System i

Networking
Remote Access Services: PPP connections

Version 5 Release 4

System i

Networking
Remote Access Services: PPP connections

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in "Notices," on page 67.

Eighth Edition (September 2007)

This edition applies to version 5, release 4, modification 0 of IBM i5/OS (product number 5722–SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

Remote Access Services: PPP connections

Point-to-Point Protocol (PPP) is an Internet standard for transmitting data over serial lines.

PPP is the most widely used connection protocol among Internet service providers (ISPs). PPP enables individual computers to access networks. The networks in turn provide access to the Internet. The System i™ product includes TCP/IP PPP support as part of its wide-area network (WAN) connectivity.

You can exchange data between locations by using PPP to connect a remote computer to your System i platform. Through PPP, remote systems that are connected to your system can access resources or other machines that belong to the same network as your system. You can also configure your system to connect to the Internet by using PPP. The iSeries™ Navigator Dial-Up Connection wizard can guide you through the process of connecting your system to the Internet or to an internal network.

What's new for V5R4

These new functions relate to Remote Access Services PPP connections.

Changed functions

- **Call log**

  Call logs are important records of the data that flows to or from the modem during a PPP session. They are saved or deleted based on the Start TCP/IP Point-to-Point (STRTCPPTP) command OUTPUT parameter (*ERROR or *PRINT or *NONE).

  In previous releases, call log spooled files were named call log*nnnnnn*, where *nnnnnn* was the job number of the *nnnnnn*/QTCP/QTPPPSSN job.

  In V5R4, all PPP sessions run as threads under job *nnnnnn*/QTCP/QTPPPCTL, where *nnnnnn* is the job number. Call log spooled files are named CL*mmmmmmmm*, where *mmmmmmmm* is the thread ID. This allows you to match session messages in the QTPPPCTL job log (which have a `Thread .... 00000028` field) with the corresponding call log.
- **QTPPPSSN and QTPPPL2SSN**
  - QTPPPSSN and QTPPPL2SSN (L2TP) jobs are PPP session jobs in releases prior to IBM® i5/OS® V5R4. They were started and ended with STRTCPPTP and End Point-to-Point TCP/IP (ENDTCPPTP) commands or by QTPPPL2TP when a tunnel was established or ended. They can also be started or ended automatically as links were started or ended by the multilink protocol.

    As of V5R4, PPP no longer uses QTPPPSSN and QTPPPL2SSN jobs. Sessions run as threads in QTPPPCTL.
  - In releases prior to i5/OS V5R4, Work with Point-to-Point TCP/IP Profiles (WRKTCPPTP) command option 14 (Work with job) brought up the active session job, or the QTPPPL2TP job if there was no active PPP session for the L2TP profile.

    In V5R4, WRKTCPPTP option 14 brings up QTPPPCTL if a session thread is active in that job.
- **Message log**

  In V5R4, there is a new message log spooled file for session messages. It collects messages from the session thread, messages from the initial thread that are the result of work on the behalf of the session, and messages from spawned processes into one spooled file.

  A message log spooled file is named ML*mmmmmmmm*, where *mmmmmmmm* is the thread ID. This allows the matching of call logs, message logs, and session messages in the QTPPPCTL job log (which have a `Thread .... 00000028` field).
- **QTPPPCTL and QTPPPL2TP**

In V5R4, QTPPPCTL job uses multiple system threads to run sessions as threads instead of as separate processes (QTPPPSSN and QTPPPL2SSN).

QTPPPCTL job starts a secondary session and link threads to replace the old QTPPPSSN and QTPPPL2SSN session and link jobs.

QTPPPCTL job is returned on application programming interfaces (APIs) and the iSeries Navigator GUI when session jobs are requested.

- **Ethernet adapters**

  In V5R4, the list of Ethernet adapters that support PPPoE expands to include type 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A, and 576A Ethernet adapters.
- **PPPoE**

  In V5R4, PPPoE can share the same adapter as IPv4 and IPv6 traffic.

How to see what's new or changed

To help you see where technical changes have been made, this information uses:

- The » image to mark where new or changed information begins.
- The « image to mark where new or changed information ends.

To find other information about what's new or changed this release, see the Memo to users.

Printable PDF

Use this to view and print a PDF of this information.

To view or download the PDF version of this document, select Remote Access Services: PPP connections (about 940 KB).

Other information

You can also view or print any of the following information:

- Manuals:
  - Find the latest program temporary fixes (PTFs), and the latest configuration information about PPP and L2TP through the PPP link on the TCP/IP for i5/OS . This link provides the latest information that supplements and overrides the information that is contained in this topic collection.
- IBM Redbooks™:
  - The ITSO Redbook V4 TCP/IP for AS/400®: More Cool Things Than Ever covers TCP/IP services and applications.
  - The ITSO Redbook IBM eServer™ iSeries IP Networks: Dynamic! covers TCP/IP services and applications.

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

PPP concepts

You can use PPP to connect a System i platform to remote networks, client PCs, another System i platform, or an Internet service provider (ISP). To fully use this protocol, you should understand both the capabilities and the i5/OS support for this protocol.

Related reference

"Related information for PPP" on page 66
Listed below are the IBM Redbooks (in PDF format) that provide additional information about Remote Access Services PPP connections. You can view or print the PDFs.

What is PPP

Point-to-Point Protocol (PPP) is a TCP/IP protocol that is used to connect one computer system to another. Computers use PPP to communicate over the telephone network or the Internet.

A PPP connection exists when two systems physically connect through a telephone line. You can use PPP to connect one system to another. For example, an established PPP connection between a branch office and a central office allows either office to transfer data to the other through the network.

PPP allows interoperability among the remote access software of different manufacturers. It also allows multiple network communication protocols to use the same physical communication line.

The following Request for Comment (RFC) standards describe the PPP protocol. You can find more information about the RFCs on the RFC Editor Web page .

- RFC-1661 Point-to-Point Protocol
- RFC-1662 PPP on HDLC-like framing
- RFC-1994 PPP CHAP

Connection profiles

Point-to-Point connection profiles define a set of parameters and resources for specific Point-to-Point Protocol (PPP) connections. You can start profiles that use these parameter settings to dial-out (originate) or to listen for (receive) PPP connections.

You can use the following two types of profiles to define a set of characteristics for a PPP connection or set of connections:

- *Originator connection profiles* are point-to-point connections that originate from the local system and are received by a remote system. You can configure outbound connections using this object.
- *Receiver connection profiles* are point-to-point connections that originate from a remote system and are received by the local system. You can configure inbound connections using this object.

A connection profile specifies how a PPP connection works. The information in a connection profile answers these questions:

- What type of connection protocol do you use? (PPP or Serial Line Internet Protocol (SLIP))
- Does your system contact the other computer by dialing out (originator)? Does your system wait to receive a call from the other system (receiver)?
- What communications line does the connection use?
- How should your system determine which IP address to use?

- How should your system authenticate another system? Where should your system store the authentication information?

The connection profile is the logical representation of the following connection details:

- Line and profile type
- Multilink settings
- Remote telephone numbers and dialing options
- Authentication
- TCP/IP settings: IP addresses and routing, and IP filtering
- Work management and connection customization
- Domain name servers

The system stores this configuration information in a connection profile. This information provides the necessary context for your system to establish a PPP connection with another system. A connection profile contains the following information:

- **The protocol type**. You can choose between PPP and SLIP. IBM suggests that you use PPP whenever possible.
- **The mode selection**. The mode selection specifies the connection type and the operating mode for this connection profile.

  Connection type. This specifies the type of line your connections rest on and whether they are dial (originator) or answer (receiver). You can select among these connection types:

  – Switched line

  – Leased (dedicated) line

  – Layer Two Tunneling Protocol (L2TP) (virtual line)

  – Point-to-Point Protocol over Ethernet (PPPoE) (virtual line)

  PPPoE is only supported for originator connection profiles.
- **Operation mode**. The available operating mode depends on the type of connection.

Table 1. Available operating modes for originator connection profiles

Connection type	**Available operating modes**
Switched line	• Dial • Dial-on-demand (dial only) • Dial-on-demand (answer enabled dedicated peer) • Dial on demand (Remote peer enabled)
Leased line	Initiator
L2TP	• Initiator • Multi-hop initiator • Remote dial
PPP over Ethernet	Initiator

Table 2. Available operating modes for receiver connection profiles

Connection type	**Available operating modes**
Switched line	Answer
Leased line	Terminator
L2TP	Terminator (Network server)

- **Link configuration**. This specifies the type of line service that this connection uses.

These choices depend on the type of mode selection that you choose. For a switched line and leased line you can choose any of these:

- Single line
- Line pool

For all other connection types (Leased, L2TP, PPPoE), the line service selection is single line only.

Related reference

"Software and hardware requirements" on page 32
A Point-to-Point Protocol (PPP) environment requires that you have two or more computers that support PPP. One of these computers, the System i platform, can either be the originator or receiver.

Group policy support

With group policy support, network administrators can define user-based group policies to manage resources. Individual users can be assigned access control policies when they log on to the Point-to-Point Protocol (PPP) or Layer Two Tunneling Protocol (L2TP) session.

Users can be identified as belonging to a specific class of user. Each class has its unique policy that defines resource limits (such as number of links allowed in a multilink bundle), attributes (such as IP forwarding), and the identification of what set of IP packet filter rules to apply. For example, with group policy support, network administrators can define a Work_at_Home group that allows full access to the network or a Vendor_Workers group that is restricted to a set of services.

Related reference

"Scenario: Connecting your system to a PPPoE access concentrator" on page 11
Many Internet service providers (ISPs) provide high-speed Internet access over a Digital Subscriber Line (DSL) using Point-to-Point Protocol over Ethernet (PPPoE). You can connect your system to these ISPs to provide high-bandwidth connections that preserve the benefits of Point-to-Point Protocol (PPP).

"Scenario: Managing remote user access to resources using group policies and IP filtering" on page 24
Group access policies identify distinct user groups for a connection, and allow you to apply common connection attributes and security settings to the entire group. You can use group policies, along with IP filtering, to permit and restrict access to specific IP addresses on your network.

Scenarios: Remote access using PPP connections

These scenarios describe how Point-to-Point Protocol (PPP) works and how to implement a PPP environment in a network. The scenarios also introduce fundamental PPP concepts from which beginners and experienced users can benefit before they proceed to the planning and configuration tasks.

Related reference

"Related information for PPP" on page 66
Listed below are the IBM Redbooks (in PDF format) that provide additional information about Remote Access Services PPP connections. You can view or print the PDFs.

Example: PPP and DHCP on a single System i

This example explains how to set up a System i model as a Dynamic Host Configuration Protocol (DHCP) server for a LAN and a remote dial-in client.

Remote clients, such as dial-in clients, often require access to a company's network. Dial-in clients can gain access to a System i model with Point-to-Point Protocol (PPP) . To access the network, the dial-in client needs IP information just like any directly attached network client. A System i DHCP server can distribute IP address information to a PPP dial-in client just like any other directly attached client. The following figure shows a remote client that must dial into the company's network to do some work.

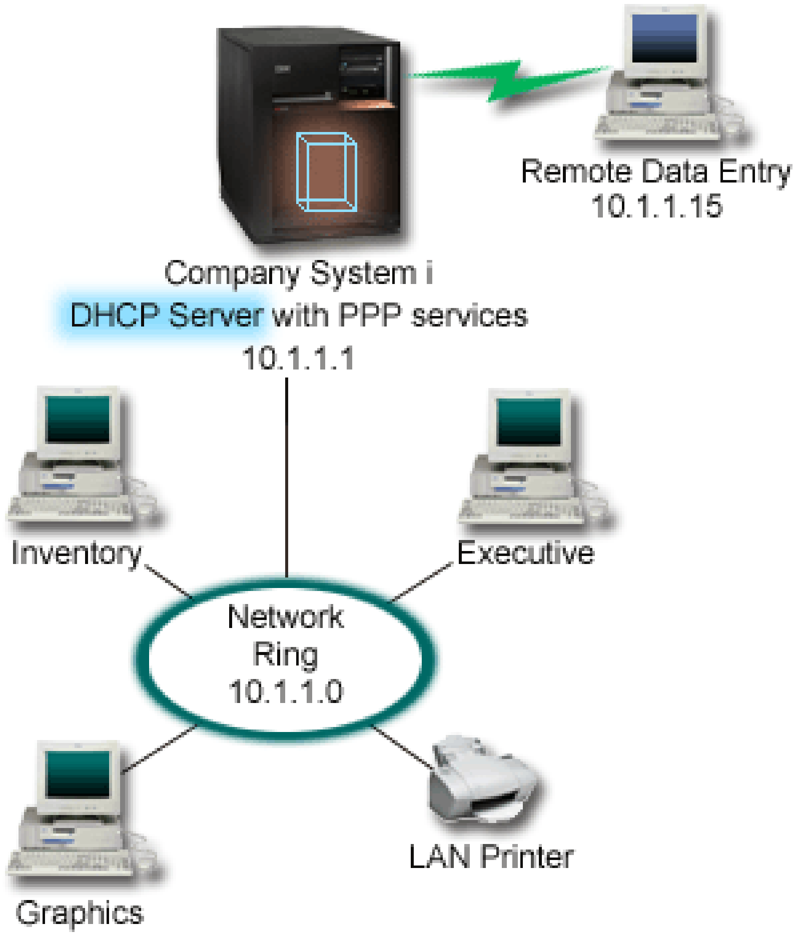


Figure 1. PPP and DHCP on a single System i model

For the remote employee to successfully become part of the company's network, the System i model must use a combination of Remote Access Services and DHCP. The Remote Access Services function creates the dial-in capability for the System i model. If set up properly, after the client establishes the dial-in connection, the PPP server tells the DHCP server to distribute TCP/IP information to the remote client.

In this example, a single DHCP subnet policy covers both the on-site network clients and the dial-in clients.

If you want your PPP profile to defer to the DHCP for IP distribution, you must do so in the PPP profile. In the TCP/IP settings of the receiver connection profile, you must set the remote IP address assignment method from Fixed to DHCP. To allow the dial-in clients to communicate with other network clients, like the LAN printer, you must also allow IP forwarding in the TCP/IP settings of the profile and the TCP/IP configuration (stack) properties. If you only set IP forwarding on in the PPP profile, the System i model will not pass the IP packets. You must set IP forwarding on in both the profile and the stack.

Also, the Local Interface IP address in the PPP profile must be an IP address that falls within the subnet definition in the DHCP server. In this example, the PPP profile Local Interface IP address should be 10.1.1.1. This address should also be excluded from the DHCP server's address pool so that it is not assigned to a DHCP client.

Planning the DHCP setup for on-site and PPP clients

Table 3. Global configuration options (applies to all clients served by the DHCP server)

Object		**Value**
Configuration options	option 1: Subnet mask	255.255.255.0
	option 6: Domain name server	10.1.1.1
	option 15: Domain name	mycompany.com
Is the system performing DNS updates?		No
Is the system supporting BOOTP clients?		No

Table 4. Subnet for both on-site and dial-in clients

Object		**Value**
Subnet Name		MainNetwork
Addresses to manage		10.1.1.3 - 10.1.1.150
Lease time		24 hours (default)
Configuration options	Inherited options	Options from Global configuration
Subnet addresses not assigned by server		10.1.1.1 (Local interface address specified in the TCP/IP Settings of the Receiver Connection Profile properties in iSeries Navigator)

Other setup

- Set the Remote IP address method to DHCP in the PPP receiver connection profile.
  1. Enable DHCP WAN client connection with a DHCP server or relay connection using the Services menu item for Remote Access Services in iSeries Navigator.
  2. Select to Use DHCP for the IP address assignment method under the TCP/IP Settings Properties of the Receiver Connection Profile in iSeries Navigator.
- Allow remote system to access other networks (IP forwarding) under the TCP/IP Settings Properties of the Receiver Connection Profile in iSeries Navigator.
- Enable IP datagram forwarding under the Settings Properties of the TCP/IP Configuration in iSeries Navigator.

Example: DHCP and PPP profile on different System i models

This example explains how to set up two System i models as the network Dynamic Host Configuration Protocol (DHCP) server and a BOOTP/DHCP relay agent for two LANs and remote dial-in clients.

The example about PPP and DHCP on a single System i model shows how to use PPP and DHCP on a single system to permit dial-in clients access to a network. If you are concerned with the physical layout of your network or with security, it might be better to have the PPP and DHCP servers separated or to have a dedicated PPP server without DHCP services. The following figure represents a network that has dial-in clients with the PPP and DHCP policies on different servers.

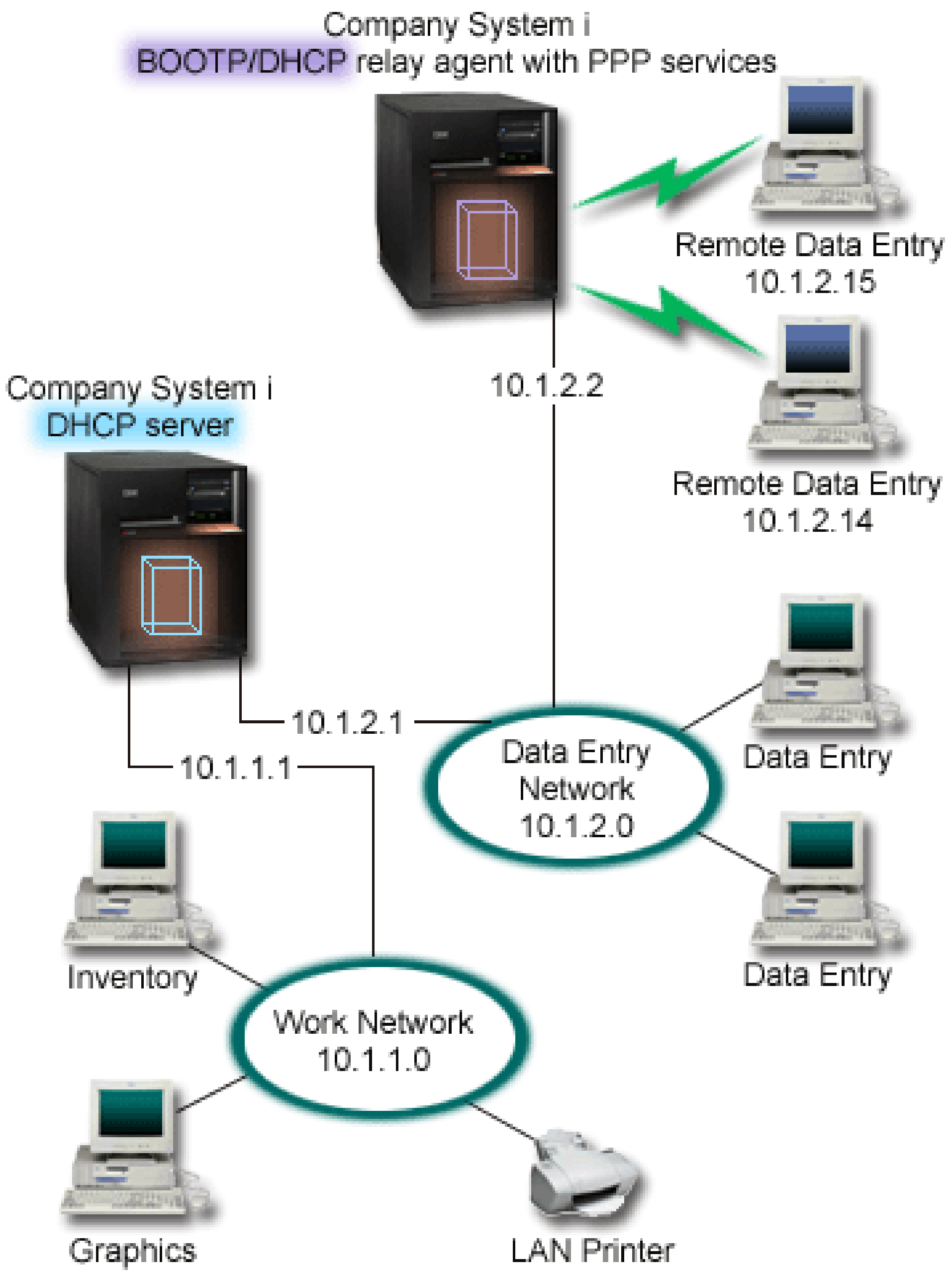


Figure 2. DHCP and PPP profile on different System i models

The remote data entry clients dial into the System i PPP server. The PPP profile on that server must have a remote IP address method of DHCP, such as in the example about PPP and DHCP on a single System i model as well as IP forwarding in the PPP profile and in the TCP/IP stack properties. Furthermore, because this server is acting as a DHCP relay agent, the BOOTP/DHCP relay agent must be on. This allows the System i Remote Access server to pass on DHCP DISCOVER packets to the DHCP server. The DHCP server then responds and distributes TCP/IP information to the dial-in clients through the PPP server.

The DHCP server is responsible for distributing IP addresses to both the 10.1.1.0 and 10.1.2.0 networks. In the data entry network, the DHCP server gives out IP addresses from 10.1.2.10 to 10.1.2.40 to either dial-in or directly attached network clients. The data entry clients also need a router address (option 3) of 10.1.2.1 to communicate with the work network, and the System i DHCP server must also have IP forwarding enabled.

Also, the Local Interface IP address in the PPP profile must be an IP address that falls within the subnet definition in the DHCP server. In this example, the PPP profile Local Interface address should be 10.1.2.2. This address should also be excluded from the DHCP server's address pool so that it is not assigned to a DHCP client. The Local Interface IP address must be an address to which the DHCP server can send reply packets to.

Planning the DHCP setup for DHCP with a DHCP relay agent

Table 5. Global configuration options (applies to all clients served by the DHCP server)

Object		Value
Configuration options	option 1: Subnet mask	255.255.255.0
	option 6: Domain name server	10.1.1.1
	option 15: Domain name	mycompany.com
Is the system performing DNS updates?		No
Is the system supporting BOOTP clients?		No

Table 6. Subnet for Work Network

Object		Value
Subnet name		WorkNetwork
Addresses to manage		10.1.1.3 - 10.1.1.150
Lease time		24 hours (default)
Configuration options	Inherited options	Options from Global configuration
Subnet addresses not assigned by server		none

Table 7. Subnet for Data Entry Network

Object		Value
Subnet Name		DataEntry
Addresses to manage		10.1.2.10 - 10.1.2.40
Lease time		24 hours (default)
Configuration options	option 3: Router	10.1.2.1
	Inherited options	Options from Global configuration
Subnet addresses not assigned by server		10.1.2.1 (Router) 10.1.2.15 (Remote Data Entry client's local interface IP address) 10.1.2.14 (Remote Data Entry client's local interface IP address)

Other setup on a System i platform running PPP

- Set up the BOOTP/DHCP relay agent TCP/IP server

Object	Value
Interface address	10.1.2.2
Relay packets to Server IP address	10.1.2.1

- Set the Remote IP address method to DHCP in the PPP receiver connection profile

1. Enable DHCP WAN client connection with a DHCP server or relay connection using the Services menu item for Remote Access Services in iSeries Navigator
2. Select to Use DHCP for the IP address assignment method under the TCP/IP Settings Properties of the Receiver Connection Profile in iSeries Navigator

- Allow remote system to access other networks (IP forwarding) under the TCP/IP Settings Properties of the Receiver Connection Profile in iSeries Navigator (to allow the remote clients to communicate with the data entry network)
- Enable IP datagram forwarding under the Settings Properties of the TCP/IP Configuration in iSeries Navigator (to allow the remote clients to communicate with the data entry network)

Scenario: Protecting an L2TP voluntary tunnel with IPSec

In this scenario, you learn how to setup a connection between a branch office host and a corporate office that uses L2TP protected by IPSec. The branch office has a dynamically assigned IP address, while the corporate office has a static, globally routable IP address.

Situation

Suppose your company has a small branch office in another state. Throughout any given workday the branch office may require access to confidential information about an System i model within your corporate intranet. Your company currently uses an expensive leased line to provide the branch office access to the corporate network. Although your company wants to continue providing secure access to your intranet, you ultimately want to reduce the expense associated with the leased line. This can be done by creating a Layer 2 Tunnel Protocol (L2TP) voluntary tunnel that extends your corporate network, such that the branch office appears to be part of your corporate subnet. VPN protects the data traffic over the L2TP tunnel.

With an L2TP voluntary tunnel, the remote branch office establishes a tunnel directly to the L2TP network server (LNS) of the corporate network. The functionality of the L2TP access concentrator (LAC) resides at the client. The tunnel is transparent to the remote client's Internet Service Provider (ISP), so the ISP is not required to support L2TP. If you want to read more about L2TP concepts, see Layer 2 Tunnel Protocol (L2TP).

Important: This scenario shows the security gateways attached directly to the Internet. The absence of a firewall is intended to simplify the scenario. It does not imply that the use of a firewall is not necessary. Consider the security risks involved any time you connect to the Internet.

Objectives

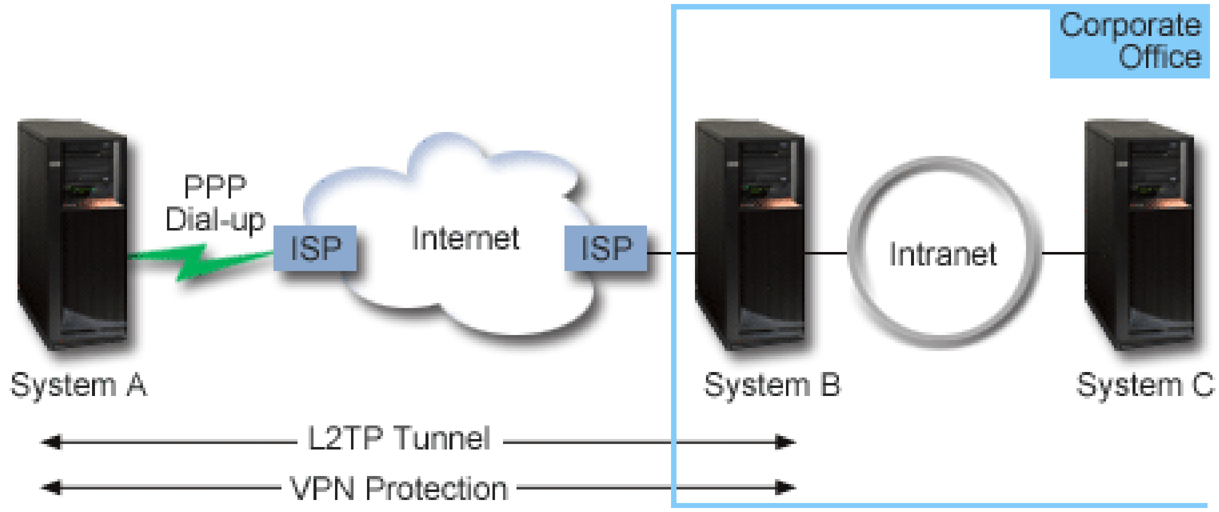
In this scenario, a branch office system connects to its corporate network through a gateway system with an L2TP tunnel protected by VPN.

The main objectives of this scenario are:

- The branch office system always initiates the connection to the corporate office.
- The branch office system is the only system at the branch office network that needs access to the corporate network. In other words, its role is that of a host, not a gateway, in the branch office network.
- The corporate system a host computer in the corporate office network.

Details

The following figure illustrates the network characteristics for this scenario:



System-A

- Must have access to TCP/IP applications on all systems in the corporate network.
- Receives dynamically assigned IP addresses from its ISP.
- Must be configured to provide L2TP support.

System-B

- Must have access to TCP/IP applications on System-A.
- Subnet is 10.6.0.0 with mask 255.255.0.0. This subnet represents the data endpoint of the VPN tunnel at the corporate site.
- Connects to the Internet with IP address 205.13.237.6. This is the connection endpoint. That is, System-B performs key management and applies IPSec to incoming and outgoing IP datagrams. System-B connects to its subnet with IP address 10.6.11.1.

In L2TP terms, *System-A* acts as the L2TP initiator, while *System-B* acts as the L2TP terminator.

Configuration tasks

Assuming that TCP/IP configuration already exists and works, you must complete the following tasks:

Scenario: Connecting your system to a PPPoE access concentrator

Many Internet service providers (ISPs) provide high-speed Internet access over a Digital Subscriber Line (DSL) using Point-to-Point Protocol over Ethernet (PPPoE). You can connect your system to these ISPs to provide high-bandwidth connections that preserve the benefits of Point-to-Point Protocol (PPP).

Situation

Your business requires a faster Internet connection, so you are interested in a Digital Subscriber Line (DSL) service with a local ISP. After an initial investigation, you find that your ISP uses PPPoE to connect its clients. You need to use this PPPoE connection to provide high-bandwidth Internet connections through your system.

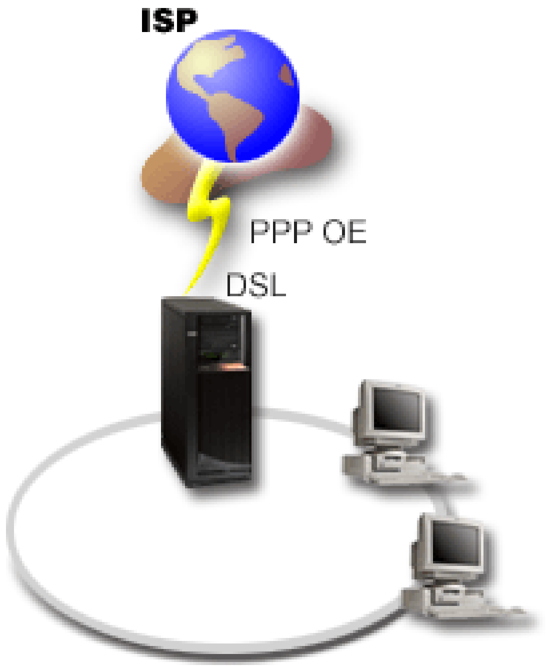


Figure 3. Connecting your system to an ISP with PPPoE

Solution

You can support a PPPoE connection to your ISP through your system. The system uses a new PPPoE virtual line type that is bound to a physical Ethernet line configured to use a type 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A, or 576A Ethernet adapter. This virtual line supports PPP session protocols over an Ethernet local area network (LAN), which is connected to a DSL modem that provides the gateway to the remote ISP. This gateway allows LAN-connected users to have high-speed Internet access using the PPPoE connection. After the connection between the system and the ISP has started, individual users on the LAN can access the ISP over PPPoE, using the IP address allocated to the system. To provide additional security, filter rules can be applied to the PPPoE virtual line to restrict certain inbound Internet traffic.

Sample configuration

To set up a sample PPP configuration from iSeries Navigator, follow these steps:

1. Configure the connection device for use with your ISP.
2. Configure an originator connection profile on your system.

   Ensure that you enter the following information:

   - **Protocol type**: `PPP`
   - **Connection type**: `PPP over Ethernet`
   - **Operating mode**: `Initiator`
   - **Link configuration**: `Single line`
3. On the General page of the New Point-to-Point Profile Properties, enter a name and description for the originator profile. This name refers to both the connection profile and the virtual PPPoE line.
4. Click **Connection** to open the Connection page. Choose the **PPPoE virtual line name** that corresponds to the name for this connection profile. After you select the line, iSeries Navigator displays the **line properties** dialog.
   a. On the General page, enter a meaningful description for the PPPoE virtual line.

b. Click **Link** to open the Link page. From the Physical Line Name select list, select the Ethernet line that this connection will use, and click **Open**. Alternately, if you need to define a new Ethernet line, type the line name and click **New**. iSeries Navigator displays the **Ethernet line properties** dialog.

| **Note:** PPPoE requires a type 2743, 2760, 2838, 2849, 287F, 5700, 5701, 5706, 5707, 573A, or 576A
| Ethernet adapter.

1) On the General page, enter a meaningful description for the Ethernet Line, and verify that the line definition is using the required hardware resources.
2) Click **Link** to open the Link page. Enter the properties for the physical Ethernet line. Refer to the documentation for your Ethernet adapter and the online help for more information.
3) Click **Other** to open the Other page. Specify the level of access and authority other users might have for this line.
4) Click **OK** to return to the PPPoE virtual line properties page.

c. Click **Limits** to define properties for LCP authentication, or click **OK** to return to New Point-to-Point Profile Connection page.

d. When you return to the Connection page, specify the PPPoE server addressing based on information provided by your ISP.

5. If your ISP requires the system to authenticate itself or if you want the system to authenticate the remote system, click **Authentication** to open the Authentication page and enter the requested information.
6. Click **TCP/IP Settings** to open the TCP/IP page, and specify the IP address handling parameters for this connection profile. The setting to be used should be provided by your ISP. To allow LAN attached users to connect to the ISP using the IP addresses allocated to the system, select **Hide addresses (Full masquerading)**.
7. Click **DNS** to open the DNS page, enter the IP address of the DNS server provided by the ISP.
8. If you want to specify the subsystem to run the connection job, click **Other** to open the Other page.
9. Click **OK** to complete the profile.

Related concepts

"Group policy support" on page 5
With group policy support, network administrators can define user-based group policies to manage resources. Individual users can be assigned access control policies when they log on to the Point-to-Point Protocol (PPP) or Layer Two Tunneling Protocol (L2TP) session.

Related tasks

"Creating a connection profile" on page 47
The first step in configuring a PPP connection between systems is to create a connection profile on the system.

Related reference

"Link configuration" on page 51
Link configuration defines the type of line service that your Point-to-Point Protocol (PPP) connection profile uses to establish a connection.

"System authentication" on page 44
PPP connections with a System i platform support several options for authenticating both remote clients dialing in to the system and connections to an ISP or another system that the system is dialing to.

"IP address handling" on page 42
Point-to-Point Protocol (PPP) connections enable several different sets of options for managing IP addresses depending on the type of connection profile.

"IP packet filtering" on page 42
IP packet filtering limits the services to individual users when they log on to a network.

Scenario: Connecting remote dial-in clients to your system

Remote users, such as telecommuters or mobile clients, often require access to a company's network. These dial-in clients can gain access to a system with Point-to-Point Protocol (PPP).

Situation

As an administrator of your company's network, you must maintain both your system and network clients. Instead of coming into work to troubleshoot and fix problems, you need the capability to work from a remote location, such as your home. Because your company does not have an Internet-bound network connection, you can dial into your system using a PPP connection. Additionally, the only modem you currently have is your 7852-400 electronic customer support modem and you need to use this modem for your connection.

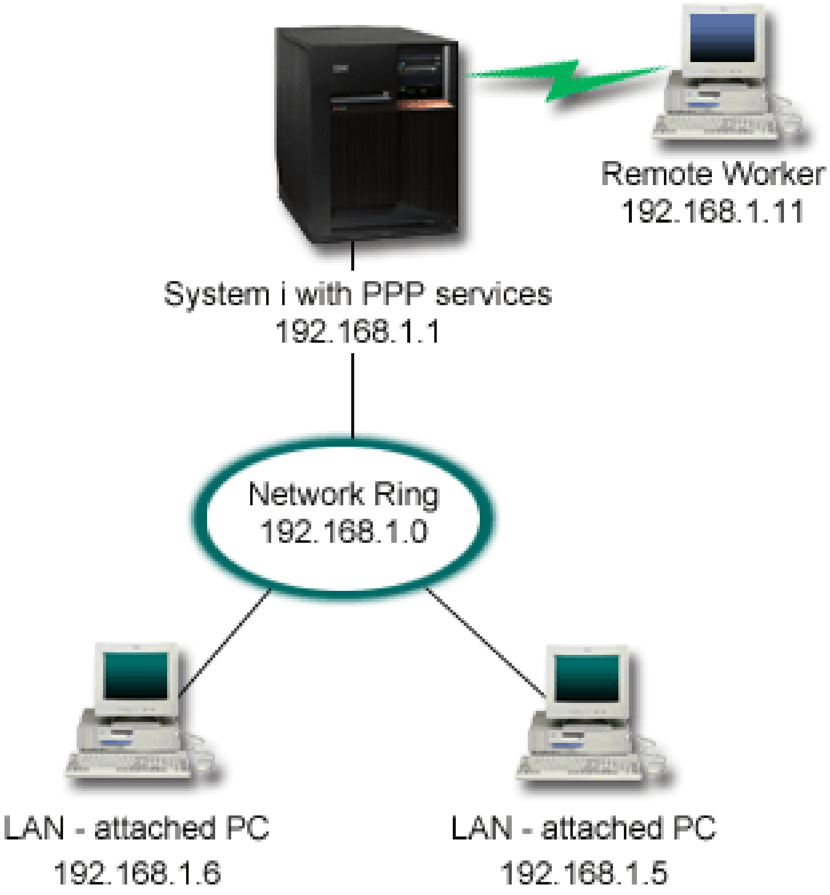


Figure 4. Connecting remote clients to your system

Solution

You can use PPP to connect your home PC to your system using your modem. Because you are using your electronic customer support modem for this type of PPP connection, you must ensure that your modem is configured for both synchronous and asynchronous modes. The figure shows a system with PPP services that is connected to a LAN with two PCs. The remote worker then dials into the system. The system authenticates itself and becomes part of the work network (`192.168.1.0`). In this case, it is easiest to assign a static IP address to the dial-in client.

The remote worker uses Challenge Handshake Authentication Protocol (CHAP-MD5) to authenticate with the system. The system cannot use MS_CHAP, so you must make sure that your PPP client uses CHAP-MD5.

If you want your remote workers to have access to the company network as implied above, IP forwarding needs to be set on in the TCP/IP stack as well as your PPP receiver profile, and IP routing must be configured correctly. If you want to limit or secure what actions your remote client can take in your network, you can use filtering rules to handle their IP packets.

The preceding figure only has one remote dial-in client, because the electronic customer support modem can only handle one connection at a time.

Sample configuration

To set up a sample PPP configuration from iSeries Navigator, follow these steps:

1. Configure Dial-up Networking and create a dial-up connection on the remote PC.
2. Configure a receiver connection profile on your system.

   Ensure that you enter the following information:

   - **Protocol type**: `PPP`
   - **Connection type**: `Switched-line`
   - **Operating mode**: `Answer`
   - **Link configuration**: `This might be single line, or a line pool, depending on your environment.`
3. On the General page of the New Point-to-Point Profile Properties, enter a name and description for the receiver profile.
4. Click **Connection** to open the Connection page. Choose the appropriate **Line name**, or create a new one by typing a new name, and clicking **New**.
   a. On the General page, highlight an existing hardware resource where your 7852–400 adapter is attached and set the Framing to **Asynchronous**.
   b. Click **Modem** to open the Modem page. From the Name select list, choose the **IBM 7852–400** modem.
   c. Click **OK** to return to New Point-to-Point Profile Properties page.
5. Click **Authentication** to open the Authentication page.
   a. Select **Require this iSeries server to verify the identity of the remote system**.
   b. Select **Authenticate locally using a validation list** and add a new remote user to the validation list.
   c. Select **Allow encrypted password (CHAP-MD5)**.
6. Click **TCP/IP Settings** to open the TCP/IP page.
   a. Select the local IP address of `192.168.1.1`.
   b. For the remote IP address, select **Fixed IP address** with a starting IP address of `192.168.1.11`.
   c. Select **Allow remote system to access other networks**.
7. Click **OK** to complete the profile.

   Related concepts

   “Planning PPP” on page 32
   Planning Point-to-Point Protocol (PPP) includes creating and administering PPP connections.

   Related tasks

   “Creating a connection profile” on page 47
   The first step in configuring a PPP connection between systems is to create a connection profile on the system.

Related reference

"Challenge Handshake Authentication Protocol with MD5" on page 45
Challenge Handshake Authentication Protocol (CHAP-MD5) uses an algorithm (MD-5) to calculate a value that is known only to the authenticating system and the remote device.

"Link configuration" on page 51
Link configuration defines the type of line service that your Point-to-Point Protocol (PPP) connection profile uses to establish a connection.

"Line pool" on page 52
To set the PPP connection to use a line from a line pool, select this line service. When the PPP connection starts, the system selects an unused line from the line pool. For dial on-demand profiles, the system does not select the line until it detects TCP/IP traffic for the remote system.

Scenario: Connecting your office LAN to the Internet with a modem

Administrators typically set up office networks for employees to access the Internet. Administrators can use a modem to connect the system to an Internet service provider (ISP). LAN-attached PC clients can communicate with the Internet using the i5/OS operating system as a gateway.

Situation

The corporate application that your company uses requires your users to access the Internet. Because the application does not require large amounts of data to be exchanged, you need to be able to use a modem to connect both your system and LAN-attached PC clients to the Internet. The following figure describes an example of this situation.

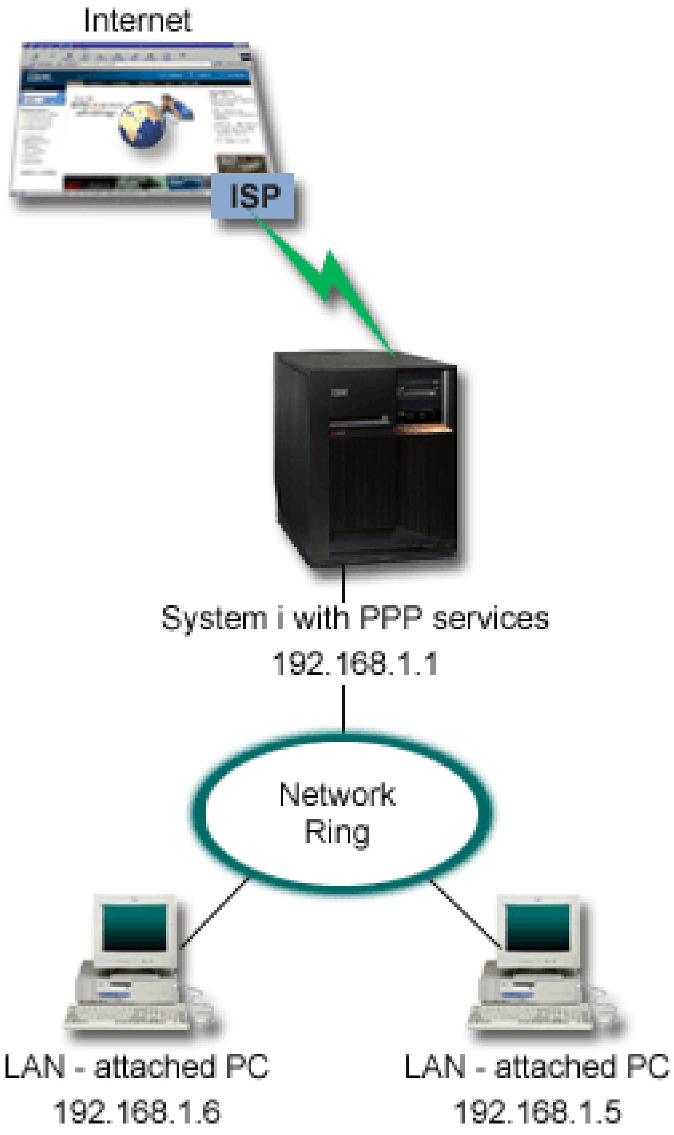


Figure 5. Connecting your office LAN to the Internet with a modem

Solution

You can use your integrated (or other compatible) modem to connect your system to your ISP. You need to create a Point-to-Point Protocol (PPP) originator profile on the system to establish the PPP connection to the ISP.

After you make the connection between the system and the ISP, your LAN-attached PCs can communicate with the Internet using the system as a gateway. In the originator profile, you need to make sure that the Hide addresses option is on, so that LAN clients that have private IP addresses can communicate with the Internet.

Now that your system and network is attached to the Internet, you must understand your security risks. Work with your ISP to understand their security policies and take further actions to protect your system and network.

Depending on your Internet usage, bandwidth might become a concern.

Sample configuration

To set up a sample configuration from iSeries Navigator, follow these steps:

1. Configure an originator connection profile on your system.

   Ensure that you select the following information:

   - **Protocol type**: `PPP`
   - **Connection type**: `Switched-line`
   - **Operating mode**: `Dial`
   - **Link configuration**: `This might be single line, or line pool, depending on your environment.`
2. On the General page of the New Point-to-Point Profile Properties, enter a name and description for the originator profile.
3. Click **Connection** to open the Connection page. Choose the appropriate Line name or create a new one by typing a new name and clicking **New**.
   a. On the General page of the new line properties, highlight an existing hardware resource. If you select an internal modem resource, then the modem type and framing type settings will be automatically selected.
   b. Click **OK** to return to New Point-to-Point Profile Properties page.
4. Click **Add**, and type the telephone number to dial to reach the ISP server. Ensure that you include any required prefix.
5. Click **Authentication** to open the Authentication page, select **Allow the remote system to verify the identity of this iSeries server**. Select the authentication protocol, and enter any required user name or password information.
6. Click **TCP/IP Settings** to open the TCP/IP page.
   a. Select **Assigned by remote system** for both local and remote IP addresses.
   b. Select **Add remote system as the default route**.
   c. Check **Hide addresses** so that your internal IP addresses are not routed on to the Internet.
7. Click **DNS** to open the Domain Name System (DNS) page, enter the IP address of the DNS server that is provided by the ISP.
8. Click **OK** to complete the profile.

To use the connection profile to connect to the Internet, right-click the connection profile from iSeries Navigator, and select **Start**. The connection is successful when the status changes to **Active**. Refresh to update the display.

Note: You must also ensure that the other systems in your network have proper routing defined, so that Internet bound TCP/IP traffic from these systems is sent through the system.

Related concepts

"Planning PPP" on page 32
Planning Point-to-Point Protocol (PPP) includes creating and administering PPP connections.

Related tasks

"Creating a connection profile" on page 47
The first step in configuring a PPP connection between systems is to create a connection profile on the system.

Related reference

"Line pool" on page 52
To set the PPP connection to use a line from a line pool, select this line service. When the PPP connection starts, the system selects an unused line from the line pool. For dial on-demand profiles, the system does not select the line until it detects TCP/IP traffic for the remote system.

“Link configuration” on page 51
Link configuration defines the type of line service that your Point-to-Point Protocol (PPP) connection profile uses to establish a connection.

Scenario: Connecting your corporate and remote networks with a modem

A modem enables two remote locations (such as a central office and a branch office) to exchange data between them. Point-to-Point Protocol (PPP) can connect two LANs together by establishing a connection between a system in the central office and another one in the branch office.

Situation

Suppose that you have a branch and corporate networks in two different locations. Every day the branch office needs to connect with the corporate office to exchange database information for their data entry applications. The amount of data exchanged does not constitute the purchase of a physical network connection, so you decide to use modems to connect the two networks as required.

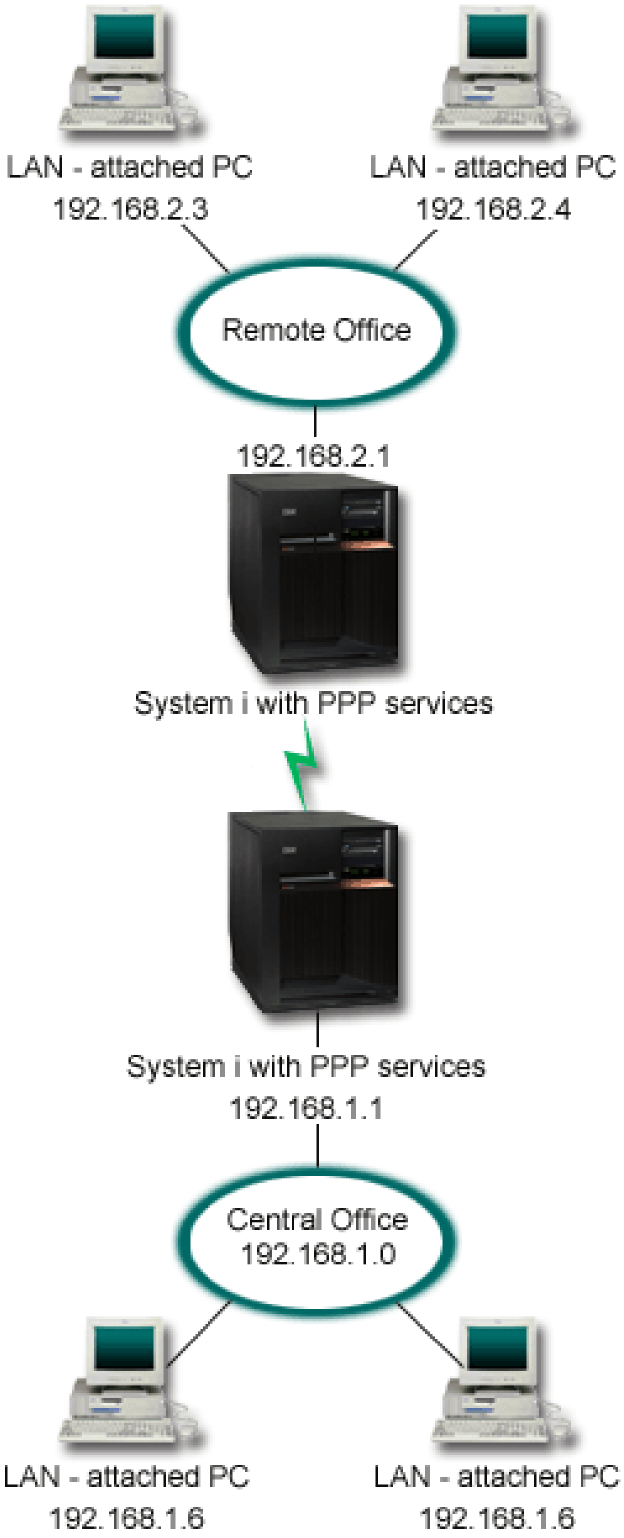


Figure 6. Connecting your corporate and remote networks with a modem

Solution

PPP can connect two LANs together by establishing a connection between the systems as shown in the figure. In this case, assume that the remote office initiates the connection to the central office. You configure an originator profile on the remote system and a receiver profile on the central office system.

If the remote office PCs need access to the corporate LAN (192.168.1.0), the central office receiver profile will need IP forwarding turned on and IP address routing should be enabled for the PCs (192.168.2, 192.168.3, 192.168.1.6, and 192.168.1.5 in this example). Also, IP forwarding for the TCP/IP stack must be activated. This configuration enables basic TCP/IP communication between the LANs. You should consider security factors and DNS to resolve host names between the LANs.

Sample configuration

To set up a sample configuration from iSeries Navigator, follow these steps:

1. Configure an originator connection profile on the remote office system.

   Ensure that you select the following information:

   - **Protocol type**: `PPP`
   - **Connection type**: `Switched-line`
   - **Operating mode**: `Dial`
   - **Link configuration**: `This might be single line, or line pool, depending on your environment.`
2. On the General page of the New Point-to-Point Profile Properties, enter a name and description for the originator profile.
3. Click **Connection** to open the Connection page. Choose the appropriate Line name or create a new one by typing a new name and clicking **New**.
   a. On the General page of the new line properties, highlight an existing hardware resource and set the Framing to **Asynchronous**.
   b. Click **Modem** to open the Modem page. From the Name select list, choose the modem that you are using.
   c. Click **OK** to return to New Point-to-Point Profile Properties page.
4. Click **Add** and type the telephone number to reach the central office system. Ensure that you include any required prefixes.
5. Click **Authentication** to open the Authentication page, and select **Allow the remote system to verify the identity of this iSeries server**. Select **Require encrypted password (CHAP-MD5)**, and enter the required user name and password information.
6. Click **TCP/IP Settings** to open the TCP/IP Settings page.
   a. For Local IP address, select the IP address of the remote office LAN interface (192.168.2.1) from the **Use fixed IP address** select box.
   b. For the remote IP address, choose **Assigned by remote system**.
   c. In the routing section, select **Add remote system as the default route**.
   d. Click **OK** to complete the originator profile.
7. Configure a receiver connection profile on the central office system.

   Ensure that you select the following information:

   - **Protocol type**: `PPP`
   - **Connection type**: `Switched-line`
   - **Operating mode**: `Answer`
   - **Link configuration**: `This might be single line, or line pool, depending on your environment.`

8. On the General page of the New Point-to-Point Profile Properties, enter a name and description for the receiver profile.
9. Click **Connection** to open the Connection page. Choose the appropriate Line name or create a new one by typing a new name and clicking **New**.
   a. On the General page, highlight an existing hardware resource and set the Framing to **Asynchronous**.
   b. Click **Modem** to open the Modem page. From the Name select list, choose the modem that you are using.
   c. Click **OK** to return to New Point-to-Point Profile Properties page.
10. Click **Authentication** to open the Authentication page.
    a. Check **Require this iSeries server to verify the identity of the remote system**.
    b. Add a new remote user to the validation list.
    c. Check the CHAP-MD5 authentication.
11. Click **TCP/IP Settings** to open the TCP/IP Settings page.
    a. For the local IP address, select the IP address of the central office interface (192.168.1.1) from the **select** box.
    b. For the remote IP address, select **Based on remote system's user ID**. The **IP Addresses Defined By User Name** dialog will appear. Click **Add**. Fill in the fields for Caller user name, IP address, and Subnet mask. In our scenario, the following will be appropriate:
       - Caller user name: `Remote_site`
       - IP address: `192.168.2.1`
       - Subnet mask: `255.255.255.0`

       Click **OK**, and click **OK** again to return to the TCP/IP Settings page.
    c. Select **IP forwarding** to enable other systems in the network to use this system as a gateway.
12. Click **OK** to complete the receiver profile.

Related tasks

"Creating a connection profile" on page 47
The first step in configuring a PPP connection between systems is to create a connection profile on the system.

Related reference

"Link configuration" on page 51
Link configuration defines the type of line service that your Point-to-Point Protocol (PPP) connection profile uses to establish a connection.

"Line pool" on page 52
To set the PPP connection to use a line from a line pool, select this line service. When the PPP connection starts, the system selects an unused line from the line pool. For dial on-demand profiles, the system does not select the line until it detects TCP/IP traffic for the remote system.

Scenario: Authenticating dial-up connections with RADIUS NAS

A Network Access Server (NAS) running on the system can route authentication requests from dial-in clients to a separate Remote Authentication Dial In User Service (RADIUS) server. If authenticated, RADIUS can also control the IP addresses assigned to the user.

Situation

Your corporate network has remote users dialing into two systems from a distributed dial-up network. You need to centralize authentication, service, and accounting, allowing one system to handle requests for validating user IDs and passwords and for determining which IP addresses are assigned to them.

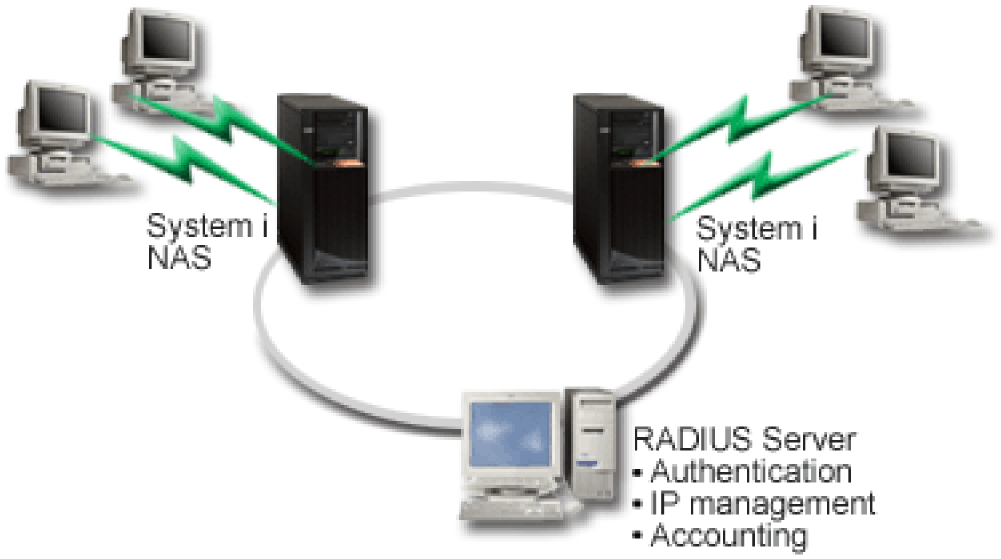


Figure 7. Authenticating dial up connections with a RADIUS server

Solution

When users attempt to connect, the NAS running on the systems forwards the authentication information to a RADIUS server on the network. The RADIUS server, which maintains all authentication information for your network, processes the authentication request and responds. If the user is validated, the RADIUS server can also be configured to assign the peers's IP address, and can activate accounting to track user activity and usage. To support RADIUS, you must define the RADIUS NAS server on the system.

Sample configuration

To set up a sample configuration from iSeries Navigator, follow these steps:

1. In iSeries Navigator, expand **Network**, right-click **Remote Access Services** and select **Services**.
2. On the **RADIUS** tab, select **Enable RADIUS Network Access Server connection**, and **Enable RADIUS for authentication**. Depending on your RADIUS solution, you can also choose to have RADIUS handle connection accounting and TCP/IP address configuration.
3. Click the **RADIUS NAS settings** button.
4. On the General page, enter a description for this server.
5. On the Authentication Server (and optionally Accounting Server) pages, click **Add** and enter the following information:
   a. In the **Local IP address** box, enter the IP address for the interface that is used to connect to the RADIUS server.
   b. In the **Server IP address** box, enter the IP address for the RADIUS server.
   c. In the **Password** box, enter the password that is used to identify the system to the RADIUS server.
   d. In the **Port** box, enter the port on the system that is used to communicate with the RADIUS server. The defaults are port 1812 for the authentication server or 1813 for the accounting server.
6. Click **OK**.
7. In iSeries Navigator, expand **Network** → **Remote Access Services**.
8. Select the Connection profile that will use the RADIUS server for authentication. RADIUS services are only applicable for receiver connection profiles.

9. On the Authentication page, select **Require this iSeries server to verify the identity of the remote system**.
10. Select **Authenticate remotely using a RADIUS server**.
11. Select the authentication protocol. (PAP, or CHAP-MD5) This protocol must also be used by the RADIUS server.
12. Select **Use RADIUS for connection editing and accounting**.
13. Click **OK** to save the change to the connection profile.

You must also setup the RADIUS server, including support for the authentication protocol, user data, passwords, and accounting information. Refer to your RADIUS vendor for more information.

When users dial in using this connection profile, the system forwards the authentication information to the specified RADIUS server. If the user is validated, the connection is allowed, and uses any connection restrictions specified in the user's information about the RADIUS server.

Related tasks

"Enabling RADIUS and DHCP services for connection profiles" on page 61
Here are the steps for enabling RADIUS or Dynamic Host Configuration Protocol (DHCP) services for PPP receiver connection profiles.

Related reference

"System authentication" on page 44
PPP connections with a System i platform support several options for authenticating both remote clients dialing in to the system and connections to an ISP or another system that the system is dialing to.

"Remote Authentication Dial In User Service overview" on page 46
Remote Authentication Dial In User Service (RADIUS) is an Internet standard protocol that provides centralized authentication, accounting and IP management services for remote access users in a distributed dial-up network.

Scenario: Managing remote user access to resources using group policies and IP filtering

Group access policies identify distinct user groups for a connection, and allow you to apply common connection attributes and security settings to the entire group. You can use group policies, along with IP filtering, to permit and restrict access to specific IP addresses on your network.

Situation

Your network has several groups of distributed users, each of whom needs access to different resources on your corporate LAN. A group of data entry users needs access to the database and several other applications. A group of people from other companies needs dial-up access to HTTP, File Transfer Protocol (FTP), and Telnet services, but for security reasons, this group must not be allowed access to other TCP/IP services or traffic. Defining detailed connection attributes and permissions for each user duplicates your efforts, and providing network restrictions for all the users of this connection profile does not ensure enough control. You want a way to define connection settings and permissions for several distinct groups of users who routinely dial into this system.

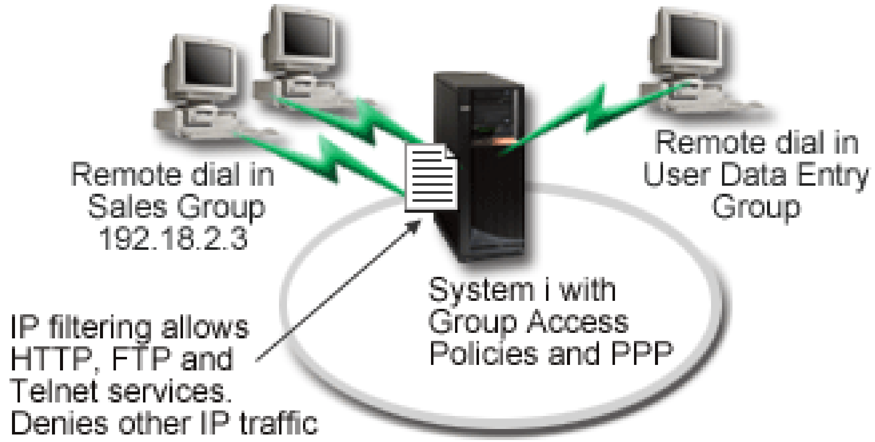


Figure 8. Applying connection settings to dial-up connections based on group policy settings

Solution

You need to apply unique IP filtering restrictions to two different groups of users. To accomplish this, you create group access policies and IP filter rules. Group access policies reference IP filter rules, so you must create your filter rules first. In this example, you need to create a PPP filter to include IP filter rules for the IBM Business Partner Group Access Policy. These filter rules permit HTTP, FTP, and Telnet services, but restrict access to all other TCP/IP traffic and services through the system. This scenario only shows the filter rules needed for the sales group; however, you can also set up similar filters for the Data Entry group.

Finally, you need to create the group access policies (one per group) to define your group. A group access policy enables you to define common connection attributes to a group of users. By adding a group access policy to a validation list on the system, you can apply these connection settings during the authentication process. The group access policy specifies several settings for the user’s session, including the ability to apply IP filtering rules that restrict the IP addresses and TCP/IP services available to a user during the session.

Sample configuration

To set up a sample configuration from iSeries Navigator, follow these steps:

1. Create the Point-to-Point Protocol (PPP) filter identifier and IP packet rules filters that specify the permissions and restrictions for this group access policy.
   a. In iSeries Navigator, expand **Network** → **Remote Access Services**.
   b. Click **Receiver Connection Profiles**, and select Group Access Policies.
   c. Right-click a predefined group listed in the right pane and select **Properties**.

      Note: If you want to create a new group access policy, right-click **Group Access Policies** and select **New Group Access Policies**. Complete the **General** tab. Then select the **TCP/IP Settings** tab and continue with step e below.
   d. Select the **TCP/IP Settings** tab, and click **Advanced**.
   e. Select **Use IP packet rules for this connection**, and click **Edit Rules File**. This will start the IP Packet Rules Editor, and open the PPP filters packet rules file.
   f. Open the **Insert** menu, and select **Filters** to add filter sets. Use the **General** tab to define the filter sets, and the **Services** tab to define the service you are permitting, such as HTTP. The following

filter set, ″services_rules,″ will permit HTTP, FTP and Telnet services. The filter rules include an implicit default deny statement, restricting any TCP/IP services or IP traffic not specifically permitted.

Note: The IP addresses in the following example are globally routable, and are for example purposes only.

```
###The following 2 filters will permit HTTP (Web browser) traffic in & out of the system.

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

###The following 4 filters will permit FTP traffic in & out of the system.

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
###The following 2 filters will permit telnet traffic in & out of the system.

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. Open the **Insert** menu, and select **Filter Interface**. Use the filter interface to create a PPP filter identifier, and include the filter sets you've defined.

   1) On the **General** tab, enter `permitted_services` for the PPP filter identifier.

   2) On the **Filter sets** tab, select the filter set **services_rules**, and click **Add**.

   3) Click OK. The following line will be added to the rules file:

      ```
      ###The following statement binds (associates) the 'services_rules' filter set with the
      PPP filter ID "permitted_services." This PPP filter ID
      can then be applied to the physical interface associated with a PPP connection profile
      or Group Access Policy.

      FILTER_INTERFACE PPP_FILTER_ID = permitted_services SET = services_rules
      ```

h. Save your changes, and exit. If you need to undo these changes later, use the character-based interface to enter the command `RMVTCPTBL *ALL`. This command removes all filter rules and NAT on the system.

i. On the **Advanced TCP/IP settings** dialog, leave the **PPP filter identifier** box blank, and click **OK** to exit. Later, you should apply the filter identifier you just created to a group access policy, not this connection profile.

2. Define a new group access policy for this user group.

a. In iSeries Navigator, expand **Network** → **Remote Access Services** → **Receiver Connection Profiles**.

b. Right click the **Group Access Policy** icon, and select **New Group Access Policy**. iSeries Navigator will display the **New Group Access Policy definition** dialog.

c. On the General page, enter a name and description for the group access policy.

d. On the TCP/IP settings page:

- Select **Use IP packet rules for this connection**, and select the PPP filter identifier **permitted_services**.

e. Select **OK** to save the group access policy.

3. Apply the group access policy to the users associated with this group.

a. Open the receiver connection profile controlling these dial-up connections.

b. On the Authentication page of the receiver connection profile, select the validation list that contains the users' authentication information, and click **Open**.

c. Select a user in the Sales group to which you want to apply the group access policy, and click **Open**.

d. Click **Apply a Group Policy to the user**, and select the group access policy defined in step 2.

e. Repeat for each Sales user.

Related concepts

"Configuring a group access policy" on page 60
The **Group Access Policies** folder under Receiver Connection Profiles provides options for configuring point-to-point connection parameters that apply to a group of remote users. It applies only to those point-to-point connections that originate from a remote system and are received by the local system.

"Group policy support" on page 5
With group policy support, network administrators can define user-based group policies to manage resources. Individual users can be assigned access control policies when they log on to the Point-to-Point Protocol (PPP) or Layer Two Tunneling Protocol (L2TP) session.

Related tasks

"Creating a connection profile" on page 47
The first step in configuring a PPP connection between systems is to create a connection profile on the system.

"Applying IP packet filtering rules to a PPP connection" on page 61
You can use a packet rules file to restrict the access of a user or a group to IP addresses on your network.

Related reference

"Validation list" on page 46
A validation list is used to store user ID and password information about remote users.

"System authentication" on page 44
PPP connections with a System i platform support several options for authenticating both remote clients dialing in to the system and connections to an ISP or another system that the system is dialing to.

Related information

IP filtering and network address translation

Scenario: Sharing a modem between logical partitions using L2TP

You have virtual Ethernet set up across four logical partitions. You want selected logical partitions to share a modem to access an external LAN.

Situation

You are the system administrator at a medium-sized company. It is time to update your computer equipment, but you want to do more than that; you want to streamline your hardware. You start the process by consolidating the work of three old systems onto one new system. You create three logical partitions on the system. The new system comes with a 2793 internal modem. This is the only input/output processor (IOP) you have that supports Point-to-Point Protocol (PPP). You also have an old 7852–400 electronic customer support modem.

Solution

Multiple systems and partitions can share the same modems for dial-up connections, eliminating the need for each system or partition to have its own modem. This is possible if you use L2TP tunnels and configure L2TP profiles that allow outgoing calls. In your network, the tunnels will run over a virtual Ethernet network and a physical network. The physical line is connected to another system that shares the modems in your network.

Details

The following figure illustrates the network characteristics for this scenario:

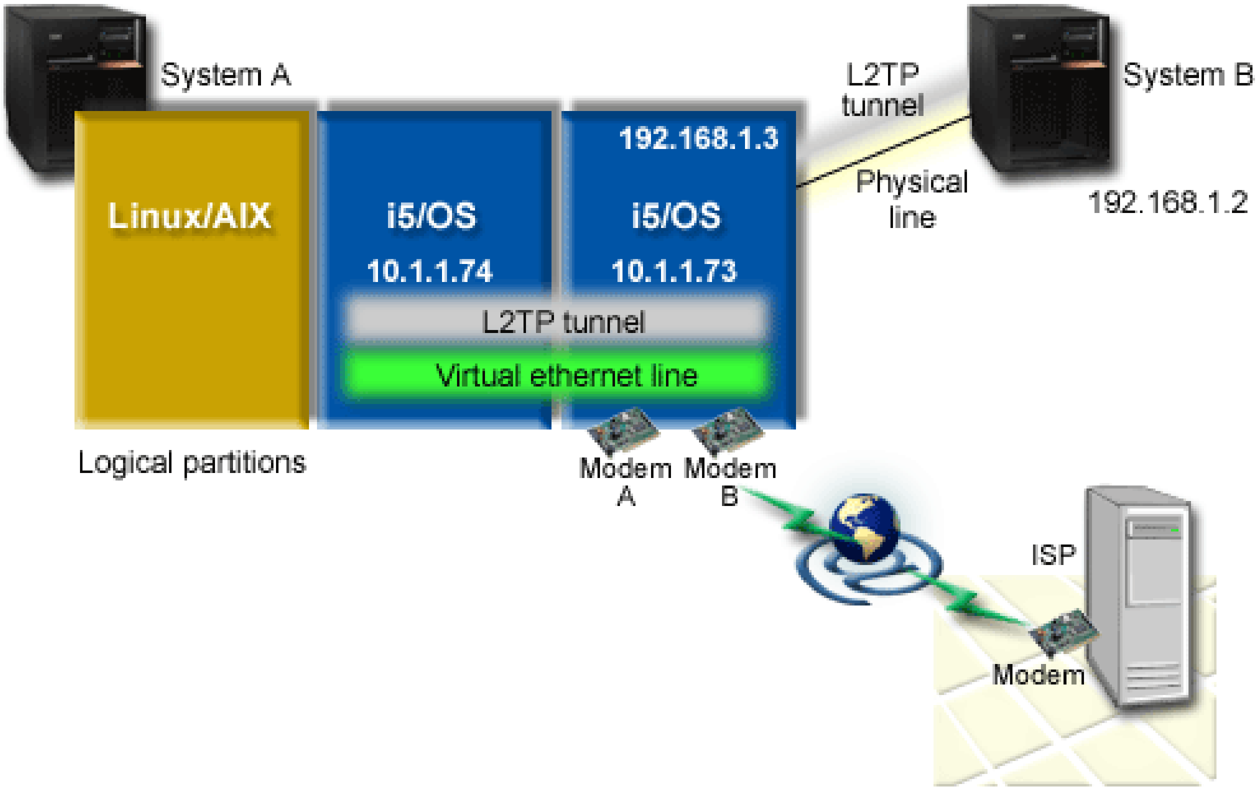


Figure 9. Multiple systems sharing the same modem for dial-up connections

Prerequisites and assumptions

System A must meet the following setup requirements:

- i5/OS Version 5 Release 3 or later, installed on the partition that owns the ASYNC capable modems
- Hardware that allows you to partition.
- iSeries Access for Windows® and iSeries Navigator (Configuration and Service component of iSeries Navigator), Version 5 Release 3, or later,

- You have created at least two logical partitions (LPAR) on the system. The partition that owns the modem must have i5/OS V5R3, or later, installed. The other partitions can have OS/400® V5R2, i5/OS V5R3, Linux®, or AIX® installed. In this scenario, the partitions are either using the i5/OS or the Linux operating system.
- You have virtual Ethernet created to communicate across partitions. See the following scenario: Scenario: Creating a virtual Ethernet for interpartition communications.

System B must have the licensed program and relevant components of iSeries Navigator installed: iSeries Access for Windows and iSeries Navigator (Configuration and Service component of iSeries Navigator) V5R2, or later.

Related information

Logical partitions

Scenario details: Sharing a modem between logical partitions using L2TP

After you complete the prerequisites, you are ready to begin configuring the Layer Two Tunneling Protocol (L2TP) profiles.

Step 1: Configuring the L2TP terminator profile for any interface on the partition that owns the modems:

To create a terminator profile for any interface, follow these steps:

1. In iSeries Navigator, expand ***your system*** → **Network** → **Remote Access Services**.
2. Right-click **Receiver Connection Profiles**, and select **New Profile**.
3. Select the following options on the Setup page and click **OK**:
   - **Protocol type**: PPP
   - **Connection type**: L2TP (virtual line)
   - **Operating mode**: Terminator (network server)
   - **Type of line service**: Single line
4. On the **New Profile - General** tab, complete the following fields:
   - **Name**: toExternal
   - **Description**: Receiver connection to dial out
   - Select **Start profile with TCP**.
5. On the **New Profile - Connection** tab, complete the following fields.
   - **Local tunnel endpoint IP address**: ANY
   - **Virtual line name**: toExternal. This line has no associated physical interfaces. The virtual line describes various characteristics of this PPP profile. After the L2TP Line Properties window opens, click the **Authentication** tab and enter your system's host name. Click **OK** to return to the **Connection** tab on the New PPP Profile Properties window.
6. Click **Allow out-going call establishment**. The **Outgoing call dial properties** dialog appears.
7. On the Outgoing Call Dial Properties page, select a line service type.
   - **Type of line service**: Line pool
   - **Name**: dialOut
   - Click **New**. The **New Line Pool Properties** dialog appears.
8. On the New line pool properties window, select the lines and modems to which you will allow the outgoing calls and click **Add**. If you need to define these lines, select **New Line**. The interfaces on the partition which owns these modems will try to use whichever line is open from this line pool. The new Line Properties window opens.
9. On the **New Line Properties - General** tab, enter information in the following fields:
   - **Name**: line1
   - **Description**: first line and first modem for line pool (2793 internal modem)

- **Hardware resource**: cmn03 (communication port)

10. Accept the defaults on all other tabs and click **OK** to return to the New Line Pool Properties window.
11. On the New Line Pool Properties window, select the lines and modems to which you will allow the outgoing calls and click **Add**. Verify the 2793 modem is a selected for the pool.
12. Select **New Line** again to add the 7852–400 electronic customer support modem. The new Line Properties window opens.
13. On the **New Line Properties - General** tab, enter information in the following fields:
    - **Name**: line2
    - **Description**: second line and second modem for line pool (7852-400 external electronic customer support modem)
    - **Hardware resource**: cmn04 (V.24 port)
    - **Framing**: Asynchronous
14. On the **New Line Properties - Modem** tab, select the external modem (7852–400) and click **OK** to return to the New Line Pool Properties window.
15. Select any other available lines you want to add to the line pool and click **Add**. In this example, verify the two new modems you added above are listed under the **Selected lines for pool** field and click **OK** to return to the Outgoing Call Dial Properties window.
16. On the Outgoing Call Dial Properties window, enter the `Default Dial Numbers` and click **OK** to return to the New PPP Profile Properties window.

    Note: These numbers might be something like your Internet service provider (ISP) which is going to be frequently called by the other systems using these modems. If the other systems specify a telephone number of *PRIMARY or *BACKUP, the actual numbers dialed will be the ones specified here. If the other systems specify an actual telephone number, the telephone number will be used instead.
17. On the **TCP/IP Settings** tab, select the following values:
    - **Local IP address**: None
    - **Remote IP address**: None

    Note: If you want to use the profile to end L2TP sessions, you need to pick the local IP address that represents the system. For the remote IP address, you can select an address pool that is in the same subnet as your system. All L2TP sessions get their IP addresses from this pool.
18. On the **Authentication** tab, accept all default values.

You are now finished configuring an L2TP terminator profile on the partition with the modems. The next step is to configure an L2TP remote dial, the originator profile for 10.1.1.74.

Related reference

"Multiple-connection profile support" on page 53
Point-to-point connection profiles that support multiple connections enable you to have one connection profile that handles many digital, analog, or L2TP calls.

Step 2: Configuring an L2TP originator profile on 10.1.1.74:

These steps guide you to create a Layer Two Tunneling Protocol (L2TP) originator profile:

1. In iSeries Navigator, expand **10.1.1.74** → **Network** → **Remote Access Services**.
2. Right-click **Originator Connection Profiles**, and select **New Profile**.
3. Select the following options on the Setup page and click **OK**:
    - **Protocol type**: PPP
    - **Connection type**: L2TP (virtual line)

- **Operating mode**: Remote dial
- **Type of line service**: Single line

4. On the **General** tab, complete the following fields:
   - **Name**: toModem
   - **Description**: originator connection going to partition owning modem
5. On the **Connection** tab, complete the following fields:

   Virtual line name: toModem. This line has no associated physical interface. The virtual line describes various characteristics of this PPP profile. The L2TP Line Properties window opens.
6. On the **General** tab, enter a description for the virtual line.
7. On the **Authentication** tab, enter the local host name of the partition and click **OK** to return to the Connection page.
8. In the **Remote telephone numbers** field, add `*PRIMARY` and `*BACKUP`. This allows the profile to use the same telephone numbers as the terminator profile on the partition owning the modems.
9. In the **Remote tunnel endpoint host name or IP address** field, enter the remote tunnel endpoint IP address (`10.1.1.73`).
10. On the **Authentication** tab, select **Allow the remote system to verify the identity of this iSeries server**.
11. Under Authentication protocol to use, select **Require encrypted password (CHAP-MD5)**. By default, **Allow extensible authentication protocol** is also selected.

    Note: The protocol should match whatever protocol the system to which you are dialing uses.
12. Enter your user name and password.

    Note: The user name and password need to match whatever the valid user name and password are on the system to which you are dialing.
13. Go to the **TCP/IP Settings** tab and verify the required fields:
    - **Local IP address**: Assigned by remote system
    - **Remote IP address**: Assigned by remote system
    - **Routing**: No additional routing is required
14. Click **OK** to save the PPP profile.

Step 3: Configuring an L2TP remote dial profile for 192.168.1.2:

You can configure a Layer Two Tunneling Protocol (L2TP) remote dial profile for 192.168.1.2 by repeating Step 2 and changing the remote tunnel endpoint to 192.168.1.3 (the physical interface to which System B connects).

Note: These are fictitious IP addresses and used for example purposes only.

Step 4: Testing the connection:

After you finish configuring both systems, you should test the connectivity to ensure that the systems are sharing the modem to reach external networks.

1. Ensure that the Layer Two Tunneling Protocol (L2TP) terminator profile is active.
   a. In iSeries Navigator, expand **10.1.1.73** → **Network** → **Remote Access Services** → **Receiver Connection Profiles**.
   b. In the right pane, find the required profile (toExternal) and verify the **Status** field is Active. If not, right-click the profile and select **Start**.
2. Start the Remote dial profile on 10.1.1.74.

a. In iSeries Navigator, expand **10.1.1.74** → **Network** → **Remote Access Services** → **Originator Connection Profiles**.

b. In the right pane, find the required profile (toModem) and verify the **Status** field is Active. If not, right-click the profile and select **Start**.

3. Start the remote dial profile on System B.

   a. In iSeries Navigator, expand **192.168.1.2** → **Network** → **Remote Access Services** → **Originator Connection Profiles**.

   b. In the right pane, find the profile you created and verify the **Status** field is Active. If not, right-click the profile and select **Start**.

4. If possible, ping the Internet service provider (ISP) or other destination that you've dialed to verify both profiles are active. You will attempt the ping from both 10.1.1.74 and 192.168.1.2.

5. As an alternative, you can also check the connection status.

   a. In iSeries Navigator, expand **the system** → **Network** → **Remote Access Services** → **Originator Connection Profiles**.

   b. In the right pane, right-click the profile you created and select **Connections**. On the Connection Status window you can see which profiles are active, inactive, connecting, and more.

Planning PPP

Planning Point-to-Point Protocol (PPP) includes creating and administering PPP connections.

Related reference

"Scenario: Connecting remote dial-in clients to your system" on page 14
Remote users, such as telecommuters or mobile clients, often require access to a company's network. These dial-in clients can gain access to a system with Point-to-Point Protocol (PPP).

"Scenario: Connecting your office LAN to the Internet with a modem" on page 16
Administrators typically set up office networks for employees to access the Internet. Administrators can use a modem to connect the system to an Internet service provider (ISP). LAN-attached PC clients can communicate with the Internet using the i5/OS operating system as a gateway.

"Related information for PPP" on page 66
Listed below are the IBM Redbooks (in PDF format) that provide additional information about Remote Access Services PPP connections. You can view or print the PDFs.

Software and hardware requirements

A Point-to-Point Protocol (PPP) environment requires that you have two or more computers that support PPP. One of these computers, the System i platform, can either be the originator or receiver.

The system must meet the following prerequisites so that the remote systems can access it.

- iSeries Navigator with TCP/IP support.
- One of the two connection profiles:
  - An originator connection profile to handle outbound PPP connections
  - A receiver connection profile to handle inbound PPP connections
- A PC workstation console installed with iSeries Access for Windows 95 or later with iSeries Navigator.
- An installed adapter

  You can choose one from the following adapters:
  - 2699*: Two-line WAN input/output adapter (IOA)
  - 2720*: PCI WAN/Twinaxial IOA
  - 2721*: PCI Two-line WAN IOA
  - 2745*: PCI Two-line WAN IOA (replaces IOA 2721)
  - 2742*: Two-line IOA (replaces IOA 2745)

  - 2771: Two-port WAN IOA, with a V.90 integrated modem on port 1 and a standard communications interface on port 2. To use port 2 of the 2771 adapter, an external modem or ISDN terminal adapter with the appropriate cable is required.
  - 2772: Two-port V.90 integrated modem WAN IOA
  - 2743/2760/2838/2849/287F/5700/5701/5706/5707/573A/576A: Ethernet adapter for PPPoE connections.
  - 2793*: 576C (CCIN of Quartz), two-port WAN IOA, with a V.92 integrated modem on port 1 and a standard communications interface on port 2. To use port 2 of the 576C adapter, an external modem or ISDN terminal adapter with appropriate cable is required. This replaces IOA model 2771.
  - 2805 Four-port WAN IOA, with an integrated V.92 integrated analog modem. This replaces models 2761 and 2772.

  * These adapters require an external V.90 modem (or above), or Integrated Services Digital Network (ISDN) terminal adapter, and an RS-232 (EIA 232) or compatible cable.
- One of the following, depending on your connection type and line:
  - external or internal modem, or channel service unit (CSU)/data service unit (DSU)
  - integrated services digital network (ISDN) terminal adapter
- You need to make arrangements for a dial-up account with an Internet Service Provider (ISP) if you plan to connect to the Internet. Your ISP should give you the necessary telephone numbers and information for the Internet connection.

Related reference

"Connection profiles" on page 3
Point-to-Point connection profiles define a set of parameters and resources for specific Point-to-Point Protocol (PPP) connections. You can start profiles that use these parameter settings to dial-out (originate) or to listen for (receive) PPP connections.

"Modems" on page 39
Both external and internal modems can be used for Point-to-Point Protocol (PPP) connections.

"CSU/DSU" on page 40
A channel service unit (CSU) is a device that connects a terminal to a digital line. A data service unit (DSU) is a device that performs protective and diagnostic functions for a telecommunications line. Typically, the two devices are packaged as a single unit, CSU/DSU.

"ISDN terminal adapters" on page 40
Integrated Services Digital Network (ISDN) provides you with a digital connection that allows you to communicate by using any combination of voice, data, and video, among other multimedia applications.

Connection alternatives

Point-to-Point Protocol (PPP) can transmit datagrams over serial point-to-point links.

PPP enables interconnection of multiple vendor equipment and multiple protocols by standardizing point-to-point communications. The PPP data link layer uses High-level Data Link Control (HDLC)-like framing for encapsulating datagrams over both asynchronous and synchronous point-to-point telecommunication links.

PPP supports a wide range of link types, but Serial Line Internet Protocol (SLIP) supports only asynchronous link types. SLIP is generally employed only for analog links. Local telephone companies offer traditional telecommunications services in an ascending scale of capabilities and cost. These services use existing telephone company voice network facilities between the customer and the central office.

PPP links establish a physical connection between a local and remote host. Connected links provide dedicated bandwidth. They also come in a variety of data rates and protocols. With PPP links, you can choose from the following connection alternatives:

Analog telephone lines

The analog connection, which uses modems to carry data over leased or switched lines, sits at the bottom of the point-to-point scale.

Leased lines are full-time connections between two specified locations, while switched lines are regular voice-telephone lines. The fastest modems today operate at an uncompressed rate of 56 kbps. Given the signal-to-noise ratio on unconditioned voice-grade telephone circuits, though, this rate is often unattainable.

Modem manufacture claims of higher bit-per-second (bps) rates are typically based on a data compression (CCITT V.42bis) algorithm that is utilized by their modems. Although V.42bis has the potential to achieve as much as four-fold reduction in data volume, compression depends on the data and rarely reaches even 50%. Data already compressed or encrypted might even increase with V.42bis applied. X2 or 56Flex extends the bps rate to 56 kbps for analog telephone lines. This is a hybrid technology that requires one end of the PPP link to be digital while the opposite end is analog. Additionally, the 56 kbps applies only when you are moving data from the digital toward the analog end of the link. This technology is well suited for connections to ISPs with the digital end of the link and hardware at their location. Typically, you can connect to a V.24 analog modem over an RS-232 serial interface with an asynchronous protocol at rates up to 115.2 kbps.

The V.90 standard put an end to the K56flex/x2 compatibility issue. The V.90 standard is the result of a compromise among the x2 and K56flex camps in the modem industry. By viewing the public switched telephone network as a digital network, V.90 technology can accelerate data from the Internet to a computer at speeds of up to 56 kbps. V.90 technology differs from other standards because it digitally encodes data instead of modulating it as analog modems do. The data transfer is a asymmetrical method, so upstream transmissions (mostly keystroke and mouse commands from a computer to the central site, which require less bandwidth) continue to flow at the conventional rates of up to 33.6 kbps. Data sent from a modem is sent as an analog transmission that mirrors the V.34 Standard. Only the downstream data transfer takes advantage of the high-speed V.90 rates.

The V.92 standard improves on V.90 by allowing upstream rates of up to 48 kbps. Additionally, connection times can be reduced because of improvements in the hand-shaking process, and modems that support a hold feature can now remain connected while the telephone line accepts in coming call or uses call-waiting.

Digital service and Digital Data Services

You can use digital service and Digital Data Services (DDS) with Point-to-Point Protocol (PPP).

Digital service

With digital service, data travels all the way from the computer of the sender to the central office of the telephone company, to the long distance provider, to the central office, and then to the computer of the receiver in digital form. Digital signaling offers much more bandwidth and higher reliability than analog signaling. A digital signaling system eliminates many of the problems that analog modems must deal with, such as noise, variable line quality, and signal attenuation.

Digital Data Services

Digital Data Services (DDS) is the most basic of digital services. DDS links are leased, permanent connections, running at fixed rates of up to 56 kbps. This service is also commonly designated as DS0.

You can connect to DDS using a special box called *channel service unit/data service unit (CSU/DSU)*, which replaces the modem in an analog scenario. DDS has physical limitations that are primarily related to the distance between the CSU/DSU and the telephone company central office. DDS works best when distance is less than 9000 m (30 000 ft). Telephone companies can accommodate longer distances with signal extenders, but this service comes at a higher cost. DDS is best suited for connecting two sites that are served by the same central office. For long distance connections that span different central offices, mileage charges can quickly add up to make DDS impractical. In such cases, Switched-56 might be a better solution. Typically, you can connect to a DDS CSU/DSU over V.35, RS449, or X.21 serial interface with synchronous protocol at rates up to 56 kbps.

Related reference

"CSU/DSU" on page 40
A channel service unit (CSU) is a device that connects a terminal to a digital line. A data service unit (DSU) is a device that performs protective and diagnostic functions for a telecommunications line. Typically, the two devices are packaged as a single unit, CSU/DSU.

"Switched-56"
When you do not need a full-time connection, you can save money by using switched digital service, which is generally called *Switch-56 (SW56)*.

Switched-56

When you do not need a full-time connection, you can save money by using switched digital service, which is generally called *Switch-56 (SW56)*.

An SW56 link is similar to Digital Data Services (DDS) setup in that the data terminal equipment (DTE) connects to the digital service by way of channel service unit/data service unit (CSU/DSU). An SW56 CSU/DSU, however, includes a dialing pad from which you enter the telephone number of the remote host. You can use SW56 to make dial-up digital connections to any other SW56 subscriber anywhere in the country or across international borders.

An SW56 call is carried over the long distance digital network just like a digitized voice call. SW56 uses the same telephone numbers as the local telephone system, and usage charges are the same as those for business voice calls.

SW56 is only in North American networks, and it is limited to single channels that can only carry data. SW56 is an alternative for locations where ISDN is unavailable.

Typically, you can connect to an SW56 CSU/DSU over V.35 or RS 449 serial interface with synchronous protocol at rates up to 56 kbps. With a V.25bis call/answer unit, data and call control flow over a single serial interface.

Related reference

"Digital service and Digital Data Services" on page 34
You can use digital service and Digital Data Services (DDS) with Point-to-Point Protocol (PPP).

"Integrated Services Digital Network"
Integrated Services Digital Network (ISDN) provides switched end-to-end digital connectivity. ISDN can carry both voice and data over the same connection.

Integrated Services Digital Network

Integrated Services Digital Network (ISDN) provides switched end-to-end digital connectivity. ISDN can carry both voice and data over the same connection.

There are different types of ISDN services, with Basic Rate Interface (BRI) being the most common. BRI consists of two 64 kbps B channels to carry customer data and a D channel to carry signaling data. The two B channels can be linked together to give a combined rate of 128 kbps. In some areas, the telephone company might limit each B channel to either 56 kbps or 112 kbps combined. There is also a physical constraint in that the customer location must be within 5400 m (18 000 ft) of the central office switch. This distance can be extended with repeaters. You can connect to ISDN with a device called a terminal adapter. Most terminal adapters have an integrated network termination unit (NT1) that allows direct connection into a telephone jack. Typically, terminal adapters connect to your computer over an asynchronous RS-232 link and use the AT command set for setup and control, much like conventional analog modems. Each brand has its own AT command extension for setting up parameters that are unique to ISDN. In the past, there were many interoperability problems between different brands of

ISDN terminal adapters. These problems were due mostly to the variety of rate adaptation protocols that were in V.110 and V.120 as well as bonding schemes for the two B channels.

The industry has now converged to synchronous PPP protocol with PPP multilink for linking two B channels. Some terminal adapter manufactures integrate V.34 (analog modem) capability into their terminal adapters. This capability enables customers with a single ISDN line to handle either ISDN or conventional analog calls by taking advantage of the simultaneous voice/data capabilities of ISDN services. With this technology, a terminal adapter can also operate as the digital system side for V.92 clients.

Typically, you need to connect to an ISDN terminal adapter over an RS-232 serial interface using asynchronous protocol at rates up to 230.4 kbps. However, the maximum system baud rate for asynchronous protocol over RS-232 is 115.2 kbps. Unfortunately, this restricts the maximum byte transfer rate to 11.5 kbps, while the terminal adapter with multilinking is capable of 14 or 16 KB uncompressed. Some terminal adapters support synchronous protocol over RS-232 at 128 kbps, but the system maximum baud rate for synchronous protocol over RS-232 is 64 kbps.

The system is capable of running asynchronous protocol over V.35 at rates up to 230.4 kbps, but terminal adapter manufacturers generally do not offer such a configuration. Interface converters that convert an RS-232 interface to a V.35 interface might be a reasonable solution for the problem, but this approach has not been evaluated for the system. Another possibility is to use terminal adapters with V.35 interface synchronous protocol at a rate of 128 kbps. Although this class of terminal adapters exists, it does not appear that many offer synchronous multilink PPP.

Related reference

"Switched-56" on page 35
When you do not need a full-time connection, you can save money by using switched digital service, which is generally called *Switch-56 (SW56)*.

"ISDN terminal adapters" on page 40
Integrated Services Digital Network (ISDN) provides you with a digital connection that allows you to communicate by using any combination of voice, data, and video, among other multimedia applications.

T1/E1 and fractional T1 connections

T1/E1 and fractional T1 are two kinds of valid connection alternatives.

T1/E1

A T1 connection bundles together 24 64-kbps (DS0) time-division multiplexed (TDM) channels over 4-wire copper circuit. This creates a total bandwidth of 1.544 mbps. An E1 circuit in Europe and other parts of the world bundles together 32 64-kbps channels for a total of 2.048 mbps. TDM allows multiple users to share a digital transmission medium by using pre-allocated time slots. Many digital private branch exchanges (PBXs) take advantage of T1 service to import multiple call circuits over one T1 line instead of having 24 wire pairs routed between the PBX and telephone company.

It is important to note that T1 can be shared between voice and data. A telephone service can come over a subset of the 24 channels of a T1 link, for instance, leaving remaining channels for Internet connectivity. A T1 multiplexer device is needed to manage the 24 DS0 channels when a T1 trunk is shared between multiple services. For a single data-only connection, the circuit can be run unchannelized (no TDM is performed on the signal). Consequently, a simpler channel service unit/data service unit (CSU/DSU) device can be used. Typically, you can connect to a T1/E1 CSU/DSU or multiplexer over a V.35 or an RS 449 serial interface with synchronous protocol at rates at a multiple of 64 kbps to 1.544 mbps or 2.048 mbps. The CSU/DSU or multiplexer provides the clocking in the network.

Fractional T1

With Fractional T1 (FT1), a customer can lease any 64-kbps submultiple of a T1 line. FT1 is useful whenever the cost of a dedicated T1 is prohibitive for the actual bandwidth that a customer uses. With FT1 you pay only for what you need. Additionally, FT1 has the following feature that is unavailable with a full T1 circuit: Multiplexing DS0 channels at the central office of the telephone company. The remote end of an FT1 circuit is at a Digital Access Cross-Connect Switch that is maintained by the telephone company. Systems that share the same digital switch can switch among DS0 channels. This scheme is popular with Internet service providers (ISPs) that use a single T1 trunk from their location to the digital switch of a telephone company. In these cases, multiple clients can be served with FT1 service. Typically, you can connect to a T1/E1 CSU/DSU or multiplexer over a V.35 or an RS 449 serial interface with synchronous protocol at some multiple of 64 kbps. With FT1, you are preallocated a subset of the 24 channels. The T1 multiplexer must be configured to fill only the time slots that are assigned for your service.

Frame relay

Frame relay is a protocol for routing frames through the network based on the IP address field (data link connection identifier) in the frame and for managing the route or virtual connection.

Frame-relay networks in the U.S. support data transfer rates at T1 (1.544 mbps) and T3 (45 mbps) speeds. You can think of frame relay as a way of utilizing existing T1 and T3 lines owned by a service provider. Most telephone companies now provide Frame Relay service for customers who want connections at 56 kbps to T1 speeds. (In Europe, Frame Relay speeds vary from 64 kbps to 2 mbps. In the U.S., Frame Relay is quite popular because it is relatively inexpensive. However, it is being replaced in some areas by faster technologies, such as asynchronous transfer mode (ATM).

L2TP (tunneling) support for PPP connections

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol that extends Point-to-Point Protocol (PPP) to support a link layer tunnel between a requesting L2TP client (L2TP Access Concentrator or LAC) and a target L2TP server endpoint (L2TP Network Server or LNS).

Layer Two Tunneling Protocol

By using Layer Two Tunneling Protocol (L2TP) tunnels, it is possible to separate the location at which the dial-up protocol ends and where the access to the network is provided. That is why L2TP is also referred to as *Virtual PPP*.

These figures illustrate three different tunneling implementations of L2TP.

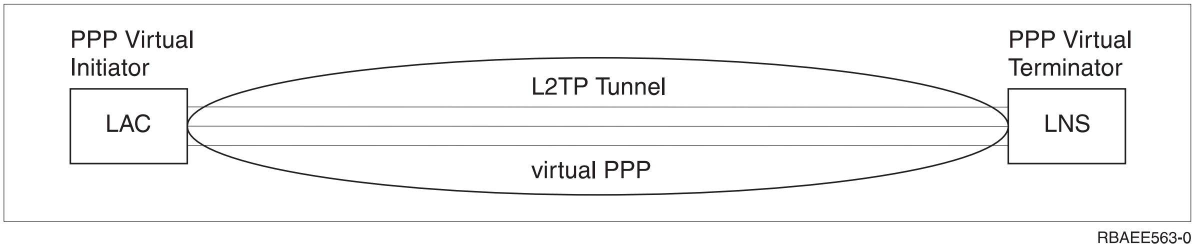


Figure 10. PPP virtual initiator or PPP virtual terminator

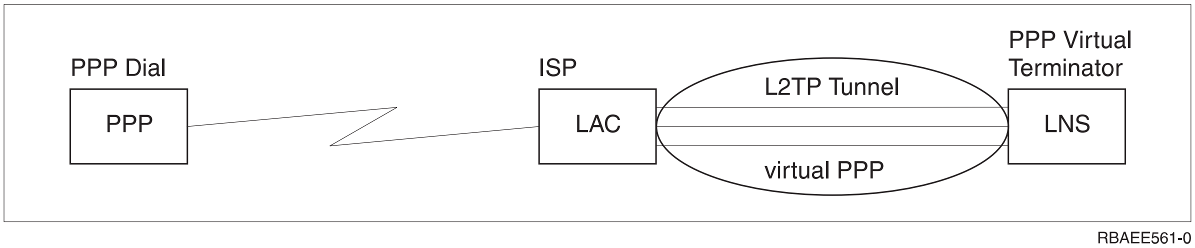


Figure 11. PPP dial initiator or PPP virtual terminator

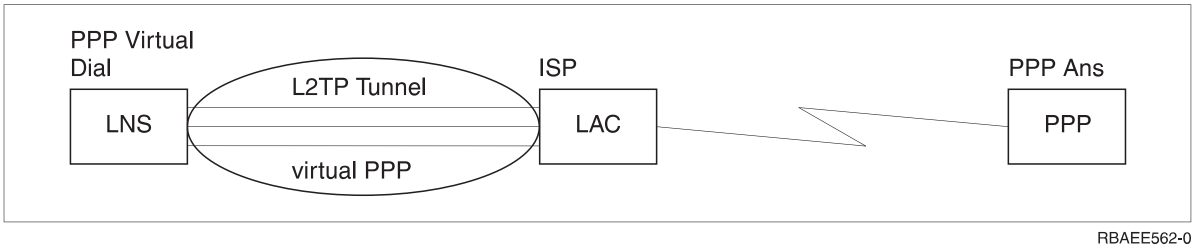


Figure 12. PPP virtual dial or PPP virtual answer

The L2TP protocol is documented as a Request for Comment (RFC) standard, RFC-2661. An L2TP tunnel can extend across an entire PPP session or only across one segment of a two-segment session. This can be represented by four different tunneling models.

Related information

Scenario: Protecting an L2TP voluntary tunnel with IPSec

RFC Editor

Voluntary tunnel:

In the voluntary tunnel model, a tunnel is created by the user, typically by the use of a Layer Two Tunneling Protocol (L2TP)-enabled client.

As a result, the user sends L2TP packets to the Internet service provider (ISP), which forwards them on to the L2TP network server (LNS). In voluntary tunneling the ISP does not need to support L2TP, and the L2TP tunnel initiator is on the same system as the remote client. In this model, the tunnel extends across the entire Point-to-Point Protocol (PPP) session from the L2TP client to the LNS.

Compulsory tunnel model - incoming call:

In the compulsory tunnel model - incoming call, a tunnel is created without any action from the user and without allowing the user any choice.

As a result, the user sends Point-to-Point Protocol packets to the Internet service provider (ISP) (Layer Two Tunneling Protocol (L2TP) access concentrator (LAC)). The ISP encapsulates the packets in L2TP and sends them in a tunnel to the L2TP network server (LNS). In the compulsory tunneling cases, the ISP must be L2TP-capable. In this model, the tunnel extends only across the segment of the PPP session between the ISP and the LNS.

Compulsory tunnel model - remote dial:

In the compulsory tunnel model - remote dial, the home gateway (L2TP network server (LNS)) initiates a tunnel to an Internet service provider (ISP) (LAC) and instructs the ISP to place a local call to the Point-to-Point Protocol (PPP) answer client.

This model is intended for cases where the remote PPP answer client has a permanent, established telephone number with an ISP. This model is expected to be used when a company with established presence on the Internet needs to establish a connection to a remote office that requires a dial-up link. In this model, the tunnel only extends across the segment of the PPP session between the LNS and the ISP.

L2TP multi-hop connection:

A Layer Two Tunneling Protocol (L2TP) multi-hop connection is a way of redirecting L2TP traffic on behalf of client L2TP access concentrators (LACs) and L2TP network servers (LNSs).

A multi-hop connection is established using an L2TP multi-hop gateway (a system that links L2TP Terminator and Initiator profiles together). To establish a multi-hop connection, the L2TP multi-hop gateway acts as both an LNS to a set of LACs at the same time as acting as an LAC to a given LNS. A tunnel is established from a client LAC to the L2TP multi-hop gateway, and then another tunnel is established between the L2TP multi-hop gateway and a target LNS. L2TP traffic from the client LAC is then redirected by the L2TP multi-hop gateway to the target LNS, and traffic from the target LNS is redirected to the client LAC.

PPPoE (DSL) support for PPP connections

Digital Subscriber Line (DSL) refers to a class of technology used to obtain more bandwidth over existing copper telephone cabling that is running between a customer's premises and an Internet service provider (ISP).

DSL allows simultaneous voice and high-speed data services over a single pair of copper telephone wires. Modem speeds have gradually increased through the use of various compression and other techniques, but at today's fastest (56 kbps), they are approaching the theoretical limit for this technology. DSL technology enables much higher speeds across the twisted pair lines from the central office to the home, school, or business. Speeds up to 2 Mbps are achievable in some areas. PPP is typically used over serial communications like dial-up modem connections. Many DSL Internet service providers now use PPP over Ethernet (PPPoE) because of its added login and security features.

A *DSL modem* is a device that is placed at either end of the copper telephone line to allow a computer (or LAN) to be connected to the Internet through a DSL connection. Unlike a dial-up connection, it typically does not require a dedicated telephone line (a POTS splitter box enables the line to be shared simultaneously). Although DSL modems resemble conventional analog modems, they provide much higher throughput.

Connection equipment

The system uses modems, Integrated Services Digital Network (ISDN) terminal adapters, token-ring adapters, Ethernet adapters, or channel service unit/data service unit (CSU/DSU) devices to handle Point-to-Point Protocol (PPP) connections.

These are four kinds of communication equipment that you can use with your PPP environment:
- Modems
- CSU/DSU
- ISDN terminal adapters
- Ethernet adapters (for PPPoE connections)

Modems

Both external and internal modems can be used for Point-to-Point Protocol (PPP) connections.

The command set used in a modem is normally described in the modem documentation. The commands are used to reset and initialize the modem, and to tell the modem to dial the telephone number of the remote system. Each modem model has to be defined before it can be used with a PPP connection profile because different modem models have different initialization command strings. If it is an internal modem, the modem strings are already defined for their use.

The system has many modem models predefined, but new models can be defined through iSeries Navigator. An existing definition can be used as a base for the new type to be defined. If you are not sure what commands your modem is using, or if you do not have access to the modem documentation, start with the Generic Hayes modem definition. The predefined definitions cannot be changed. However, additional commands can be added to the existing initialization command or dial string.

You can use the electronic customer support modem that is included with the system to establish PPP connections. On older systems, the electronic customer support modem was an IBM 7852-400 external modem. This modem has been replaced by the MultiTech MT5600BA-V92 V.92 Data/Fax World Modem. On newer systems, the 2771, 2793, or any of the other supported internal modems can be used as the electronic customer support modem.

Related reference

"Software and hardware requirements" on page 32
A Point-to-Point Protocol (PPP) environment requires that you have two or more computers that support PPP. One of these computers, the System i platform, can either be the originator or receiver.

CSU/DSU

A channel service unit (CSU) is a device that connects a terminal to a digital line. A data service unit (DSU) is a device that performs protective and diagnostic functions for a telecommunications line. Typically, the two devices are packaged as a single unit, CSU/DSU.

You can think of a CSU/DSU as a very high-powered and expensive modem. Such a device is required for both ends of a T-1 or T-3 connection; the units at both ends must be from the same manufacturer.

Related reference

"Software and hardware requirements" on page 32
A Point-to-Point Protocol (PPP) environment requires that you have two or more computers that support PPP. One of these computers, the System i platform, can either be the originator or receiver.

"Digital service and Digital Data Services" on page 34
You can use digital service and Digital Data Services (DDS) with Point-to-Point Protocol (PPP).

ISDN terminal adapters

Integrated Services Digital Network (ISDN) provides you with a digital connection that allows you to communicate by using any combination of voice, data, and video, among other multimedia applications.

You need to verify that your terminal adapter is rated for use on the system.

Follow these steps to configure your terminal adapter:

1. In iSeries Navigator, select your system and expand **Network** → **Remote Access Services**.
2. Right-click **Modems**, and select **New Modem**.
3. From the **New Modem Properties** dialog box, enter the correct values in all the **field** boxes of the **General** tab. Ensure that you specify ISDN terminal adapter as the communications device.
4. Select the **ISDN Parameters** tab.
5. Add or change ISDN properties on the **ISDN Parameters** tab to match the properties required by your terminal adapter.

Related tasks

“Example: Configuring an ISDN terminal adapter” on page 57
The example demonstrates how to configure an Integrated Services Digital Network (ISDN) terminal adapter.

Related reference

“Software and hardware requirements” on page 32
A Point-to-Point Protocol (PPP) environment requires that you have two or more computers that support PPP. One of these computers, the System i platform, can either be the originator or receiver.

“Integrated Services Digital Network” on page 35
Integrated Services Digital Network (ISDN) provides switched end-to-end digital connectivity. ISDN can carry both voice and data over the same connection.

ISDN terminal adapter suggestions:

There are several different terminal adapters that you can use.

The suggested external Integrated Services Digital Network (ISDN) terminal adapter, or ISDN modem, is the **3Com/U.S. Robotics Courier I ISDN V.Everything**. It supports V.34 analog modem connections, V.90 (X2), V.92, and multilink PPP over ISDN in both origination and answer modes on the system. It also automatically supports Challenge Handshake Authentication Protocol (CHAP) over the ISDN PPP connection. The following ISDN terminal adapters are also available: Zyxel Omni.net Plus TA, Zyxel Omni.net LCD plus TA, and ADtran ISU 2x64 Dual Port.

- **Connections that originate from the system.** CHAP challenges that originate from the receiving side are answered by the Courier I terminal adapter, while negotiating Password Authentication Protocol (PAP) authentication with the system. PAP responses do not appear on the ISDN connection.
- **Connections that the system answers.** The Courier I requires CHAP authentication by the calling side if the answer configuration causes the system to open authentication with a CHAP challenge. If the system opens authentication with PAP, the Courier I terminal adapter authenticates with PAP.

If you are using a pre-1999 Courier I modem, verify that the Courier I modem is connected to your system by a V.35 cable to get the best performance from your ISDN connection. An RS-232 to V.35 modem cable is supplied with the Courier I modem; however, older versions of this cable have the wrong gender V.35 connector. Contact 3Com/US Robotics Customer Support for a replacement.

Note: According to 3Com/US Robotics, the V.35 version of this terminal adapter is no longer from third party suppliers, though some V.35 versions might still come from third-party suppliers. The RS-232 version is still suggested at somewhat reduced performance on the system because RS-232 connections are limited to 115.2 KB.

Be sure to set the V.35 line speed on the system to 230.4 kbps.

ISDN terminal adapter restrictions:

The terminal adapters in this topic have been evaluated. They are suggested only for the origination of Integrated Services Digital Network (ISDN) remote connections from the system.

3Com Impact IQ ISDN:

This terminal adapter is not suggested for the System i platform for the following reasons:

- The terminal adapter does not support V.34 analog modem connections. However, it can support V.34 analog modem connections by using the external RJ-11 connection.
- The terminal adapter does not currently support V.90 connections.
- The terminal adapter might not be connected to the system at speeds greater than 115 200 bps.
- The terminal adapter does not automatically support Challenge Handshake Authentication Protocol (CHAP). If you set S84 to 0, CHAP authentication is performed.

- The system is unable to determine when the connection ends when monitoring the Data Set Ready signal from the terminal adapter. This causes a potential system security exposure.

Motorola BitSurfr Pro ISDN:

This terminal adapter is not suggested for the System i platform for the following reasons:

- The terminal adapter does not support V.34 analog modem connections. However, it can support V.34 analog modem connections by using the external RJ-11 connection.
- The terminal adapter does not currently support V.90 connections.
- The terminal adapter might not be connected to the system at speeds greater than 115 200 bps.
- The terminal adapter does not automatically support CHAP authentication. However, setting @M2=C allows CHAP authentication to be performed.
- The terminal adapter does not automatically permit answering both single-link and multilink PPP calls. The remote origination terminal adapter must be set to the same protocol (single-link or multilink) as the answering terminal adapter.
- The hardware flow control mechanism does not work well with this terminal adapter. This causes degraded performance when the system is sending data on a multilink PPP connection.

IP address handling

Point-to-Point Protocol (PPP) connections enable several different sets of options for managing IP addresses depending on the type of connection profile.

- DHCP can centrally manage IP address assignments for your network. Learn how to setup and manage DHCP services for your network. Refer to Dynamic Host Configuration Protocol
- DNS can help you manage host names and their associated IP addresses. Learn how to setup and manage DNS services for your network. Refer to Domain Name System
- BOOTP is used to associate client workstations with your system, and assign them IP addresses. Learn how to setup and manage BOOTP services for your network. Refer to Bootstrap Protocol

Related reference

"Scenario: Connecting your system to a PPPoE access concentrator" on page 11
Many Internet service providers (ISPs) provide high-speed Internet access over a Digital Subscriber Line (DSL) using Point-to-Point Protocol over Ethernet (PPPoE). You can connect your system to these ISPs to provide high-bandwidth connections that preserve the benefits of Point-to-Point Protocol (PPP).

IP packet filtering

IP packet filtering limits the services to individual users when they log on to a network.

Packet filtering can permit or deny access based on destination IP addresses or ports or both. Different policies are enforced by defining multiple sets of packet filter rules with each having their own unique PPP filter identifier. Packet filter rules can be assigned for a particular receiver connection profile or can be assigned by using a Group Policy that will apply the filter rules for that category of user. The packet filter rules themselves are not defined in PPP, but are defined under IP Packet Rules in iSeries Navigator.

For L2TP connections, VPN with IPSec filtering should be used to protect network traffic.

Related reference

"Scenario: Connecting your system to a PPPoE access concentrator" on page 11
Many Internet service providers (ISPs) provide high-speed Internet access over a Digital Subscriber Line (DSL) using Point-to-Point Protocol over Ethernet (PPPoE). You can connect your system to these ISPs to provide high-bandwidth connections that preserve the benefits of Point-to-Point Protocol (PPP).

Related information

IP filtering and network address translation

Virtual Private Networking (VPN)

IP address management strategy

Before configuring a PPP connection profile, you should be familiar with your network IP address management strategy. This strategy influences many of the decisions throughout the configuration process including your authentication strategies, security considerations, and TCP/IP settings.

Originator connection profiles

Typically, the local and remote IP addresses defined for an originator profile will be defined as *Assigned by remote system*. This enables the administrators on the remote system to have control over the IP addresses that will be used for the connection. Most all connections to Internet service providers (ISP) will be defined this way, although many ISPs can offer fixed IP addresses for an additional fee.

If you define fixed IP addresses for either the local or remote IP address, you must be sure that the remote system is defined to accept the IP addresses you have defined. One typical application is to define your local IP address as a fixed IP address and the remote to be assigned by the remote system. The system you are connecting can be defined the same way so when you connect, the two systems will exchange IP addresses with each other as a way to learn the IP address of the remote system. This might be useful for one office calling another office for temporary connectivity.

Another consideration is whether you want to enable IP address masquerading. For example, if the system connects to the Internet through an ISP, this can allow an attached network behind the system to access the Internet. Basically, the system hides the IP addresses of the systems on the network behind the local IP address assigned by the ISP, thus making all IP traffic appear to be from the system. There are also additional routing considerations for both the systems on the LAN (to ensure their Internet traffic is sent to the system) as well as the system where you need to enable the **add remote system as the default route** box.

Receiver connection profiles

Receiver connection profiles have many more IP address considerations and options than the Originator Connection Profile does. How you configure the IP addresses depends on the IP address management plan for your network, your specific performance and functional requirements for this connection, and the security plan.

Local IP addresses

For a single receiver profile, you can define a unique IP address or use an existing local IP address on your system to identify the end of the PPP connection. For receiver profiles defined to support multiple connections at the same time, you must use an existing local IP address. If no existing local IP addresses are present, you can create a virtual IP address for this purpose.

Remote IP addresses

There are many options for assigning remote IP addresses to PPP clients. The following options can be specified on the TCP/IP page of the receiver connection profile.

Note: If you want the remote system to be considered part of the LAN, you should configure IP address routing, specify an IP address within the IP address range for LAN-attached systems, and verify that IP forwarding has been enabled for both this connection profile and the system.

Table 8. IP address assignment options for receiver profile connections

Option	Description
Fixed IP address	You define the single IP address that is to be given to remote users when they dial in. This is a host only IP address (Subnet mask is 255.255.255.255) and is only for single connection receiver profiles.
Address Pool	You define the starting IP address and then a range of how many additional IP addresses to define. Each user that connects will then be given a unique IP address within the defined range. This is a host only IP address (Subnet mask is 255.255.255.255) and is only for multiple connection receiver profiles.
RADIUS	The remote IP address and it's subnet mask will be determined by the Radius server. This is only if the following is defined: • Radius support for authentication and IP addressing has been enabled from the Remote Access Server services configuration. • Authentication is enabled for the receiver connection profile and is defined to be authenticated remotely by Radius.
DHCP	The remote IP address is determined by the DHCP server directly or indirectly through DHCP relay. This is only if DHCP support has been enabled from the Remote Access Server services configuration. This is a host only IP address (Subnet mask is 255.255.255.255).
Based on remote system's user ID	The remote IP address is determined by the user ID defined for the remote system when it is authenticated. This allows the administrator to assign different remote IP addresses (and their associated subnet masks) to the user that dials in. This also allows additional routes to be defined for each of these user IDs, so that you can tailor the environment to the known remote user. Authentication must be enabled for this function to work properly.
Define additional IP addresses based on remote system's user ID	This option allows you to define IP addresses based on the user ID of the remote system. This option is automatically selected (and must be used) if the remote IP address assignment method is defined as **Based on remote system's user ID**. This option is also allowed for IP address assignment methods of Fixed IP address and Address Pool. When a remote user connects to the system, a search will be made to determine if a remote IP address is defined specifically for this user. If it is then that IP address, mask and set of possible routes will be used for the connection. If the user is not defined, the IP address will default to the defined Fixed IP address or the next Address Pool IP address.
Allow remote system to define it's own IP address	This option allows a remote user to define their own IP address if they negotiate to do so. If they do not negotiate to use their own IP address, the remote IP address will be determined by the defined remote IP address assignment method. This option is initially disabled and careful consideration should be used before enabling it.
IP address routing	The dial-up client and the system must have IP address routing properly configured if the client needs access to any IP addresses on the LAN to which the system belongs.

System authentication

PPP connections with a System i platform support several options for authenticating both remote clients dialing in to the system and connections to an ISP or another system that the system is dialing to.

The system supports several methods for maintaining authentication information, ranging from simple validation lists on the system that contain lists of authorized users and associated passwords to support for Remote Authentication Dial In User Service (RADIUS) servers that maintain detailed authentication information for your network users. The system also supports several options for encrypting user ID and password information, ranging from a simple password exchange to support with Challenge Handshake

Authentication Protocol (CHAP-MD5). You can specify your preferences for system authentication, including a user ID and password to validate the system when dialing out, on the **Authentication** tab of the connection profile in iSeries Navigator.

Related reference

"Scenario: Connecting your system to a PPPoE access concentrator" on page 11
Many Internet service providers (ISPs) provide high-speed Internet access over a Digital Subscriber Line (DSL) using Point-to-Point Protocol over Ethernet (PPPoE). You can connect your system to these ISPs to provide high-bandwidth connections that preserve the benefits of Point-to-Point Protocol (PPP).

"Scenario: Authenticating dial-up connections with RADIUS NAS" on page 22
A Network Access Server (NAS) running on the system can route authentication requests from dial-in clients to a separate Remote Authentication Dial In User Service (RADIUS) server. If authenticated, RADIUS can also control the IP addresses assigned to the user.

"Scenario: Managing remote user access to resources using group policies and IP filtering" on page 24
Group access policies identify distinct user groups for a connection, and allow you to apply common connection attributes and security settings to the entire group. You can use group policies, along with IP filtering, to permit and restrict access to specific IP addresses on your network.

Challenge Handshake Authentication Protocol with MD5

Challenge Handshake Authentication Protocol (CHAP-MD5) uses an algorithm (MD-5) to calculate a value that is known only to the authenticating system and the remote device.

With CHAP, the user ID and the password are always encrypted, so it is a more secure protocol than Password Authentication Protocol (PAP). This protocol is effective against playback and trial-and-error access attempts. CHAP authentication can occur more than once during a connection.

The authenticating system sends a challenge to the remote device that is attempting to connect to the network. The remote device responds with a value that is calculated by a common algorithm (MD-5) that both devices use. The authenticating system checks the response against its own calculation. Authentication is acknowledged when the values match; otherwise, the connection is ended.

Related reference

"Scenario: Connecting remote dial-in clients to your system" on page 14
Remote users, such as telecommuters or mobile clients, often require access to a company's network. These dial-in clients can gain access to a system with Point-to-Point Protocol (PPP).

"Password Authentication Protocol" on page 46
Password Authentication Protocol (PAP) uses a two-way handshake to provide the peer system with a simple method to establish its identity.

Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) enables third-party authentication modules to interact with the PPP implementation.

EAP extends PPP by providing a standard support mechanism for authentication schemes such as token (smart) cards, Kerberos, Public Key, and S/Key. EAP responds to the increasing demand to augment authentication with third-party security devices. EAP protects secure virtual private networks (VPN) from hackers that use dictionary attacks and password guessing. EAP improves on Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

With EAP, the authentication information is not included in the information, but rather with the information. This allows remote systems to negotiate the necessary authentication before receiving or passing on any information.

The system does not directly support EAP. You can, however, use remote authentication with a Remote Authentication Dial In User Service (RADIUS) server that might support some of the additional authentication schemes described previously.

Password Authentication Protocol

Password Authentication Protocol (PAP) uses a two-way handshake to provide the peer system with a simple method to establish its identity.

The handshake is conducted when establishing a link. After the link is established, the remote device sends a user ID and password pair to the authenticating system. Depending on the correctness of the pair, the authenticating system either continues or ends the connection.

PAP authentication requires the user name and password to be sent to the remote system in clear text form. With PAP, the user ID and password are never encrypted, which makes them possible to trace and vulnerable to hacker attack. For this reason, you should use Challenge Handshake Authentication Protocol (CHAP) whenever possible.

Related reference

"Challenge Handshake Authentication Protocol with MD5" on page 45
Challenge Handshake Authentication Protocol (CHAP-MD5) uses an algorithm (MD-5) to calculate a value that is known only to the authenticating system and the remote device.

Remote Authentication Dial In User Service overview

Remote Authentication Dial In User Service (RADIUS) is an Internet standard protocol that provides centralized authentication, accounting and IP management services for remote access users in a distributed dial-up network.

The RADIUS client-server model has a Network Access Server (NAS) operating as a client to a RADIUS server. The system, acting as the NAS, sends user and connection information to a designated RADIUS server using the RADIUS standard protocol defined in RFC 2865.

RADIUS servers act on received user connection requests by authenticating the user and then return all configuration information necessary to the NAS, so that the NAS (the system) can deliver authorized services to the authenticated dial-in user.

If a RADIUS server cannot be reached, the system can route authentication requests to an alternate server. This enables global enterprises to offer their users a dial-in service with a unique login user ID for corporate-wide access, no matter what access point is being used.

When an authentication request is received by the RADIUS server, the request is validated; then the RADIUS server decrypts the data packet to access the user name and password information. The information is passed onto the appropriate security system that is supported. This might be UNIX® password files, Kerberos, a commercial security system, or even a custom-developed security system. The RADIUS server sends back to the system any services that the authenticated user is authorized to use, such as an IP address. RADIUS accounting requests are handled in a similar manner. Remote user's accounting information can be sent to a designated RADIUS accounting server. The RADIUS accounting standard protocol is defined in RFC 2866. The RADIUS accounting server acts on received accounting requests by logging the information from the RADIUS accounting request.

Related reference

"Scenario: Authenticating dial-up connections with RADIUS NAS" on page 22
A Network Access Server (NAS) running on the system can route authentication requests from dial-in clients to a separate Remote Authentication Dial In User Service (RADIUS) server. If authenticated, RADIUS can also control the IP addresses assigned to the user.

Validation list

A validation list is used to store user ID and password information about remote users.

You can use existing validation lists or create your own from the Receiver Connection Profile authentication page. Validation list entries also require you to identify an authentication protocol type to associate with the user ID and password. This might be **encrypted - CHAP-MD5/EAP** or **unencrypted - PAP**.

See the online help for more information.

Related reference

"Scenario: Managing remote user access to resources using group policies and IP filtering" on page 24
Group access policies identify distinct user groups for a connection, and allow you to apply common connection attributes and security settings to the entire group. You can use group policies, along with IP filtering, to permit and restrict access to specific IP addresses on your network.

Bandwidth considerations for multilink

Additional bandwidth is often required to complete certain tasks, but it is not always required.

The purchase of specialized hardware and expensive communication lines might not be justified. The PPP Multilink Protocol (MP) groups multiple PPP links together to form a single virtual link or bundle. The aggregation of multiple links increases the total effective bandwidth between two systems by using standard modems and telephone lines. You can include up to six links in an MP bundle. To establish a multilink connection, both ends of the PPP link must support the multilink protocol. The multilink protocol is documented as a Request for Comment (RFC) standard RFC-1990.

Bandwidth On Demand

The ability to dynamically add and remove physical links allows a system to be configured to supply bandwidth only when it is needed. This approach is commonly referred to as Bandwidth on Demand and allows you to only pay for the additional bandwidth when you actually use it. To realize the benefits of Bandwidth on Demand, at least one peer must be capable of monitoring utilization of the total bandwidth currently in an MP bundle. Links can be added to or removed from the bundle when bandwidth utilization exceeds values defined by configuration. The Bandwidth Allocation Protocol allows peers to negotiate adding and removing links in an MP bundle. RFC-2125 documents both the PPP Bandwidth Allocation Protocol (BAP) and Bandwidth Allocation Control Protocol (BACP).

Related information

RFC Editor

Configuring PPP

Before you can use PPP to set up a point-to-point connection, you must configure your PPP environment.

Related reference

"Related information for PPP" on page 66
Listed below are the IBM Redbooks (in PDF format) that provide additional information about Remote Access Services PPP connections. You can view or print the PDFs.

Creating a connection profile

The first step in configuring a PPP connection between systems is to create a connection profile on the system.

The connection profile is the logical representation of the following connection details:

- Line and profile type
- Multilink settings
- Remote telephone numbers and dialing options
- Authentication

- TCP/IP settings: IP addresses and routing
- Work management and connection customization
- Domain name servers

Remote Access Services, under the Network directory, contains the following objects:

- Originator connection profiles
- Receiver connection profiles
- **Modems**

Follow these steps to create a connection profile:

1. In iSeries Navigator, select your system and expand **Network** → **Remote Access Services**.
2. Select one from the following options:
   - Right-click **Originator Connection Profiles** to set the system to initiate.
   - Right-click **Receiver Connection Profiles** to set the system to allow incoming connections from remote systems and users.
3. Select **New Profile**.
4. On the New Point-to-Point Connection Profile Setup page, select the protocol type.
5. Specify the mode selections.
6. Select the link configuration.
7. Click **OK**.

   The New Point-to-Point Profile Properties page appears. You can set the rest of the values that are specific to your network. See the online help for specific information.

Related tasks

"Associating a modem with a line description" on page 58
The topic demonstrates the steps for associating a modem with a line description.

Related reference

"Scenario: Connecting your system to a PPPoE access concentrator" on page 11
Many Internet service providers (ISPs) provide high-speed Internet access over a Digital Subscriber Line (DSL) using Point-to-Point Protocol over Ethernet (PPPoE). You can connect your system to these ISPs to provide high-bandwidth connections that preserve the benefits of Point-to-Point Protocol (PPP).

"Scenario: Connecting remote dial-in clients to your system" on page 14
Remote users, such as telecommuters or mobile clients, often require access to a company's network. These dial-in clients can gain access to a system with Point-to-Point Protocol (PPP).

"Scenario: Connecting your office LAN to the Internet with a modem" on page 16
Administrators typically set up office networks for employees to access the Internet. Administrators can use a modem to connect the system to an Internet service provider (ISP). LAN-attached PC clients can communicate with the Internet using the i5/OS operating system as a gateway.

"Scenario: Connecting your corporate and remote networks with a modem" on page 19
A modem enables two remote locations (such as a central office and a branch office) to exchange data between them. Point-to-Point Protocol (PPP) can connect two LANs together by establishing a connection between a system in the central office and another one in the branch office.

"Scenario: Managing remote user access to resources using group policies and IP filtering" on page 24
Group access policies identify distinct user groups for a connection, and allow you to apply common connection attributes and security settings to the entire group. You can use group policies, along with IP filtering, to permit and restrict access to specific IP addresses on your network.

Protocol type: PPP or Serial Line Internet Protocol (SLIP)

PPP replaces Serial Line Internet Protocol (SLIP) as the protocol of choice for point-to-point connections.

PPP enables interoperability among the remote access software of different manufacturers. PPP also enables multiple network communication protocols to use the same physical communication line.

The SLIP Request for Comment (RFC) never becomes an Internet standard because of the following deficiencies:

- SLIP has no standard way to define IP addressing between the two hosts. This means that an unnumbered net cannot be used.
- SLIP has no support for error detection or error compression. Error detection or error compression is implemented in PPP.
- SLIP has no support for system authentication, while PPP has two-way authentication.

SLIP is still used today, and it is supported on the i5/OS operating system. However, IBM suggests that you use PPP when setting up point-to-point connectivity. SLIP provides no support for multilink connections. Compared to SLIP, PPP has better authentication. PPP performs better because of its compression facilities.

Note: SLIP connection profiles that are defined with ASYNC line types are no longer supported in this release. If you have these connection profiles, you must migrate them to either a SLIP profile or a PPP profile that uses a PPP line type.

Mode selections

The mode selections for a Point-to-Point Protocol (PPP) connection profile include selections for the connection type and the operating mode. Your mode selections specify how your system uses the new PPP connection.

Follow these steps to specify your mode selections:

1. Select one of the following connection types:
   - Switched line
   - Leased line
   - Layer Two Tunneling Protocol (L2TP) (virtual line)
   - Point-to-Point Protocol over Ethernet (PPPoE) line
2. Select the operating mode that is appropriate for the new PPP connection.
3. Record the connection type and operating mode that you selected. You need this information when you start to configure your PPP connections.

Switched line:

When you use a modem (internal or external) or an external Integrated Services Digital Network (ISDN) terminal adapter to connect over a telephone line, select the switched line connection.

The switched line connection type has the following operating modes:

Answer

Choose this operating mode to enable a remote system to dial into the system.

Dial

Choose this operating mode to enable the system to dial out to a remote system.

Dial on-demand (dial only)

Choose this operating mode to enable the system to automatically dial out to a remote system when TCP/IP traffic for the remote system is detected on the system. The connection ends when the data transmission is complete, and no TCP/IP traffic occurs for a specific period of time.

Dial on-demand (answer-enabled dedicated peer)

Choose this operating mode to enable the system to answer calls from a dedicated remote system. This operating mode also allows the system to call the remote system when TCP/IP traffic for the remote system is detected. If both systems use i5/OS operating system and use this operating mode, TCP/IP traffic flows between the two systems on demand and without the need for a permanent physical connection. This operating mode requires a dedicated resource. The remote peer must dial in for the operating mode to function properly.

Dial on-demand (remote peer enabled)

Choose this operating mode to enable a remote system to be dialed or answered. To handle incoming calls, you must reference an existing answer profile from a Point-to-Point Protocol (PPP) connection profile that specifies this operating mode. This enables one answer profile to handle all incoming calls from one or more remote peers and a separate dial on-demand profile for each outgoing call. This operating mode does not require a dedicated resource to handle the incoming calls from remote peers.

Leased line:

If you have a dedicated line between the local system and the remote system, select the leased line connection. If you have a leased line, you do not need a modem or an Integrated Services Digital Network (ISDN) terminal adapter to connect the two systems.

A leased line connection between two systems is considered a permanent or dedicated line. It is always open. One end of the leased line connection is configured as the initiator, and the other end is configured as the terminator.

The leased line connection type has the following operating modes:

Terminator

Choose this operating mode to enable a remote system to access the system through a dedicated line. This operating mode refers to a leased line answer profile.

Initiator

Choose this operating mode to enable the system to access a remote system through a dedicated line. This operating mode refers to a leased line dial profile.

L2TP (virtual line):

If you want to provide a connection between systems that use Layer Two Tunneling Protocol (L2TP), select the L2TP connection.

After an L2TP tunnel is established, a virtual Point-to-Point Protocol (PPP) connection is made between your system and the remote system. By using L2TP tunneling in conjunction with IP security (IP-SEC), you can send, route, and receive secure data over the Internet.

The L2TP (virtual line) connection type has the following operating modes:

Terminator

Choose this operating mode to enable a remote system to connect to the system over an L2TP tunnel.

Initiator

Choose this operating mode to enable the system to connect to a remote system over an L2TP tunnel.

Remote dial

Choose this operating mode to enable the system to connect to another system or an Internet service provider (ISP) over an L2TP tunnel, and to direct the ISP to dial a remote PPP client.

Multi-hop initiator

Choose this operating mode to enable the system to establish a multi-hop connection.

Note: The L2TP Terminator profile that this multi-hop initiator is associated with needs to have the **Allow multi-hop connection** box checked and have a PPP validation list entry that links the PPP user name to the multi-hop initiator profile.

PPPoE line:

Point-to-Point Protocol over Ethernet (PPPoE) connections use a virtual line to send PPP data (through an Ethernet adapter) to a Digital Subscriber Line (DSL) modem that is provided by your Internet service provider (ISP). The modem is also connected to the Ethernet-based LAN.

This enables high-speed Internet access for LAN users through PPP sessions on the i5/OS operating system. After the connection between the system and the ISP has started, individual users on the LAN can start unique sessions with the ISP over PPPoE.

PPPoE connections are only used by originator connection profiles. The connections imply an Initiator operating mode and use only a single line.

Link configuration

Link configuration defines the type of line service that your Point-to-Point Protocol (PPP) connection profile uses to establish a connection.

The types of line service depend on the connection type that you specify.

Related reference

"Scenario: Connecting your system to a PPPoE access concentrator" on page 11
Many Internet service providers (ISPs) provide high-speed Internet access over a Digital Subscriber Line (DSL) using Point-to-Point Protocol over Ethernet (PPPoE). You can connect your system to these ISPs to provide high-bandwidth connections that preserve the benefits of Point-to-Point Protocol (PPP).

"Scenario: Connecting remote dial-in clients to your system" on page 14
Remote users, such as telecommuters or mobile clients, often require access to a company's network. These dial-in clients can gain access to a system with Point-to-Point Protocol (PPP).

"Scenario: Connecting your office LAN to the Internet with a modem" on page 16
Administrators typically set up office networks for employees to access the Internet. Administrators can use a modem to connect the system to an Internet service provider (ISP). LAN-attached PC clients can communicate with the Internet using the i5/OS operating system as a gateway.

"Scenario: Connecting your corporate and remote networks with a modem" on page 19
A modem enables two remote locations (such as a central office and a branch office) to exchange data between them. Point-to-Point Protocol (PPP) can connect two LANs together by establishing a connection between a system in the central office and another one in the branch office.

Single line:

To define a Point-to-Point Protocol (PPP) line that is associated with an analog modem, select this line service. This option is also used for leased lines where a modem is not required. The PPP connection profile always uses the same i5/OS communications port resource.

An analog single line, if required, might be configured as `shared` between an answer profile and a dial profile. The dynamic resource sharing is a new function designed to enhance resource usability. Until V5R2, the modem resources were committed as soon as the profile using it was started. This was limiting the user to one resource per session, even if the resource was in the passive wait state. Now, new sharing rules apply when a specific resource has been accessed. There are two cases: first, a dial profile was started before an answer profile; second, an answer profile was started before a dial profile. The assumption is that the resource sharing is enabled. In the first case, the dial profile that was started will successfully connect. The answer profile that was started second, will wait for the line to become available. After the dial connection was ended, the answer profile will request the line, and will start. In the second case, the answer profile that was started will wait for the incoming connections. Unless an incoming connection was made, the dial profile that was started second, will ″borrow″ the line from the answer profile, which will ″lend″ the line. The outgoing connection will then be established. After the connection was ended, the dial profile will return the line to the answer profile which will again be ready to accept incoming connections. To enable the sharing function, click the **modem** tab for a switched line description, and select **Enable Dynamic Resource Sharing**.

Single line service is also used for L2TP (virtual line) and PPPoE (virtual line) connection types. For L2TP (virtual line) connection types, there is no hardware communications port resource used with the single line. Rather, the single line used with an L2TP connection is *virtual* in that there is no physical PPP hardware that is required to establish the tunnel. The single line used with a PPPoE connection is also virtual in that it provides a mechanism for treating a physical Ethernet line as if it were a PPP line that supports remote connections. The PPPoE virtual line is bound to a physical Ethernet line and is used to support PPP protocol data transfers over the Ethernet LAN connection to a DSL modem.

Line pool:

To set the PPP connection to use a line from a line pool, select this line service. When the PPP connection starts, the system selects an unused line from the line pool. For dial on-demand profiles, the system does not select the line until it detects TCP/IP traffic for the remote system.

You can use a line pool instead of defining a particular line description for a connection profile. You can specify one or more line descriptions in a line pool.

A line pool also enables a single connection profile to handle either multiple incoming analog calls or a single outgoing analog call. The line returns to the line pool when the PPP connection ends.

If you use the line pool to handle multiple incoming analog calls simultaneously, you need to indicate the maximum number of incoming connections. You can set this on the **Connections** tab of the **New Point-to-Point Profile Properties** dialog when you configure your connection profile. Use the Multilink setting to use line pools for single connections with increased bandwidth.

Advantages of using line pools:

- You do not commit a line resource to a PPP connection until it starts.

  For PPP connections that use a specific line, the connection ends if the line is not available unless the dynamic resource sharing is enabled. For connections that use a line pool, at least one line in the line pool must be available when the profile starts.

  In addition, if the resources are configured as shared (enable dynamic resource sharing), additional resource availability is achieved particularly for outgoing connections.
- You can use dial-on-demand profiles with line pools to use resources more efficiently.

  The system selects a line from the line pool only when using a dial-on-demand connection. Other connections can use the same line at other times.
- You can start more PPP connections with less resources to support.

  For example, if your environment needs four unique connection types but you only need two lines at any given time, you can use a line pool to make this environment work. You can create four dial-on-demand connection profiles and have each profile reference a line pool that contains two line descriptions. Each of the lines will be for use by all four connection profiles, thus allowing two connections to be active at any time. By using a line pool, you do not need to have four separate lines.

Also, if your environment is a combination between a PPP Client and a PPP Server, lines can be shared (enable dynamic resource sharing) whether they are used as 'single lines' or placed in a 'line pool'. The profile that started first will not commit the resource unless the connection is active. For example, if the PPP Server is started, and is listening for the incoming connections, it will 'lend' a line it uses to the PPP Client that started and 'borrowed' the shared line from the PPP Server.

Configure line pools

Line pools are defined within a connection profile. For basic line pool configuration, follow these steps:

1. In iSeries Navigator, select your system and expand **Networking** → **Remote Access Services**.
2. Create a connection profile to either dial or receive calls. Select from one of the following options:
   - Right-click **Originator Connection Profiles** to set the system to initiate a connection to a remote system.
   - Right-click **Receiver Connection Profiles** to set the system to allow incoming connections from remote systems and users.
3. Select **New profile**.
4. For an originator profile (dialing out) select: PPP, Switched line, and the Operating mode (typically dial). For link configuration, select **Line pool**. Click **OK** and iSeries Navigator will open a properties window for this connection profile.

   Note: You can also select a line pool when you create receiver connection profiles. The Line pool option might or might not be listed, depending on the following field values: protocol type, connection type, and operating mode.
5. On the General page, name the profile and enter a description.
6. On the Connection page, enter a name for the line pool and click **New**. This will open the **New Line Pool Properties** dialog which will display all the available lines and modems for this system.
7. Select the lines you want to use, and add them to the pool. You can also click **New line** to define a new line.
8. Click **OK** to save this line pool, and return to the New Point-to-Point Profile properties.
9. Complete the necessary information about the other pages (for example, TCP/IP settings and Authentication).
10. The connection profile will go down the list of available lines (within the pool) until a resource is available and use that line for the connection. Use iSeries Navigator help for further assistance.

Related reference

"Scenario: Connecting remote dial-in clients to your system" on page 14
Remote users, such as telecommuters or mobile clients, often require access to a company's network. These dial-in clients can gain access to a system with Point-to-Point Protocol (PPP).

"Scenario: Connecting your office LAN to the Internet with a modem" on page 16
Administrators typically set up office networks for employees to access the Internet. Administrators can use a modem to connect the system to an Internet service provider (ISP). LAN-attached PC clients can communicate with the Internet using the i5/OS operating system as a gateway.

"Scenario: Connecting your corporate and remote networks with a modem" on page 19
A modem enables two remote locations (such as a central office and a branch office) to exchange data between them. Point-to-Point Protocol (PPP) can connect two LANs together by establishing a connection between a system in the central office and another one in the branch office.

Multiple-connection profile support:

Point-to-point connection profiles that support multiple connections enable you to have one connection profile that handles many digital, analog, or L2TP calls.

This is useful when you want multiple users to connect to your system but do not want to specify a separate point-to-point connection profile to handle each PPP line. This feature is especially useful for the 2805 4-port integrated modem where four lines can be used from one adapter.

For analog lines with multiple-connection profile support, all lines in the specified line pool are used up to the maximum number of connections. Basically, a separate connection profile job is started for each line that is defined in the line pool. All connection profile jobs wait for incoming calls on their respective lines.

Local IP address for multiple-connection profiles

You can use the local IP address with multiple-connection profiles, but it must be an existing IP address that is defined on your system. You can use the local IP address pull down list to select the existing IP address. Remote users can access the resources that are on your local network if you choose the local IP address as the local IP address for your PPP profile. Also, you must define the IP addresses that are in the remote IP address pool to be in the same network as the local IP address.

If you do not have a local IP address or do not want the remote users to access the LAN, you must define a virtual IP address for your system. A virtual IP address is also known as a circuitless interface. Your point-to-point profiles can use this IP address as their local IP address. Because this IP address is not tied to a physical network, it does not automatically forward traffic to other networks that are attached to your system.

To create a Virtual IP address, follow these steps:

1. In iSeries Navigator, expand your system and access **Network** → **TCP/IP configuration** → **IPV4** → **Interfaces**.
2. Right-click **Interfaces** and select **New Interface** → **Virtual IP**.
3. Follow the Interface Wizard instructions to create your Virtual IP interface. Your point-to-point connection profiles can use the virtual IP address once it is created. You can use the pull down list from the **Local IP address** field that is on the TCP/IP Settings page to use the IP address with your profile.

   Note: The virtual IP address must be active before starting your multiple-connection profile; otherwise, the profile will not start. To activate the IP address after creating the interface, you select the option to start the IP address when using the Interface Wizard.

Remote IP address pools for multiple-connection profiles

You can also use remote IP address pools with multiple-connection profiles. A typical one-connection point-to-point profile only allows you to specify one remote IP address, which is given to the calling system when the connection is made. Because multiple callers can now connect simultaneously, a remote IP address pool is used to define a starting remote IP address as well as a range of additional IP addresses that are given to the calling system.

Line pool restrictions

These restrictions apply when using line pools for multiple connections:

- A specific line can only exist in one line pool at a time. If you remove a line from a line pool, it can be used in another line pool.
- When starting a multiple connection profile that uses a line pool, all lines in the line pool are used up to the maximum number of connections value in the profile. When there are no lines, all new connections will fail. Also, if there are no lines in the line pool, and another profile starts, it will end.

- When you start a single connection profile that has a line pool, the system uses only one line from the line pool. If you start a multiple connection profile that uses the same line pool, any remaining lines in the line pool are for use.

  Related tasks

  "Step 1: Configuring the L2TP terminator profile for any interface on the partition that owns the modems" on page 29
  To create a terminator profile for any interface, follow these steps:

Remote IP address pools:

The system can use remote IP address pools for any answering or stopping point-to-point connection profile that is used with multiple incoming connections.

This includes Layer Two Tunneling Protocol (L2TP) and line pools with a maximum number of connections greater than one. This function enables the system to assign a unique remote IP address to each incoming connection.

The first system to connect receives the IP address defined in the Starting IP address field. If that IP address is already in use, the next IP address within the range is given out. For example, assume that the Starting IP address is 10.1.1.1 and the Number of IP addresses is defined as 5. The IP addresses within the remote IP address pool will be 10.1.1.1, 10.1.1.2, 10.1.1.3, 10.1.1.4, and 10.1.1.5. The subnet mask defined for the remote IP address pool addresses will always be 255.255.255.255.

These restrictions apply when using remote IP address pools:

- More than one connection profile can specify the same address pool. However, when all the IP addresses in the pool are used, any subsequent connection request is refused until another connection ends and an IP address becomes available.
- To allocate specific IP addresses to some remote systems while allowing other incoming systems to use an IP address from the pool, follow these steps:
  1. Enable Remote system authentication from the **Authentication** tab, so the user name of the remote system can be learned.
  2. Define a remote IP address pool for all incoming connection requests that do not require a specific IP address.
  3. Define remote IP addresses for specific users by checking **Define additional IP addresses based on remote system's user ID**, and then clicking **IP addresses defined by User Name**.

  When the remote user is connected to the system, the system determines whether a specific IP address is defined for this user. In this case, the IP address is given to the remote system; otherwise, an IP address from the remote IP address pool is returned.

Configuring your modem for PPP

A modem provides you with analog connection capabilities (leased and switched lines). For your analog Point-to-Point Protocol (PPP) connections, you can use an external modem, internal modem, or Integrated Services Digital Network (ISDN) terminal adapter.

Related reference

"Troubleshooting PPP" on page 64
If you experience Point-to-Point Protocol (PPP) connection problems, you can use the checklist to gather error information. This checklist can help you identify error symptoms and resolve PPP connection problems.

Configuring a new modem

You can configure a new modem using an existing modem description or base the modem description on a previous modem description.

To configure a new modem, follow these steps.

1. In iSeries Navigator, select your system and expand **Network** → **Remote Access Services**.
2. Right-click **Modems**, and select **New Modem**.
3. On the **General** tab, enter the correct values in all the field boxes.
4. Optional: Click the **Additional Parameters** tab to add any necessary initialization commands for your modem.
5. Click **OK** to save your entries, and close the New Modem Properties page.

Using an existing modem description

To determine if you can use an existing modem description, follow these steps:

1. In iSeries Navigator, select your system and expand **Network** → **Remote Access Services**.
2. Select **Modems**.
3. Review the modem list, and find the manufacturer name, model, and make of your modem.

   Note: If your modem is included in the default list, you do not need to do any further steps.
4. Right-click the modem description that closely matches your modem, and select **Properties** to review the command strings.
5. Consult your modem documentation to determine the specific command strings for your modem.

   Use the default modem properties if the command strings match your modem requirements. Otherwise, you need to create a modem description for your modem, and add it to the modem list.

Creating a modem description based on a previous modem description

To create a modem description based on a previous modem description, follow these steps:

1. In iSeries Navigator, select your system and expand **Network** → **Remote Access Services**.
2. Select **Modems**.
3. From the modem list, right-click **Generic hayes**, and select **New modem based on**.
4. From the **New Modem** dialog, change the command strings to match the information that is required by your modem.

   Related reference

   "Troubleshooting PPP" on page 64
   If you experience Point-to-Point Protocol (PPP) connection problems, you can use the checklist to gather error information. This checklist can help you identify error symptoms and resolve PPP connection problems.

Setting modem command strings

You can find the equivalent command string in the user manual for your modem. Use the manufacturer's suggested setting in the modem description.

Table 9. Modems defined on the system and command strings

Modem property	Correct command string for most modems
Modem reset to factory defaults	AT&F or AT&Z
Modem initialization:	
Display Verbal Results Codes	Q0 and V1
Normal CD and DTR modes	&C1 and &D2
Echo mode off	E0
Data Set Ready (DSR) to follow Carrier Detect	&S1

Table 9. Modems defined on the system and command strings (continued)

Modem property	**Correct command string for most modems**
Enable hardware flow control (RTS/CTS)	
Enable error correction and, optionally, compression (V.42/V.42 bis)	
Ensure DTE-DCE line speed is enabled to run at fixed 115.2 kbps (or the maximum allowed by the modem)	
(Optional) Enable the inactivity time If the modem supports this function	
Modem Answer mode:	
Answer after *n* rings	S0=*n* where *n* = 1 or 2
Disconnect if no carrier (connection) after *m* seconds	S7=*m*
Modem Dial type	ATDT for tone dialing or ATDP for pulse dialing

Example: Configuring an ISDN terminal adapter

The example demonstrates how to configure an Integrated Services Digital Network (ISDN) terminal adapter.

1. In iSeries Navigator, select your system and expand **Network** → **Remote Access Services**.
2. Right-click **Modems**, and select **New Modem**.
3. On the **General** tab, enter the correct values in all the **field** boxes.
4. Optional: Click the **ISDN Parameters** tab to add any necessary initialization commands for your modem.

   For ISDN terminal adapters, the commands and parameters in this list are sent to the terminal adapter only for the following conditions:
   - When commands or parameters in the list are either changed or added
   - As a result of certain error recovery actions that the system performs

   Consequently, these commands should include and be limited to the following settings:
   - Setting the ISDN switch type and version that is provided by the local telephone company.
   - Setting the directory numbers and the service profile identifiers (SPIDs) that are provided by the local telephone company.
   - Setting the Terminal Entry IDs (TEIs) that might be provided by the local telephone company.
   - Setting B channel protocol (asynchronous-to-synchronous PPP).
   - Other modem settings that have variable length parameters that require a carriage return to indicate the parameter length.
   - Saving and activating the new settings so they are restored after either resetting them or powering off the system.
   - The *U* interface active state probe command (ATD*x*), which allows the system to determine when synchronization with the ISDN central office switch has been achieved. The *x* can be any of the digits that are allowed for a telephone number, including # and *.
5. Click **Add** to additional modem commands. These can be with or without an associated parameter and a brief description to the command list. Any commands that you specify without an associated parameter can be assigned a parameter when the modem is associated with a line description.
6. Click **OK** to save your entries, and close the New Modem Properties page.

   Related reference

   "ISDN terminal adapters" on page 40
   Integrated Services Digital Network (ISDN) provides you with a digital connection that allows you to communicate by using any combination of voice, data, and video, among other multimedia applications.

Associating a modem with a line description

The topic demonstrates the steps for associating a modem with a line description.

1. In iSeries Navigator, select your system and expand **Network** → **Remote Access Services** → **Originator Connection Profiles or Receiver Connection Profiles**.
2. Select one of the following options:
   - To work with an existing connection profile, right-click a connection profile, and select **Properties**.
   - To work with a new connection profile, create a new one.
3. From the New Point-to-Point Profile Properties page, select the **Connection** tab, and click **New**.
   - Enter a name for the link configuration.
   - Click **New** to open the New Line Properties window.
4. From New Line Properties window, click the **Modem** tab, and select the modem from the list. The selected modem will be associated with this line description. For internal modems, the appropriate modem definition should already be selected. For more information, see the online help.

You can configure originator connection profiles to borrow a PPP line and modem assigned to a receiver connection profile that is awaiting an incoming call. The originating connection will return the PPP line and modem to the receiver connection profile when the connection has ended. To enable this new function, select the **Enable dynamic resource sharing** option from the **Modem** tab of the PPP line configuration window. You can configure PPP lines from the **Connection** tab of Receiver and Originator Connection Profiles.

Related tasks

"Creating a connection profile" on page 47
The first step in configuring a PPP connection between systems is to create a connection profile on the system.

Configuring a remote PC

To connect to a System i platform from a personal computer (PC) that runs any Windows 32-bit operating systems, you should verify that the modem is installed and configured properly, and ensure that you installed TCP/IP and Dial-Up Networking on the PC.

See your Microsoft® Windows documentation for information about configuring Dial-up Networking on the PC. Ensure that you specify or enter the following information:

- The type of dial-up connection should be **PPP**.
- If you are using encrypted passwords, ensure that you use CHAP-MD5 (MS-CHAP is not supported by the i5/OS operating system). Some versions of Windows do not support MD-5 CHAP directly, but it can be configured with additional help from Microsoft.
- If you are using unencrypted (or unsecured) passwords, Password Authentication Protocol (PAP) is automatically used. Any other unsecured protocol type is not supported by the system.
- Typically, IP addressing is defined by the remote system or the i5/OS operating system. If you intend to use alternate IP addressing methods (such as defining your own IP addresses), ensure that the system is also configured to accept your addressing method.
- Add DNS IP address if appropriate for your environment.

Configuring Internet access through the AT&T Global Network

If you want to communicate with the AT&T Global Network, you need to configure special profiles.

To access this service, you can use the AT&T Global Network Dial Connection wizard to help you configure a switched-dial PPP connection profile to dial the AT&T Global Network. The wizard walks you through about eight panels and takes about ten minutes to complete. You can cancel the wizard at any time and no existing data is saved.

The following types of applications can use the AT&T Global Network connection:

- **Mail Exchange**: It allows you to periodically retrieve mail from a single AT&T Global Network account and send it to your system for distribution to your Lotus® Mail users or to your Simple Mail Transfer Protocol (SMTP) users.
- **Dial-up Networking**: Use other dial-up networking applications with AT&T Global Network, such as standard Internet access.

You maintain the AT&T Global Network connection profiles like any other PPP connection profiles.

You need one of these adapters to use the AT&T Global Network Dial Connection wizard:

- 2699: Two-line WAN IOA
- 2720: PCI WAN/Twinaxial IOA
- 2721: PCI Two-line WAN IOA
- 2745: PCI Two-line WAN IOA (replaces IOA 2721)
- 2771: Two-port WAN IOA, with a V.90 integrated modem on port 1 and a standard communications interface on port 2. To use port 2 of the 2771 adapter, an external modem or ISDN terminal adapter with the appropriate cable is required.
- 2772: Two-port V.90 integrated modem WAN IOA
- 2793: 576C (CCIN of Quartz), two-port WAN IOA, with a V.92 integrated modem on port 1, and a standard communications interface on port 2. This replaces model 2771.
- 2805: Four-port WAN IOA, with an integrated V.92 integrated modem. This replaces models 2761 and 2772.

Before starting the AT&T Global Network Dial Connection wizard, you need to collect this information about your environment:

- The AT&T Global Network account information (account number, user ID, and password) for the mail exchange application or the dial-up networking application.
- The IP addresses of mail server and domain name server for the mail exchange application.
- The name of the modem that is used for single line connections.

To start the AT&T Global Network Dial Connection wizard, follow these steps:

1. In iSeries Navigator, expand your system and access **Network** → **Remote Access Services**.
2. Right-click **Originator Connection Profiles**, and select **New AT&T Global Network Dial Connection**.
3. When the AT&T Global Network Dial Connection wizard starts, click **Help** for information about completing a panel.

Connection wizards

You can use connection wizards to guide you through connection profile configuration.

New Dial Connection Wizard

This wizard describes the steps to configure a dial-up connection profile to access your ISP or intranet. You need to get some information from your network administrator or ISP to complete the wizard. For more information about completing this wizard, see the online help.

IBM Universal Connection Wizard

This wizard describes the steps to configure a profile that can be used by Electronic Customer Support software to connect to IBM. Electronic service support provides monitoring of your unique i5/OS environment to supply you with recommendations of personalized fixes for your system and situation.

Related information

Configuring a group access policy

The **Group Access Policies** folder under Receiver Connection Profiles provides options for configuring point-to-point connection parameters that apply to a group of remote users. It applies only to those point-to-point connections that originate from a remote system and are received by the local system.

To configure a new group access policy, follow these steps:

1. In iSeries Navigator, select your system and expand **Network** → **Remote Access Services** → **Receiver Connection Profiles**.
2. Right-click **Group Access Policies**, and select **New Group Access Policy**.
3. On the **General** tab, enter a name and description for the new group access policy.
4. Click the **Multilink** tab, and set up the multilink configuration.

   The multilink configuration specifies that you want to have multiple physical lines join together in a bundle. The maximum number of lines per bundle can be between 1 and 6. Because you do not know the type of line setting until a connection is made, the default value is always 1. The group policy can be used to extend or limit the Multilink protocol's capabilities for a specific user.

   Maximum links per bundle specifies the maximum number of links (or lines) that you want to become the one logical line. The maximum number of lines cannot be greater than the number of free lines when this group policy is applied to a session for a PPP profile.

   Check **Require bandwidth allocation protocol** if you want to specify that a connection is established only if the remote system supports the Bandwidth Allocation Protocol (BACP). If BACP cannot be negotiated, only a single link is allowed.
5. Click the **TCP/IP Settings** tab to enable any of the following settings:

   Allow remote system to access other networks (IP forwarding). This option specifies whether you want IP forwarding. If you select this option, you are essentially enabling the system to act as a router for this connection. This allows IP datagrams not destined for this system to pass through this system onto a connected network. If you leave this option blank, the IP discards those datagrams from the remote system that are not destined for any addresses local to this system.

   There might be security reasons why you do not want to allow IP forwarding. In contrast, an ISP generally provides IP forwarding. Note that this takes effect only if system-wide IP datagram forwarding is enabled; otherwise, it is ignored even if marked. System-wide IP datagram forwarding can be displayed from the **General** tab on the IPv4 Properties page.

   Request TCP/IP header compression (VJ). This option specifies whether you want IP to compress header information after it establishes a connection. Compressing typically increases performance, particularly for interactive traffic or slow serial lines. Header compression follows the Van Jacobson (VJ) method defined in RFC 1332. For PPP, compression is negotiated when the connection is established. If the other end of the connection does not support VJ compression, the system establishes a connection that does not use compression.

   Use IP packet rules for this connection. This option specifies whether you want to apply a filter rule for this group policy. Filter rules control the IP traffic in your network. You can use this IP packet filtering component to protect your system by filtering packets according to the rules that you specify. The rules are based on packet header information.

Applying a group policy to a remote access user

You can apply a group policy to a remote access user when you complete the point-to-point properties for a new receiver connection profile.

To apply a group policy to a remote access user, complete the following steps:

1. Click **Authentication** to open the Authentication page.
2. Click **Require this iSeries server to verify the identity of the remote system**.

3. Select **Authenticate locally using a validation list**.
4. If there is an existing validation list, select it from the list, and click **Open**. If you are creating it for the first time, enter a name for the new validation list, and click **New**.
5. Click **Add** to add a new user to the validation list.
6. On the Add User window, specify the following information:
   a. Select the authentication protocol for which the user name is defined.
   b. Enter the user name and password.

      Note: For security purposes, it is suggested that you do not use the same password for a user defined for Challenge Handshake Authentication Protocol 22314 (CHAP), Extensible Authentication Protocol (EAP), and Password Authentication Protocol (PAP).
   c. Check **Apply a group policy to the user**, select a group policy from the list, and click **Open**.

   You can change the group policy properties or work with the existing setup.
7. Click **OK** to complete the configuration and return to the Point-to-Point Properties page.

   Related reference

   "Scenario: Managing remote user access to resources using group policies and IP filtering" on page 24
   Group access policies identify distinct user groups for a connection, and allow you to apply common connection attributes and security settings to the entire group. You can use group policies, along with IP filtering, to permit and restrict access to specific IP addresses on your network.

   Related information

   IP filtering and network address translation

Applying IP packet filtering rules to a PPP connection

You can use a packet rules file to restrict the access of a user or a group to IP addresses on your network.

The IP filtering and network address translation topic in the Information Center discusses how to create IP packet rules that you can reference for a PPP connection profile.

You can see existing IP Packet filtering rules in two ways:

- Connection profile level
  1. When you complete the **Point-to-Point Properties** for a **Receiver Connection Profile**, select the TCP/IP Settings page, and click **Advanced**.
  2. Check **Use IP packet rules for this connection**, and select a PPP filter identifier from the list.
  3. Click **OK** to apply the PPP filter to the connection profile.
- User level
  1. Open an existing group access policy or create a new group access policy.
  2. Click the TCP/IP Settings page.
  3. Check **Use IP packet rules for this connection**, and select a PPP filter identifier from the list.
  4. Click **OK** to apply the PPP filter.

  Related reference

  "Scenario: Managing remote user access to resources using group policies and IP filtering" on page 24
  Group access policies identify distinct user groups for a connection, and allow you to apply common connection attributes and security settings to the entire group. You can use group policies, along with IP filtering, to permit and restrict access to specific IP addresses on your network.

Enabling RADIUS and DHCP services for connection profiles

Here are the steps for enabling RADIUS or Dynamic Host Configuration Protocol (DHCP) services for PPP receiver connection profiles.

1. In iSeries Navigator, select your system and expand **Network** → **Remote Access Services**.

2. Right-click **Remote Access Services**, and select **Services**.
3. Click the **DHCP-WAN** tab. This will automatically enable DHCP, and detect which DHCP server and relay agents (if any) are running on the system.
4. To enable RADIUS services, click the **RADIUS** tab.
   a. Select **Enable RADIUS Network Access Server connection**
   b. Select **Enable RADIUS for authentication**.
   c. If applicable to your RADIUS solution, you can also enable RADIUS accounting and TCP/IP address configuration.
5. Click the **RADIUS NAS settings** button to configure the connection to the RADIUS server.
6. Click **OK** to return to iSeries Navigator.

   Related reference

   "Scenario: Authenticating dial-up connections with RADIUS NAS" on page 22
   A Network Access Server (NAS) running on the system can route authentication requests from dial-in clients to a separate Remote Authentication Dial In User Service (RADIUS) server. If authenticated, RADIUS can also control the IP addresses assigned to the user.

Managing PPP

This topic contains information about the PPP management tasks that you can do on the system.

Related reference

"Related information for PPP" on page 66
Listed below are the IBM Redbooks (in PDF format) that provide additional information about Remote Access Services PPP connections. You can view or print the PDFs.

Setting properties for PPP connection profiles

When you create a connection profile, you typically select the protocol, connection type, and operating mode for the new connection profile on the Point-to-Point Connection Profile Setup window.

After you enter your selections on this window, the connection profile property sheet appears. The selections that you specify on the Point-to-Point Connection Profile Setup window determine the page content and tab order of the connection profile property sheet. The property sheet is different for originator connection profiles and receiver connection profiles.

You can use these guidelines when you complete each page of the New Point-to-Point Profile Properties window. The settings that you select on each page depend on your environment and the type of connection that you are configuring. The iSeries Navigator online help describes each option that is shown on the window. For more information, you can also refer to the PPP examples and procedures .

Monitoring PPP activity

You can view a connection profile and a session log by using iSeries Navigator.

About PPP connection jobs:

- There are two PPP control jobs that are used to manage the individual PPP connection jobs. These jobs run in the QSYSWRK subsystem:
  - QTPPPCTL - Main PPP Control job. This job manages each PPP connection job.
  - QTPPPL2TP - L2TP server. This job manages the L2TP tunnel establishment and only runs if an L2TP profile is currently running.
- PPP connection threads in QTPPPCTL run under the QTCP user name.
- SLIP connection jobs run in the QSYSWRK subsystem under the QTCP user name. There are two types of SLIP job names:
  - QTPPDIAL*nn* are dial-out jobs where *nn* is any number from 1 to 99.

- QTPPANS*nn* are dial-in jobs where *nn* is any number from 1 to 99.

Working with connection profiles:

1. In iSeries Navigator, expand your system and access **Network** → **Remote Access Services**. Select **Originator Connection Profile** or **Receiver Connection Profile**.
2. In the Profile column, right-click any connection profile name, and select one of the following options:
   - **Connections** opens a window to display information about all connections associated with the profile. The information can include connection data for a current connection, previous connections, or both. Options to see job output, connection details, call logs, or message logs for each connection are available.
   - **Properties** opens the Property pages to display current properties for a connection.

Viewing connection information:

1. In iSeries Navigator, expand your system and access **Network** → **Remote Access Services**. Select **Originator Connection Profile** or **Receiver Connection Profile**.
2. In the Profile column, right-click any connection profile name that does not have an Inactive status, and select **Connections** to view connection information.

   Each connection for this profile is shown (current and previous). The status field indicates the current status of the connection. Additional information such as the user ID of the connected user, thread ID, local and remote IP addresses, and the name of the PPP job might be shown depending on the status of each PPP job.
3. To view job output, details for a connection, call logs, or message logs, right-click a connection to enable the buttons.
4. To view QTPPPCTL, click **Jobs**. From the connections window, right-click the job name, and select **Printer Output** or **Job Log** to display information about all the connection threads associated with the QTPPPCTL.
5. To view connection details click **Details**. Details can only be displayed for currently active connections. The details window will allow you to see additional connection information for this particular connection.
6. To view call logs, click **Call Log**.
7. To view message logs, click **Message Log**.

Working with PPP Output from the system:

To work with PPP output, enter WRKTCPPTP from the system command line:

- To work with ALL active PPP jobs (including the QTPPPCTL and QTPPPL2TP jobs), press F14 (Work with active jobs).
- To work with all output for a particular connection profile, select **option 8** (work with output) for that profile.
- To print PPP profile configuration, select **option 6** (Print) for that profile. Then use the WRKSPLF command to access the printed output.

Connection status:

The connection profile status is displayed in the **Status** field for each profile in the list of connection profiles under **Network** → **Remote Access Services** after selecting either Originator or Receiver profiles. Status for an individual connection is displayed using the Connections window.

Table 10. Primary status description

Primary status description	Explanation
Waiting for connection requests	Receiver profile is ready for a connection

Table 10. Primary status description (continued)

Primary status description	Explanation
Waiting for incoming call	The system is ready for a connection
Connecting	In the process of connecting with the remote system
Active/Active connections	Connection has been made and the job is running successfully
Inactive	No jobs are currently running for this connection profile
Ended	Information available
Multihop terminator is starting a multihop initiator	Multihop in progress
Multihop connection is active	Multihop successfully connected

Table 11. Secondary status description

Secondary status description	Explanation
Initializing modem	initializing modem at the start of a dialup connection
Waiting for modem connection	PPP Server in the listen state
DIALING xxx-xxxx	number dialed by the dialup client
Incoming call detected	PPP Server detects an incoming modem call
Modem connected	PPP handshaking successfully complete
Operational	PPP connection active
Link terminated	Connection ended by the peer
Stopped	Profile or job ended
Authentication failure	PPP connections failed to establish due to failed authentication
Connection inactivity timeout	PPP connections failed to establish due to inactivity timeout
Negotiating IP addresses	PPP connections ended due to IP negotiation problems
Remote modem did not answer	PPP connections failed to establish due to no response from the other side
Protocol reject	PPP connections failed to establish due to NCP negotiation failure
Retry failure	PPP connection failed to establish because retry count was exceeded
Received PPPoE session confirmation from peer	PPPoE negotiation successfully complete
L2TP call established	L2TP tunnel up message

Troubleshooting PPP

If you experience Point-to-Point Protocol (PPP) connection problems, you can use the checklist to gather error information. This checklist can help you identify error symptoms and resolve PPP connection problems.

Current and relevant information about program temporary fixes (PTFs) and troubleshooting is documented on the TCP/IP for i5/OS Web site. This Web site provides the latest information that supplements and overrides the information that is contained in this topic.

1. Required supporting material:
   - Remote host type, operating system, and level

- i5/OS host operating system level
- All output files that are saved in an output queue with the same name as the profile
- Job logs for QTPPPCTL and QTPPPL2TP (if an L2TP profile)
- The connection script that is used in your environment
- Status of connection profile before and after the connection fails

2. Recommended supporting material:
   - Line description
   - Connection profile

     Option 6 from WRKTCPPTP prints the profile settings.
   - Modem type and model
   - Modem command strings
   - Communications trace

The ITSO Redbook V4 TCP/IP for AS/400: More Cool Things Than Ever covers the following PPP problems. It also provides detailed problem resolution information.

To identify the problems and find out the solutions, see the checklist in the following table.

Table 12. PPP problems from ITSO Redbook

Problem	Solution
Modem hardware configuration Wrong configuration of dip-switches and other hardware settings	Make sure that the modem is configured for the correct framing type. This can be either *Asynchronous* or *Synchronous*. Refer to the modem manual for more information.
Modem AT commands The modem you are trying to use is not in the predefined list of modems in iSeries Navigator.	Create a new modem.
PPP users and passwords You are getting user name and password errors when attempting a PPP connection.	• Ensure that the user ID and password are entered using the same case. • Ensure that the authentication protocol used by the peers is the same. • Do not use PAP at one peer, while the other peer is configured as CHAP.
PPP lines for starting a connection profile Identified PPP lines are used by the same hardware resource.	Remember to vary off other lines using the same hardware resource.
PPP protocol Connection errors can occur due to misconfiguration of the PPP protocol.	Investigating the lower-levels of the PPP protocol might be necessary in some situations where the peers are unable to communicate with each other due to a configuration error. If the PPP log or the job log of the PPP job does not show any indication of the problem, you can investigate the problem by using the communications trace function.

Related concepts

"Configuring your modem for PPP" on page 55

A modem provides you with analog connection capabilities (leased and switched lines). For your analog Point-to-Point Protocol (PPP) connections, you can use an external modem, internal modem, or Integrated Services Digital Network (ISDN) terminal adapter.

"Configuring a new modem" on page 55
You can configure a new modem using an existing modem description or base the modem description on a previous modem description.

Related reference

"Related information for PPP"
Listed below are the IBM Redbooks (in PDF format) that provide additional information about Remote Access Services PPP connections. You can view or print the PDFs.

Related information for PPP

Listed below are the IBM Redbooks (in PDF format) that provide additional information about Remote Access Services PPP connections. You can view or print the PDFs.

IBM Redbooks

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

Web sites

Find the latest program temporary fixes (PTFs), and the latest configuration information for PPP and L2TP through the PPP link on the TCP/IP for i5/OS Web site . This Web site provides the latest information that supplements and overrides the information that is contained in this topic collection.

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming Interface Information

This Remote access services: PPP connections publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

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

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA