una Línea de abonado digital (DSL) utilizando el protocolo punto a punto por Ethernet (PPPoE). Puede conectar el sistema a estos ISP para proporcionar conexiones con un amplio ancho de banda que conserven las ventajas del protocolo punto a punto (PPP).

Filtrado de paquetes IP

El filtrado de paquetes IP limita los servicios que se prestan a usuarios individuales cuando inician una sesión en una red.

El filtrado de paquetes puede permitir o denegar el acceso según las direcciones IP de destino o los puertos, o ambos. 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 aplicará 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 Reglas de paquetes IP, en System i Navigator.

En el caso de las conexiones L2TP, hay que usar VPN con el filtrado IPSec para proteger el tráfico de red.

Referencia relacionada

"Caso práctico: conexión del sistema a un concentrador de acceso PPPoE" en la página 10
Muchos proveedores de servicios de Internet (ISP) ofrecen acceso a Internet de alta velocidad a través de una Línea de abonado digital (DSL) utilizando el protocolo punto a punto por Ethernet (PPPoE). Puede conectar el sistema a estos ISP para proporcionar conexiones con un amplio ancho de banda que conserven las ventajas del protocolo punto a punto (PPP).

Información relacionada

Filtrado de IP y conversión de direcciones de red

Redes privadas virtuales (VPN)

Estrategia de gestión de direcciones IP

Antes de configurar un perfil de conexión PPP, conviene que conozca bien su estrategia de gestión de direcciones IP. Esta estrategia afecta a muchas de las decisiones que deberá tomar durante el proceso de configuración, entre ellas las estrategias de autenticación, las consideraciones sobre seguridad y los valores de TCP/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, debe asegurarse de que el sistema remoto esté definido para aceptar las direcciones IP que ha definido. Lo que hace una aplicación típica es definir la dirección IP 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 IP como procedimiento para averiguar la dirección IP 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 sistema se conecta a Internet a través de un ISP, esto puede permitir que una red conectada detrás del sistema acceda a Internet. Básicamente, el sistema oculta las direcciones IP de los sistemas de la red detrás de la dirección IP local asignada por el ISP, haciendo así que todo el tráfico IP proceda en apariencia del sistema. 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 sistema), y para el sistema en el que tendrá que habilitar el recuadro **Añadir sistema remoto como ruta predeterminada**.

Perfiles de conexión de receptor

Para los perfiles de conexión de receptor se deben tener en cuenta muchas más consideraciones y opciones sobre las direcciones IP que para los perfiles de conexión de originador. A la hora de configurar las direcciones IP debe tener en cuenta el plan de gestión de direcciones IP de la red, los requisitos de rendimiento y funcionales específicos de esta conexión y el plan de seguridad.

Direcciones IP locales

En el caso de un perfil de receptor individual, puede definir una dirección IP exclusiva o bien utilizar una dirección IP local existente en el sistema para identificar el final de la conexión PPP. 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. Si no hay direcciones IP locales ya existentes, podrá crear una dirección IP virtual con esta finalidad.

Direcciones IP remotas

Existen muchas opciones para asignar direcciones IP remotas a los clientes PPP. A continuación figuran las opciones que se pueden especificar en la página TCP/IP del perfil de conexión de receptor.

Nota: si quiere que el sistema remoto forme parte de la LAN, deberá configurar el direccionamiento de direcciones IP, especificar una dirección IP comprendida en el rango de direcciones IP de los sistemas conectados a la LAN y verificar que el reenvío de IP está habilitado para este perfil de conexión y para el sistema.

Tabla 8. Opciones de asignación de direcciones IP para las conexiones de perfil de receptor

Opción	Descripción
Dirección IP fija	Se define la dirección IP individual que se ha de dar a los usuarios remotos cuando se conectan por línea telefónica. Es una dirección IP solo de host (la máscara de subred es 255.255.255.255) y solamente está destinada 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 IP exclusiva que esté comprendida dentro del rango definido. Es una dirección IP solo de host (la máscara de subred es 255.255.255.255) y solamente está destinada 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 es válida 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 directamente por el servidor DHCP o indirectamente por medio de la retransmisión DHCP. Esta opción solo es válida 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 host (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.
Definir direcciones IP adicionales basándose en el ID de usuario del sistema remoto	Esta opción le permite definir direcciones IP 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 IP Dirección IP fija y Agrupación de direcciones. Cuando un usuario remoto se conecta al sistema, 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 IP, la máscara y un conjunto de posibles rutas para esa conexión. Si el usuario no está definido, la dirección IP tomará de forma predeterminada la dirección IP fija definida o la próxima dirección IP 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.
Direccionamiento de direcciones IP	El cliente que accede por línea telefónica y el sistema deben tener debidamente configurado el direccionamiento de las direcciones IP si el cliente tiene que acceder a direcciones IP de la LAN a la que pertenece el sistema.

Autenticación del sistema

Las conexiones PPP con una plataforma System i dan soporte a varias opciones para autenticar los clientes remotos que acceden telefónicamente al sistema y las conexiones que se establecen con un ISP u otro sistema al que esté accediendo telefónicamente el sistema.

El sistema da soporte a varios métodos para mantener información de autenticación. Estos métodos incluyen desde simples listas de validación en el sistema que contienen listas de usuarios autorizados y las contraseñas, hasta el soporte de servidores RADIUS (Remote Authentication Dial In User Service). Los servidores RADIUS mantienen información detallada de usuarios de red. El sistema también da soporte a varias opciones para cifrar información de ID de usuario y contraseñas, que van desde el simple intercambio de contraseñas hasta el soporte con el protocolo de autenticación de reconocimiento de identificación (CHAP-MD5). Podrá especificar sus preferencias para la autenticación del sistema, incluyendo un ID de usuario y una contraseña para validar el sistema cuando acceda telefónicamente, en la pestaña **Autenticación** del perfil de conexión, en System i Navigator.

Referencia relacionada

"Caso práctico: conexión del sistema a un concentrador de acceso PPPoE" en la página 10
Muchos proveedores de servicios de Internet (ISP) ofrecen acceso a Internet de alta velocidad a través de una Línea de abonado digital (DSL) utilizando el protocolo punto a punto por Ethernet (PPPoE). Puede conectar el sistema a estos ISP para proporcionar conexiones con un amplio ancho de banda que conserven las ventajas del protocolo punto a punto (PPP).

"Caso práctico: autenticación de conexiones por línea telefónica con NAS de RADIUS" en la página 22
Un servidor de acceso a red (NAS) que se esté ejecutando en el sistema puede direccionar las peticiones de autenticación desde los clientes de acceso telefónico a un servidor RADIUS (Remote Authentication Dial In User Service) aparte. Si la autenticación es satisfactoria, el servidor RADIUS también puede controlar las direcciones IP asignadas al usuario.

"Caso práctico: gestión del acceso de usuarios remotos a los recursos mediante las políticas de grupo y el filtrado de IP" en la página 24
Las políticas de acceso de grupo identifican los distintos grupos de usuarios de una conexión y permiten aplicar atributos de conexión comunes y valores de seguridad a todo el grupo. Puede utilizar políticas de grupo, junto con el filtrado de IP, para permitir y restringir el acceso a direcciones IP específicas de la red.

Protocolo de autenticación de reconocimiento de identificación con MD5

El Protocolo de autenticación de reconocimiento de identificación (CHAP-MD5) 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 el protocolo de autenticación de contraseñas (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. La autenticación queda reconocida si los valores coinciden; en caso contrario, se finaliza la conexión.

Referencia relacionada

"Caso práctico: conexión de clientes de acceso telefónico remoto al sistema" en la página 13
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 sistema con protocolo punto a punto (PPP).

"Protocolo de autenticación de contraseñas" en la página 48
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.

Protocolo de autenticación extensible

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 con dispositivos de seguridad de terceros. EAP protege las redes privadas virtuales (VPN) seguras contra los piratas informáticos que realizan ataques mediante diccionario y adivinan contraseñas. EAP ofrece más ventajas que el Protocolo de autenticación de contraseñas (PAP) y el protocolo de autenticación de reconocimiento de identificación (CHAP).

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

El sistema no da soporte directamente a EAP. Sin embargo, se puede utilizar la autenticación remota con un servidor RADIUS (Remote Authentication Dial In User Service) que dé soporte a algunos de los esquemas de autenticación adicionales descritos anteriormente.

Protocolo de autenticación de contraseñas

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 lleva a cabo 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 de autenticación de reconocimiento de identificación (CHAP) siempre que sea posible.

Referencia relacionada

"Protocolo de autenticación de reconocimiento de identificación con MD5" en la página 47
El Protocolo de autenticación de reconocimiento de identificación (CHAP-MD5) emplea un algoritmo (MD-5) para calcular un valor que solo conocen el sistema que autentica y el dispositivo remoto.

Visión general de RADIUS (Remote Authentication Dial In User Service)

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 sistema, 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 sistema) pueda prestar servicios autorizados al usuario autenticado que accede por llamada telefónica.

Si no es posible establecer contacto con un servidor RADIUS, el sistema puede direccionar las peticiones de autenticación a un servidor alternativo. Ello permite a las empresas globales prestar a los correspondientes usuarios un servicio de acceso por llamada telefónica 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; a continuación, 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. Podría ser un sistema de archivos de contraseña UNIX, Kerberos, un sistema de seguridad comercial o incluso un sistema de seguridad desarrollado de manera personalizada. El servidor RADIUS devuelve al sistema los

servicios que el usuario autenticado esté autorizado a utilizar, como podría ser una dirección IP. Las peticiones de contabilidad RADIUS se manejan de forma parecida. 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.

Referencia relacionada

"Caso práctico: autenticación de conexiones por línea telefónica con NAS de RADIUS" en la página 22
Un servidor de acceso a red (NAS) que se esté ejecutando en el sistema puede direccionar las peticiones de autenticación desde los clientes de acceso telefónico a un servidor RADIUS (Remote Authentication Dial In User Service) aparte. Si la autenticación es satisfactoria, el servidor RADIUS también puede controlar las direcciones IP asignadas al usuario.

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.

Referencia relacionada

"Caso práctico: gestión del acceso de usuarios remotos a los recursos mediante las políticas de grupo y el filtrado de IP" en la página 24
Las políticas de acceso de grupo identifican los distintos grupos de usuarios de una conexión y permiten aplicar atributos de conexión comunes y valores de seguridad a todo el grupo. Puede utilizar políticas de grupo, junto con el filtrado de IP, para permitir y restringir el acceso a direcciones IP específicas de la red.

Consideraciones sobre el ancho de banda para multienlace

Puede ocurrir que en algunas ocasiones, aunque no en todas, se necesite más ancho de banda para completar algunas tareas.

Puede no estar justificada la adquisición de hardware especializado y de líneas de comunicaciones de precio elevado. El protocolo multienlace (MP) PPP agrupa múltiples enlaces PPP para formar un solo enlace virtual o paquete compuesto. La agregación de múltiples enlaces aumenta el ancho de banda efectivo total entre dos sistemas si se utilizan módems y líneas telefónicas estándar. Se pueden incluir hasta seis enlaces en un paquete compuesto MP. 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.

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 que hay actualmente en un paquete compuesto MP. 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.

Información relacionada

RFC Editor

Configuración de PPP

Para poder utilizar PPP con el fin de configurar una conexión punto a punto, debe configurar el entorno PPP.

Referencia relacionada

"Información relacionada con los Servicios de acceso remoto" en la página 70
Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas Servicios de acceso remoto. Puede ver o imprimir los archivos PDF que desee.

Creación de un perfil de conexión

El primer paso para configurar una conexión PPP entre sistemas consiste en crear un perfil de conexión en el sistema.

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 y opciones de marcación
- 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
- Perfiles de conexión de receptor
- **Módems**

Para crear un perfil de conexión, siga estos pasos:

1. En System i 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 sistema para el inicio.
   - Pulse **Perfiles de conexión de receptor** con el botón derecho del ratón para establecer el sistema para que permita 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.

Tareas relacionadas

"Asociación de un módem a una descripción de línea" en la página 61
Este tema demuestra los pasos necesarios para asociar un módem a una descripción de línea.

Referencia relacionada

"Caso práctico: conexión del sistema a un concentrador de acceso PPPoE" en la página 10
Muchos proveedores de servicios de Internet (ISP) ofrecen acceso a Internet de alta velocidad a través de una Línea de abonado digital (DSL) utilizando el protocolo punto a punto por Ethernet (PPPoE). Puede conectar el sistema a estos ISP para proporcionar conexiones con un amplio ancho de banda que conserven las ventajas del protocolo punto a punto (PPP).

"Caso práctico: conexión de clientes de acceso telefónico remoto al sistema" en la página 13
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 sistema con protocolo punto a punto (PPP).

"Caso práctico: conexión de la LAN de oficina a Internet con un módem" en la página 16
Normalmente, los administradores configuran redes de oficina que permiten a los empleados acceder a Internet. Los administradores pueden utilizar un módem para conectar el sistema a un proveedor de servicios de Internet (ISP). Los clientes PC conectados a la LAN pueden comunicarse con Internet utilizando el sistema operativo i5/OS como pasarela.

"Caso práctico: conexión de las redes corporativa y remota con un módem" en la página 19
El módem permite que dos ubicaciones remotas (como una oficina central y una sucursal) intercambien datos entre ellas. El protocolo punto a punto (PPP) puede conectar dos LAN entre sí estableciendo una conexión entre un sistema en la oficina central y otro en la sucursal.

"Caso práctico: gestión del acceso de usuarios remotos a los recursos mediante las políticas de grupo y el filtrado de IP" en la página 24
Las políticas de acceso de grupo identifican los distintos grupos de usuarios de una conexión y permiten aplicar atributos de conexión comunes y valores de seguridad a todo el grupo. Puede utilizar políticas de grupo, junto con el filtrado de IP, para permitir y restringir el acceso a direcciones IP específicas de la red.

Tipo de protocolo: PPP o Protocolo Internet de línea serie (SLIP)

PPP sustituye al Protocolo Internet de línea serie (SLIP) como protocolo que conviene elegir para las conexiones punto a punto.

El protocolo punto a punto (PPP) permite que haya 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.

La petición de comentarios (RFC) de SLIP nunca llega 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 hosts. 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 sistema operativo i5/OS. Sin embargo, IBM 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 de protocolo punto a punto (PPP) consisten en seleccionar el tipo de conexión y la modalidad de operación. Las selecciones de modalidad especifican cómo emplea el sistema 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 (Layer Two Tunneling Protocol) (línea virtual)
   - Línea de protocolo punto a punto por Ethernet (PPPoE)
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:

Cuando utiliza un módem (interno o externo) o un adaptador de terminal de red digital de servicios integrados (RDSI) externo para conectarse a través de una línea telefónica, seleccione la conexión de línea conmutada.

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

Respuesta

Elija esta modalidad de operación para permitir que un sistema remoto realice una conexión telefónica con el sistema.

Marcación

Elija esta modalidad de operación para permitir que el sistema establezca una conexión telefónica con un sistema remoto.

Marcación a petición (solo marcar)

Elija esta modalidad de operación si desea permitir que el sistema pueda acceder telefónicamente de forma automática a un sistema remoto al detectarse tráfico TCP/IP del sistema remoto 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 para permitir que el sistema responda llamadas de un sistema remoto dedicado. Esta modalidad de operación también permitirá que el sistema llame al sistema remoto cuando se detecte tráfico TCP/IP para el sistema remoto. Si los dos sistemas utilizan el sistema operativo i5/OS 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 de protocolo punto a punto (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:

Si tiene una línea dedicada entre el sistema local y el sistema remoto, seleccione la conexión de línea alquilada. Si tiene una línea alquilada, no necesita un módem ni un adaptador de terminal de red digital de servicios integrados (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. 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 sistema a través de una línea dedicada. Esta modalidad de operación hace referencia a un perfil de respuesta de línea alquilada.

Iniciador

Elija esta modalidad operativa para permitir que el sistema acceda 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):

Si desea proporcionar una conexión entre sistemas que emplean el protocolo L2TP (Layer Two Tunneling Protocol), seleccione la conexión L2TP.

Una vez establecido un túnel L2TP, se hace una conexión de protocolo punto a punto (PPP) virtual entre el sistema 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 sistema a través de un túnel L2TP.

Iniciador

Elija esta modalidad operativa para permitir que el sistema se conecte a un sistema remoto a través de un túnel L2TP.

Marcación remota

Elija esta modalidad de operación si desea permitir que el sistema pueda conectarse a un proveedor de servicios de Internet (ISP) a través de un túnel L2TP e indicar al ISP que acceda telefónicamente a un cliente PPP remoto.

Iniciador multisalto

Elija esta modalidad de operación si desea permitir que el sistema 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.

Línea PPPoE:

Las conexiones de Protocolo punto a punto por Ethernet (PPPoE) utilizan una línea virtual para enviar datos PPP (a través de un adaptador Ethernet) a un módem de Línea de abonado digital (DSL) proporcionado por el proveedor de servicios de Internet (ISP). El módem también está conectado a la LAN basada en Ethernet.

Esto permite el acceso a Internet de alta velocidad de usuarios de LAN mediante sesiones PPP en el sistema operativo i5/OS. Una vez iniciada la conexión entre el sistema y el ISP, los usuarios individuales de la LAN pueden empezar sesiones exclusivas con el ISP por PPPoE.

Las conexiones PPPoE solo se emplean en los perfiles de conexión de originador. Las conexiones implican la modalidad de operación de iniciador y únicamente utilizan una línea individual.

Configuración de enlace

La configuración de enlace define el tipo de servicio de línea que el perfil de conexión del protocolo punto a punto (PPP) utiliza para establecer una conexión.

Los tipos de servicio de línea dependen del tipo de conexión que se especifique.

Referencia relacionada

"Caso práctico: conexión del sistema a un concentrador de acceso PPPoE" en la página 10
Muchos proveedores de servicios de Internet (ISP) ofrecen acceso a Internet de alta velocidad a través de una Línea de abonado digital (DSL) utilizando el protocolo punto a punto por Ethernet (PPPoE). Puede conectar el sistema a estos ISP para proporcionar conexiones con un amplio ancho de banda que conserven las ventajas del protocolo punto a punto (PPP).

"Caso práctico: conexión de clientes de acceso telefónico remoto al sistema" en la página 13
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 sistema con protocolo punto a punto (PPP).

"Caso práctico: conexión de la LAN de oficina a Internet con un módem" en la página 16
Normalmente, los administradores configuran redes de oficina que permiten a los empleados acceder a Internet. Los administradores pueden utilizar un módem para conectar el sistema a un proveedor de servicios de Internet (ISP). Los clientes PC conectados a la LAN pueden comunicarse con Internet utilizando el sistema operativo i5/OS como pasarela.

"Caso práctico: conexión de las redes corporativa y remota con un módem" en la página 19
El módem permite que dos ubicaciones remotas (como una oficina central y una sucursal) intercambien datos entre ellas. El protocolo punto a punto (PPP) puede conectar dos LAN entre sí estableciendo una conexión entre un sistema en la oficina central y otro en la sucursal.

Una sola línea:

Para definir una línea de Protocolo punto a punto (PPP) asociada a un módem analógico, seleccione este servicio de línea. 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 de i5/OS.

Si es necesario, se podría configurar una línea individual analógica como `compartida` entre un perfil de respuesta y un perfil de marcación. El compartimiento dinámico de recursos es una nueva función diseñada para mejorar la utilización de los recursos. Hasta la versión V5R2, los recursos del módem quedaban comprometidos en cuanto se iniciaba el perfil que lo utilizaba. Esto limitaba al usuario a un

solo recurso por sesión, aunque el recurso estuviera en estado de espera pasiva. Ahora, cuando se accede a un recurso concreto, las reglas de compartimiento son distintas. Se dan dos casos: el primero, cuando se ha iniciado un perfil de marcación antes que un perfil de respuesta; el segundo, cuando se ha iniciado un perfil de respuesta antes que un perfil de marcación. Se supone que la función de compartimiento de recursos está habilitada. En el primer caso, el perfil de marcación iniciado se conectará satisfactoriamente. El perfil de respuesta iniciado en segundo lugar esperará a que la línea esté disponible. Una vez finalizada la conexión de marcación, el perfil de respuesta solicitará la línea y se iniciará. En el segundo caso, el perfil de respuesta iniciado esperará a que haya conexiones entrantes. A menos que se haya establecido una conexión entrante, el perfil de marcación iniciado en segundo lugar ″pedirá prestada″ la línea del perfil de respuesta, el cual ″prestará″ la línea. Entones se establecerá la conexión saliente. Una vez finalizada la conexión, el perfil de marcación devolverá la línea al perfil de respuesta, que volverá a estar listo para aceptar nuevas conexiones entrantes. Para habilitar la función de compartimiento, pulse la pestaña **Módem** de una descripción de línea conmutada y seleccione **Habilitar compartimiento dinámico de recursos**.

El servicio de una sola línea también se emplea para los tipos de conexión L2TP (línea virtual) y PPPoE (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 individual. Por el contrario, la línea individual 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. La línea individual que se emplea con una conexión PPPoE también se considera virtual en el sentido de que proporciona un mecanismo para tratar una línea Ethernet física como si fuese una línea PPP que diera soporte a conexiones remotas. La línea virtual PPPoE está enlazada con una línea Ethernet física y se emplea para dar soporte a las transferencias de datos de protocolo PPP a través de la conexión de LAN Ethernet a un módem DSL.

Agrupación de líneas:

Para establecer que la conexión PPP utilice una línea de una agrupación de líneas, seleccione este servicio de línea. Al empezar la conexión PPP, el sistema selecciona en la agrupación de líneas una línea que no se esté utilizando. En el caso de los perfiles de marcación a petición, el sistema 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 para conexiones individuales con más ancho de banda.

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, a menos que esté habilitado el compartimiento dinámico de recursos. En el caso de las conexiones que emplean una agrupación de líneas, debe haber al menos una línea disponible en la agrupación de líneas al iniciarse el perfil.

  Además, si los recursos están configurados como compartidos (habilitar el compartimiento dinámico de recursos), se logrará una mayor disponibilidad de los recursos, especialmente en las conexiones salientes.

- Podrá utilizar perfiles de marcación a petición con agrupaciones de líneas para que el uso de los recursos resulte más eficaz.

  El sistema 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 podrá ser utilizada por los cuatro perfiles de conexión, permitiendo así que haya dos conexiones activas en todo momento. Al utilizar una agrupación de líneas, no haría falta que tuviera cuatro líneas independientes.

  Asimismo, si su entorno está formado por un cliente PPP y un servidor PPP, las líneas se pueden compartir (habilitar el compartimiento dinámico de recursos) con independencia de si se utilizan como 'líneas individuales' o de si están en una 'agrupación de líneas'. El perfil que se inició en primer lugar no comprometerá el recurso a menos que la conexión esté activa. Por ejemplo, si el servidor PPP está iniciado y a la escucha de conexiones entrantes, dicho servidor 'prestará' una línea utilizada por él al cliente PPP que se inició y 'pidió prestada' la línea compartida del servidor PPP.

Configuración de las agrupaciones de líneas

Las agrupaciones de líneas se definen en un perfil de conexión. Para crear una configuración de agrupación de líneas básica, efectúe los siguientes pasos:

1. En System i Navigator, seleccione su sistema y expanda **Red** → **Servicios de acceso remoto**.
2. Cree un perfil de conexión para efectuar o recibir llamadas. Seleccione una de las siguientes opciones:
   - Pulse **Perfiles de conexión de originador** con el botón derecho del ratón para establecer el sistema para que inicie una conexión con un sistema remoto.
   - Pulse **Perfiles de conexión de receptor** con el botón derecho del ratón para establecer el sistema para que permita las conexiones entrantes de los sistemas y usuarios remotos.
3. Seleccione **Perfil nuevo**.
4. Para un perfil originador (que efectúa llamadas), seleccione: PPP, línea conmutada y la modalidad de operación (normalmente de marcación). Para la configuración del enlace, seleccione **Agrupación de líneas**. Pulse **Aceptar** e System i Navigator abrirá una ventana de propiedades para este perfil de conexión.

   Nota: también puede seleccionar una agrupación de líneas al crear los perfiles de conexión de receptor. La opción de Agrupación de líneas puede figurar en la lista o no, en función de los siguientes valores de los campos: tipo de protocolo, tipo de conexión y modalidad de operación.
5. En la página General, dé un nombre al perfil y especifique una descripción.
6. En la página Conexión, especifique un nombre para la agrupación de líneas y pulse **Nueva**. Se abrirá el diálogo **Propiedades de la nueva agrupación de líneas**, que mostrará todas las líneas y módems disponibles en este sistema.
7. Seleccione las líneas que desea utilizar y añádalas a la agrupación. También puede pulsar **Línea nueva** para definir una línea nueva.
8. Pulse **Aceptar** para guardar esta agrupación de líneas y regresar a las propiedades del Perfil punto a punto nuevo.
9. Complete la información necesaria sobre las demás páginas (por ejemplo, los valores TCP/IP y la autenticación).

10. El perfil de conexión recorre la lista de líneas disponibles (en la agrupación) hasta encontrar un recurso disponible que pueda utilizarse para la conexión. Utilice la ayuda de System i Navigator para obtener asistencia.

Referencia relacionada

"Caso práctico: conexión de clientes de acceso telefónico remoto al sistema" en la página 13
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 sistema con protocolo punto a punto (PPP).

"Caso práctico: conexión de la LAN de oficina a Internet con un módem" en la página 16
Normalmente, los administradores configuran redes de oficina que permiten a los empleados acceder a Internet. Los administradores pueden utilizar un módem para conectar el sistema a un proveedor de servicios de Internet (ISP). Los clientes PC conectados a la LAN pueden comunicarse con Internet utilizando el sistema operativo i5/OS como pasarela.

"Caso práctico: conexión de las redes corporativa y remota con un módem" en la página 19
El módem permite que dos ubicaciones remotas (como una oficina central y una sucursal) intercambien datos entre ellas. El protocolo punto a punto (PPP) puede conectar dos LAN entre sí estableciendo una conexión entre un sistema en la oficina central y otro en la sucursal.

Soporte para 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 sistema, 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 2805 de 4 puertos, en el que hay cuatro líneas que se pueden utilizar desde un solo adaptador.

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 una hebra de perfil de conexión aparte para cada línea definida en la agrupación de líneas. Todas las hebras 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 sistema. Para seleccionar la dirección IP 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 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 o si no quiere que los usuarios remotos accedan a la LAN, deberá definir una dirección IP virtual para el sistema. 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 IP, puesto que no está ligada a una red física, no reenvía automáticamente el tráfico a otras redes conectadas al sistema.

Para crear una dirección IP virtual, siga estos pasos:

1. En System i Navigator, expanda el sistema y acceda a **Red → Configuración TCP/IP → IPV4 → Interfaces**.
2. Pulse **Interfaces** con el botón derecho del ratón y seleccione **Interfaz nueva → IP virtual**.

3. Siga las instrucciones facilitadas por el asistente de la 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 IP 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 IP después de crear la interfaz, seleccione la opción de iniciar la dirección IP cuando utilice el asistente de la interfaz.

Agrupaciones de direcciones IP remotas para perfiles de múltiples conexiones

También podrá utilizar las 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, no podrán establecerse nuevas conexiones. Además, si no hay líneas 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, se podrán emplear las otras líneas de la agrupación.

Tareas relacionadas

"Paso 1: configuración del perfil de terminador L2TP para cada una de las interfaces de la partición que posee los módems" en la página 30
Siga estos pasos para crear un perfil de terminador para cada interfaz:

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 detención que se utilice con múltiples conexiones entrantes.

Esto incluye L2TP (Layer Two Tunneling Protocol) 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 IP ya se está utilizando, se asignará la próxima dirección IP que haya dentro del rango. Por ejemplo, supongamos que la dirección IP inicial es 10.1.1.1 y que el número de direcciones IP es 5. Las direcciones IP que haya 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 IP de la agrupación, se rechazarán las subsiguientes peticiones de conexión hasta que otra conexión finalice y una dirección IP pase a estar disponible.
- Para asignar direcciones IP concretas a determinados sistemas remotos permitiendo a la vez que otros sistemas entrantes utilicen una dirección IP 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 al sistema, el sistema determina si se ha definido una dirección IP específica para ese usuario. Si es así, se asignará esa dirección IP al sistema remoto; en caso contrario, se le asignará una dirección IP de la agrupación de direcciones IP remotas.

Configuración del módem para PPP

Los módems permiten realizar conexiones analógicas (líneas alquiladas y conmutadas). Para las conexiones de protocolo punto a punto (PPP) analógicas, puede utilizar un módem externo, un módem interno o un adaptador de terminal de red digital de servicios integrados (RDSI).

Referencia relacionada

"Resolución de problemas de PPP" en la página 69
Si surgieran problemas de conexión del protocolo punto a punto (PPP), puede utilizar la 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.

Configuración de un módem nuevo

Puede configurar un módem nuevo utilizando una descripción de módem existente o basar la descripción de módem en una descripción de módem anterior.

Para configurar un módem nuevo, siga estos pasos.

1. En System i Navigator, seleccione su sistema 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.

Utilización de la descripción de un módem existente

Para determinar si puede utilizar la descripción de un módem existente, siga estos pasos:

1. En System i Navigator, seleccione su sistema 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 predeterminada, 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 predeterminadas 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.

Creación de una descripción de módem basada en una descripción de módem anterior

Para crear una descripción de módem basada en una descripción de módem anterior siga estos pasos:

1. En System i Navigator, seleccione su sistema y expanda **Red** → **Servicios de acceso remoto**.
2. Seleccione **Módems**.
3. En la lista de módems, pulse **Hayes genérico** 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.

Referencia relacionada

"Resolución de problemas de PPP" en la página 69
Si surgieran problemas de conexión del protocolo punto a punto (PPP), puede utilizar la 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.

Establececimiento de series para los mandatos del módem

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.

Tabla 9. Módems definidos en el sistema y series de mandatos

Propiedad del módem	**Serie de mandato correcta para la mayoría de los módems**
Restablecimiento del módem en los valores predeterminados 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 o 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: configuración de un adaptador de terminal RDSI

En el ejemplo se muestra cómo configurar un adaptador de terminal de red digital de servicios integrados (RDSI).

1. En System i Navigator, seleccione su sistema 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 recuadros de **campo**.
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 realiza el sistema en caso de errores

   En consecuencia, estos mandatos deben permitir y limitarse a los siguientes valores:

   - 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).
   - 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 sistema 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.

Referencia relacionada

"Adaptadores de terminal RDSI" en la página 42
La Red digital de servicios integrados (RDSI) proporciona una conexión digital que le permite comunicarse mediante cualquier combinación de voz, datos y vídeo, entre otras aplicaciones multimedia.

Asociación de un módem a una descripción de línea

Este tema demuestra los pasos necesarios para asociar un módem a una descripción de línea.

1. En System i Navigator, seleccione el sistema y expanda **Red** → **Servicios de acceso remoto** → **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 la ventana Propiedades de línea nueva.

4. En la ventana 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.

Puede configurar los perfiles de conexión de originador para que pidan prestada una línea PPP y un módem asignados al perfil de conexión de receptor que está en espera de una llamada entrante. La conexión de origen devolverá la línea PPP y el módem al perfil de conexión de receptor cuando la conexión haya finalizado. Para habilitar esta nueva función, marque la opción **Habilitar compartimiento dinámico de recursos** en la pestaña **Módem** de la ventana de configuración de líneas PPP. Puede configurar líneas PPP desde la pestaña **Conexión** de los perfiles de conexión de originador y de receptor.

Tareas relacionadas

"Creación de un perfil de conexión" en la página 50
El primer paso para configurar una conexión PPP entre sistemas consiste en crear un perfil de conexión en el sistema.

Configuración de un PC remoto

Para conectarse a una plataforma System i desde un sistema personal (PC) que ejecute un sistema operativo Windows de 32 bits, debe comprobar que el módem esté 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 CHAP-MD5 (el sistema operativo i5/OS 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 el protocolo de autenticación de contraseñas (PAP). El sistema no da soporte a ningún otro tipo de protocolo no protegido.
- En general, el sistema de direcciones IP lo define el sistema remoto o el sistema operativo i5/OS. Si piensa utilizar métodos de direcciones IP alternativos (como el de definir sus propias direcciones IP), asegúrese de que el sistema también está configurado para aceptar su método de direcciones.
- Añada la dirección IP del DNS, si ello es apropiado para su entorno.

Configuración del acceso a Internet por medio de AT&T Global Network

Si desea comunicarse con la red AT&T Global Network, debe configurar perfiles especiales.

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 los siguientes:

- **Mail Exchange**: permite recuperar periódicamente los mensajes de correo recibidos en una única cuenta de AT&T Global Network y enviarlos al sistema 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).
- 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.
- 2793/576C: adaptador de E/S de WAN de dos puertos, con un módem integrado V.92 en el puerto 1 y una interfaz de comunicaciones estándar en el puerto 2. Sustituye al modelo 2771.
- 2805: adaptador de E/S de WAN de cuatro puertos, con un módem V.92 integrado. Sustituye a los modelos 2761 y 2772.

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 del 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 System i Navigator, expanda el sistema 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

Puede utilizar asistentes de conexión para que le sirvan de guía en la configuración de perfiles de conexión.

Asistente de nueva conexión por línea telefónica

Este asistente describe los pasos necesarios para configurar un perfil de conexión por línea telefónica para acceder al ISP o a una intranet. Para llegar hasta el final del asistente, deberá solicitar algunos datos al administrador de la red o al ISP. En la ayuda en línea hallará más información sobre cómo completar este asistente.

Asistente de IBM Universal Connection

Este asistente describe los pasos necesarios para 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 i5/OS exclusivo con el fin de recomendarle arreglos personalizados en función del sistema y de su situación.

Información relacionada

Configuración de una política de acceso de grupo

La carpeta **Políticas de acceso de grupo**, en 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, siga estos pasos:

1. En System i, seleccione el sistema 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.

   Con la configuración multienlace, especifica que desea reunir múltiples líneas físicas para formar un paquete compuesto. El número máximo de líneas por paquete compuesto puede oscilar entre 1 y 6. Puesto que no se conoce el valor del tipo de línea hasta que se establece una conexión, el valor predeterminado 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 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, únicamente está permitido un solo enlace.
5. Pulse la pestaña **Valores de TCP/IP** para habilitar cualquiera de los siguientes valores:

   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 sistema funcione como direccionador para esta conexión. Con esta opción, los datagramas de IP no destinados a este sistema pasan a través de este sistema hasta una red conectada. Si deja esta opción en blanco, el IP descarta aquellos datagramas del sistema remoto que no estén destinados a una dirección local de este sistema.

   Tal vez, por razones de seguridad, no le interese permitir el reenvío de IP. No obstante, un ISP generalmente siempre proporciona 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 **General** de la página Propiedades de IPv4.

   Solicitar compresión de cabecera TCP/IP (VJ). Esta opción especifica si desea que el IP comprima la información de cabecera después de establecer una conexión. Normalmente, 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 sistema 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. Las reglas de filtrado controlan el tráfico IP en la red. Este componente de filtrado de paquetes IP permite proteger el sistema al filtrar los paquetes según las reglas que especifique. Las reglas se basan en la información de cabecera de los paquetes.

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, siga estos pasos:

1. Pulse **Autenticación** para abrir la página Autenticación.
2. Pulse **Exigir que este servidor iSeries 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 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 la ventana Añadir usuario, especifique la siguiente información:
   a. Seleccione el protocolo de autenticación para el que está definido el nombre del usuario.
   b. 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).

   c. Marque la opción **Aplicar una política de grupo al usuario**, seleccione una política de grupo en la lista y pulse **Abrir**.

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

Referencia relacionada

"Caso práctico: gestión del acceso de usuarios remotos a los recursos mediante las políticas de grupo y el filtrado de IP" en la página 24
Las políticas de acceso de grupo identifican los distintos grupos de usuarios de una conexión y permiten aplicar atributos de conexión comunes y valores de seguridad a todo el grupo. Puede utilizar políticas de grupo, junto con el filtrado de IP, para permitir y restringir el acceso a direcciones IP específicas de la red.

Información relacionada

Filtrado de IP y conversión de direcciones de red

Aplicación de reglas de filtrado de paquetes IP a una conexión PPP

Puede utilizar un archivo de reglas de paquete para restringir el acceso de un usuario o un grupo a las direcciones IP de la red.

En Information Center hallará el tema Filtrado de IP y conversión de direcciones de red que 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 ver 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.
  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.
4. Pulse **Aceptar** para aplicar el filtro PPP.

Referencia relacionada

"Caso práctico: gestión del acceso de usuarios remotos a los recursos mediante las políticas de grupo y el filtrado de IP" en la página 24
Las políticas de acceso de grupo identifican los distintos grupos de usuarios de una conexión y permiten aplicar atributos de conexión comunes y valores de seguridad a todo el grupo. Puede utilizar políticas de grupo, junto con el filtrado de IP, para permitir y restringir el acceso a direcciones IP específicas de la red.

Habilitación de servicios de RADIUS y DHCP para perfiles de conexión

A continuación, se muestran los pasos necesarios para habilitar servicios RADIUS o DHCP (Protocolo de configuración dinámica de hosts) para los perfiles de conexión de receptor PPP.

1. En System i Navigator, seleccione su sistema y expanda **Red** → **Servicios de acceso remoto**.
2. Pulse **Servicios de acceso remoto** con el botón derecho del ratón y seleccione **Servicios**.
3. Pulse la pestaña **DHCP-WAN**. Así se habilitará automáticamente DHCP y se detectará qué servidor y agentes de retransmisión DHCP (si los hubiera) se están ejecutando en el sistema.
4. Para habilitar los servicios RADIUS, pulse la pestaña **RADIUS**.
   a. Seleccione **Habilitar conexión de servidor de acceso a red RADIUS**.
   b. Seleccione **Habilitar RADIUS para autenticación**.
   c. Si fuera pertinente para su solución RADIUS, también puede habilitar la configuración de direcciones TCP/IP y contabilidad de RADIUS.
5. Pulse el botón **Valores de NAS de RADIUS** para configurar la conexión con el servidor RADIUS.
6. Pulse **Aceptar** para volver a System i Navigator.

Referencia relacionada

"Caso práctico: autenticación de conexiones por línea telefónica con NAS de RADIUS" en la página 22
Un servidor de acceso a red (NAS) que se esté ejecutando en el sistema puede direccionar las peticiones de autenticación desde los clientes de acceso telefónico a un servidor RADIUS (Remote Authentication Dial In User Service) aparte. Si la autenticación es satisfactoria, el servidor RADIUS también puede controlar las direcciones IP asignadas al usuario.

Gestión de PPP

Este tema contiene información sobre las tareas de gestión de PPP que puede realizar en el sistema.

Referencia relacionada

"Información relacionada con los Servicios de acceso remoto" en la página 70
Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas Servicios de acceso remoto. Puede ver o imprimir los archivos PDF que desee.

Establecimiento de 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 la ventana Configuración de perfil de conexión punto a punto.

Una vez que haya entrado sus selecciones en esa ventana, aparece la hoja de propiedades del perfil de conexión. Las selecciones que especifique en la ventana 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 de la ventana 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 System i Navigator describe todas las opciones que figuran en la ventana. También podrá hallar más información en los ejemplos y procedimientos de PPP.

Supervisión de la actividad de PPP

Puede ver un perfil de conexión y las anotaciones de sesión utilizando System i Navigator.

Acerca de los trabajos de conexión PPP:

- Hay dos trabajos de control de PPP que se emplean para gestionar las hebras de las conexiones PPP individuales. Estos trabajos se ejecutan en el subsistema QSYSWRK:
  - QTPPPCTL: trabajo de control de PPP principal. Este trabajo gestiona cada una de las hebras de conexión PPP.
  - QTPPPL2TP: trabajo servidor L2TP. Este trabajo gestiona el establecimiento de túneles L2TP y solo se ejecuta si en ese momento está funcionando un perfil L2TP.
- Las hebras de conexión PPP en QTPPPCTL se ejecutan con el nombre de usuario QTCP.
- Los trabajos de conexión SLIP se ejecutan en el subsistema QSYSWRK con 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*nnn*, que son trabajos de marcación de entrada, siendo *nnn* cualquier número comprendido entre 1 y 999.

Trabajo con perfiles de conexión:

1. En System i Navigator, expanda el sistema 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:
   - **Conexiones**, que abre una ventana 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. Hay opciones disponibles para ver la salida del trabajo, los detalles de la conexión, las anotaciones de llamadas o las anotaciones de mensajes de cada conexión.
   - **Propiedades**, que abre la página Propiedades, en la que se visualizan las propiedades actuales de una conexión.

Visualización de información de conexiones:

1. En System i Navigator, expanda el sistema 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 muestra 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, el ID de hebra, las direcciones IP local y remota, y el nombre del trabajo PPP.
3. Si desea ver la salida del trabajo, los detalles de una conexión, las anotaciones de llamadas o las anotaciones de mensajes, pulse una conexión con el botón derecho del ratón para habilitar los botones.
4. Para ver QTPPPCTL, pulse **Trabajos**. En la ventana de conexiones, pulse con el botón derecho el nombre del trabajo y seleccione **Salida de impresora** o **Anotaciones de trabajo** para mostrar información sobre todas las hebras de conexiones asociadas con QTPPPCTL.

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. La ventana de detalles le permitirá ver información adicional sobre esta conexión en concreto.
6. Para ver las anotaciones de llamadas, pulse **Anotaciones de llamadas**.
7. Para ver las anotaciones de mensajes, pulse **Anotaciones de mensajes**.

Trabajo con salida PPP del sistema:

Para trabajar con salida PPP, entre WRKTCPPTP en la línea de mandatos del sistema:

- 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. A continuación, utilice el mandato WRKSPLF para acceder a la salida impresa.

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, bajo **Red → Servicios de acceso remoto**, tras seleccionar ya sea perfiles de originador o de receptor. El estado de una conexión individual se visualiza mediante la ventana Conexiones.

Tabla 10. Descripción de estado primario

Descripción de estado primario	Explicación
En espera de peticiones de conexión	El perfil de receptor está preparado para una conexión
En espera de llamada entrante	El sistema 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
Terminador multisalto iniciando un iniciador multisalto	Multisalto en proceso
Conexión multisalto activa	Multisalto conectado satisfactoriamente

Tabla 11. Descripción de estado secundario

Descripción de estado secundario	Explicación
Inicializando módem	Se está inicializando el módem al principio de una conexión por línea telefónica
En espera de conexión de módem	El servidor PPP está en estado de escucha
MARCANDO xxx-xxxx	Número marcado por el cliente que accede por línea telefónica
Detectada llamada entrante	El servidor PPP detecta una llamada de módem entrante
Módem conectado	El establecimiento de enlace PPP se ha realizado satisfactoriamente
Operativo	Conexión PPP activa
Enlace terminado	Conexión finalizada por el similar

Tabla 11. Descripción de estado secundario (continuación)

Descripción de estado secundario	Explicación
Detenido	El perfil o el trabajo ha finalizado
Anomalía de autenticación	No se pudieron establecer conexiones PPP porque la autenticación ha fallado
Excedido tiempo de espera de inactividad de conexión	No se pudieron establecer conexiones PPP porque se acabó el tiempo de espera de inactividad
Negociando direcciones IP	Conexiones PPP finalizadas por problemas de negociación de IP
El módem remoto no ha respondido	No se pudieron establecer conexiones PPP por falta de respuesta del otro extremo
Rechazo de protocolo	No se pudieron establecer conexiones PPP por anomalía en negociación NCP
Anomalía de reintentos	No se pudieron establecer conexiones PPP porque se ha excedido la cuenta de reintentos
Recibida confirmación de sesión PPPoE del similar	La negociación de PPPoE se ha realizado satisfactoriamente
Establecida llamada L2TP	Mensaje de activación del túnel L2TP

Resolución de problemas de PPP

Si surgieran problemas de conexión del protocolo punto a punto (PPP), puede utilizar la 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.

La información actual relacionada con los arreglos temporales de programa (PTF) y la resolución de problemas se facilita en el sitio Web de TCP/IP para i5/OS. Este sitio Web proporciona la información más reciente que complementa y prevalece sobre la información que figura en el presente tema.

1. Material de soporte obligatorio:
   - Sistema operativo, nivel y tipo de host remoto
   - Nivel del sistema operativo de host de i5/OS
   - Todos los archivos de salida que se guardan en una cola de salida que tiene el mismo nombre que el perfil
   - Las anotaciones de trabajo de QTPPPCTL y QTPPPL2TP (si existe un perfil L2TP)
   - El script de la conexión que 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 Redbook ITSO V4 TCP/IP for AS/400: More Cool Things Than Ever cubre los problemas de PPP siguientes. Además, facilita información detallada sobre la resolución de problemas.

Para identificar los problemas y encontrar las soluciones, consulte la lista de comprobación en la tabla siguiente.

Tabla 12. Problemas de PPP del Redbook ITSO

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 System i 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.
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.

Conceptos relacionados

"Configuración del módem para PPP" en la página 59
Los módems permiten realizar conexiones analógicas (líneas alquiladas y conmutadas). Para las conexiones de protocolo punto a punto (PPP) analógicas, puede utilizar un módem externo, un módem interno o un adaptador de terminal de red digital de servicios integrados (RDSI).

"Configuración de un módem nuevo" en la página 59
Puede configurar un módem nuevo utilizando una descripción de módem existente o basar la descripción de módem en una descripción de módem anterior.

Referencia relacionada

"Información relacionada con los Servicios de acceso remoto"
Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas Servicios de acceso remoto. Puede ver o imprimir los archivos PDF que desee.

Información relacionada con los Servicios de acceso remoto

Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas Servicios de acceso remoto. Puede ver o imprimir los archivos PDF que desee.

IBM Redbooks

- IBM i5/OS IP Networks: Dynamic!
- V4 TCP/IP for AS/400: More Cool Things Than Ever

Sitios Web

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 el sitio Web de TCP/IP for i5/OS . Este sitio Web proporciona la información más reciente que complementa y prevalece sobre la información que figura en la presente colección de temas.

Referencia relacionada

"Archivo PDF para Servicios de acceso remoto" en la página 1
Puede ver e imprimir un archivo PDF de esta información.

Apéndice. Avisos

Esta información ha sido creada para los productos y servicios ofrecidos en EE.UU.

Es posible que en otros países IBM no ofrezca los productos, los servicios o los dispositivos que se describen en este documento. Póngase en contacto con el representante local de IBM que le informará sobre los productos y servicios disponibles actualmente en su área. Las referencias hechas a productos, programas o servicios de IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar puede utilizarse cualquier otro producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran alguno de los temas tratados en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Para realizar consultas relacionadas con los caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o bien envíe su consulta por escrito a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japón

El párrafo siguiente no puede aplicarse en el Reino Unido ni en cualquier otro país en el que tales disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGUNA CLASE, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícitas ni explícitas, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información incluida en este documento está sujeta a cambios periódicos, que se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Cualquier referencia hecha en esta información a sitios Web no de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno como promoción de esos sitios Web. Los materiales de estos sitios Web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios Web es de la entera responsabilidad del usuario.

IBM puede utilizar o distribuir la información que usted le suministre del modo que IBM considere conveniente sin incurrir por ello en ninguna obligación para con usted.

Los licenciatarios de este programa que deseen obtener información acerca del mismo con el fin de: (i) intercambiar la información entre programas creados independientemente y otros programas (incluido este) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
Estados Unidos

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluyendo en algunos casos el pago de una tarifa.

El programa bajo licencia descrito en este documento, así como todo el material bajo licencia disponible para él, lo proporciona IBM bajo el Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programas bajo Licencia de IBM, el Acuerdo de Licencia para Código Máquina de IBM o cualquier otro acuerdo equivalente entre ambas partes.

Cualquier información de rendimiento que aparezca en este documento ha sido determinada en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos podrían ser distintos. Algunas mediciones se han realizado en sistemas en fase de desarrollo y, por lo tanto, no hay ninguna garantía que estas mediciones sean las mismas en los sistemas normalmente disponibles. Además, algunas mediciones podrían haberse estimado mediante extrapolación. Los resultados reales podrían ser diferentes. Los usuarios de este documento deberían verificar los datos aplicables para su entorno específico.

La información referente a productos no IBM se ha obtenido de los suministradores de dichos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha comprobado dichos productos y no puede afirmar la exactitud en cuanto a rendimiento, compatibilidad u otras características relativas a productos no IBM. Las consultas acerca de las posibilidades de los productos no IBM deben dirigirse a los suministradores de los mismos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para que los ejemplos sean lo más completos posible, incluyen los nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con los nombres y direcciones utilizados por alguna empresa real es pura coincidencia.

LICENCIA DE DERECHOS DE COPIA:

Esta información contiene programas de aplicación de muestra en el lenguaje fuente, que ilustran técnicas de programación en varias plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de la forma deseada sin tener que efectuar ningún pago a IBM, con el objetivo de desarrollar, utilizar, comercializar o distribuir programas de aplicación conformes a la interfaz de programación de aplicaciones para la plataforma operativa para la que se han escrito los programas de ejemplo. Estos ejemplos no se han verificado a fondo bajo todas las condiciones. IBM, por lo tanto, no puede garantizar ni dar por supuesta la fiabilidad, la posibilidad de servicio, ni el funcionamiento de estos programas.

Cada copia o parte de estos programas de ejemplo o cualquier trabajo derivado de estos debe incluir una nota de derechos de copia como esta:

© (nombre de su empresa) (año). Algunas partes de este código procede de los programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o los años_. Reservados todos los derechos.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Información sobre la interfaz de programación

Esta publicación Servicios de acceso remoto: conexiones PPP documenta interfaces de programación que permiten al cliente escribir programas para obtener los servicios de IBM i5/OS.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:

AIX
AS/400
eServer
i5/OS
IBM
IBM (logotipo)
iSeries
Lotus
OS/400
Redbooks
System i

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos o en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos y otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Los demás nombres de compañías, productos o servicios pueden ser marcas registradas o de servicio de terceros.

Términos y condiciones

Los permisos para utilizar estas publicaciones están sujetos a los siguientes términos y condiciones.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Aparte de la autorización que se concede explícitamente en este permiso, no se otorga ningún otro permiso, licencia ni derecho, ya sea explícito o implícito, sobre las publicaciones, la información, los datos, el software o cualquier otra propiedad intelectual contenida en ellas.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer del fabricante, no se sigan debidamente las instrucciones anteriores.

No puede bajar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN ″TAL CUAL″, SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.

Impreso en España