IBM

eserver

iSeries

Remote Access Services: PPP connections

IBM Confidential

IBM

@server

iSeries

Remote Access Services: PPP connections

IBM Confidential

Contents

Part 1. Remote Access Services: PPP connections

Point-to-Point Protocol (PPP) is an Internet standard for transmitting data over serial lines. It is the most widely used connection protocol among Internet Service Providers (ISPs). PPP allows individual computers to access networks, which in turn provide access to the Internet. The iSeries server 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 iSeries server. Through PPP, remote systems that are connected to your iSeries server can access resources or other machines that belong to the same network as your server. You can also configure your iSeries server to connect to the Internet by using PPP. The iSeries Navigator Dial-Up Connection Wizard can guide you through the process of connecting your iSeries server to the Internet or to an internal network.

- What's new for V5R2? describes updates to Remote Access Services for this release.
- Print this topic allows you to download or print the PDF version of this information.

Understanding Remote Access Services: PPP Connections

These topics quickly introduce you to remote access services that are on your iSeries 400 server. The topics below can help you plan a PPP environment for your network.

- **PPP scenarios** are samples of different connectivity implementations of PPP. Each example provides instructions and specify sample values for configuring the PPP connection.
- **PPP concepts** provides information on PPP concepts and iSeries 400 server requirements for PPP connections.
- **Plan PPP** provides information on PPP concepts and iSeries 400 server requirements for PPP connections.

Using Remote Access Services: PPP Connections

These topics can assist you as you configure and manage PPP connections on your iSeries 400 server.

- **Configure PPP** outlines the basic steps for configuring a PPP connection.
- **Manage PPP** provides information that you can use as a guide for managing PPP connections.
- **Troubleshoot PPP** describes basic PPP connection errors and points you to relevant troubleshooting information.

You can also find other information about PPP here. This page contains links to useful and related iSeries server information.

Chapter 1. What's new for V5R2

For V5R2, iSeries Navigator can enable PPP over Ethernet (PPPoE) connections originating from the iSeries server. This support provides a new PPPoE virtual line type, which is bound to a physical Ethernet line, to establish a PPP connection using an Ethernet LAN adapter attached to a DSL modem. Once the connection between the iSeries and the ISP has started, individual users on the LAN can access the ISP over the iSeries PPPoE connection. You can access this new function from the Originator connection profile dialog or the Universal Connection Wizard.

For more information, see Connect your iSeries server to a PPPoE access concentrator

Several additions to iSeries Navigator now make it easier to configure and manage PPP connections, including:

- The DHCP-WAN configuration dialog will now automatically contact the DHCP server and client interface to determine the IP address for the DHCP-WAN client interface. To access this dialog:
  - Expand **Network > Remote Access Services**
  - Right-click on **Remote Access Services**
  - Select **Services**
  - Select the **DHCP-WAN** tab
- An improved connections status dialog now displays connection details for L2TP, L2TP multihop, multilink and PPP over Ethernet connections, making it easier to manage your PPP connections.
- The ability to create Originator and Receiver connection profiles and Group Access Policies have been added to the Task Pad.
- The New Dial Connection Wizard and the Universal Connection Wizard have been renamed, and are now called New Internet or ISP Dial Connection, and New IBM Universal Connection.
- Originator connection profiles may now ″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 dialog. You can configure PPP lines from the Connection tab of Receiver and Originator connection profiles.
- Line pool properties may no longer be modified while they are in use, which prevents potential line pool problems.
- Support for the Initiator-on-demand and Remote dial-on-demand operating modes has been dropped from Originator connection profiles using L2TP connections.

Chapter 2. Print this topic

You can view or download a PDF version of this document for viewing or printing. You need Adobe® Acrobat® Reader to view PDF files. You can download a copy from Adobe  .

To view or download the PDF version, select Remote Access Services: PPP connections  (277 KB or about 58 pages).

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

1. Open the PDF in your browser (click the link above).
2. In the menu of your browser, click **File**.
3. Click **Save As**.
4. Navigate to the directory in which you would like to save the PDF.
5. Click **Save**.

Chapter 3. PPP scenarios

The following scenarios help you understand how PPP works, and how you can implement a PPP environment in your network. These scenarios introduce fundamental PPP concepts from which beginners and experienced users can benefit before they proceed to the planning and configuration tasks.

Scenario: Connect your iSeries server to a PPPoE access concentrator

Many ISPs offer high speed Internet access over DSL using PPPoE. The iSeries server can connect to these service providers to offer high bandwidth connections that preserve the benefits of PPP.

Scenario: Connect remote dial-in clients to your iSeries server

Remote users, such as telecommuters or mobile clients, often require access to a company's network. These dial-in clients can gain access to an iSeries server with PPP.

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

Administrators typically set up office networks that allow employees access to the Internet. They can use a modem to connect the iSeries server to an Internet Service Provider (ISP). LAN-attached PC clients can communicate with the Internet using the iSeries server as a gateway.

Scenario: Connect 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. PPP can connect the two LANs together by establishing a connection between an iSeries server in the central office and another iSeries server in the branch office.

Scenario: Authenticate dial up connections with RADIUS NAS

A Network Access Server (NAS) running on the iSeries server can route authentication requests from dial-in clients to a separate RADIUS server. If authenticated, RADIUS can also control the IP addresses and ports to the user.

Scenario: Manage 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 some common connection attributes and security setting to the entire group. In combination with IP filtering, this allows you to permit and restrict access to specific IP addresses on your network.

Scenario: PPP and DHCP on a single iSeries server

Dial-in clients or remote users can gain access to an iSeries server in a company's network with PPP. The DHCP Wide Area Network (WAN) client on the same iSeries allows remote users to obtain a dynamically assigned IP address using the same services as LAN attached users.

Scenario: DHCP and PPP profile on different iSeries servers

Security concerns or the physical layout of a network lead most companies to separate network services and distribute them to different servers. This scenario handles the added complexity of having a separate PPP server and a DHCP server. Like the previous scenario, this setup allows remote users to dial in and gain access to a company's network.

Scenario: PPP and VPN: L2TP voluntary tunnel protected by VPN

A branch office can connect to the corporate office through Layer 2 Tunnel Protocol (L2TP). An L2TP voluntary tunnel establishes a virtual PPP link. In effect, L2TP extends the corporate office's network, such that the branch office appears to be part of the corporate subnet. VPN protects the data traffic over the L2TP tunnel.

Scenario: Connect your iSeries server to a PPPoE access concentrator

Situation: Your business requires a faster Internet connection, so you're interested in a DSL service with a local ISP. After an initial investigation, you find that your ISP uses PPPoE to connect its clients. You would like to use this PPPoE connection to provide high-bandwidth Internet connections through your iSeries server.

Figure 1. Connecting your iSeries server to an ISP with PPPoE

Solution: You can support a PPPoE connection to your ISP through your iSeries server. The iSeries server makes use of a new PPPoE virtual line type which is bound to a physical Ethernet line configured to use a type 2838 Ethernet adapter. This virtual line supports PPP session protocols over an Ethernet LAN connected to a DSL modem which provides the gateway to the remote ISP. This allows LAN connected users to have high speed internet access using the iSeries servers PPPoE connection. Once the connection between the iSeries and the ISP has started, individual users on the LAN can access the ISP over PPPoE, using the IP address allocated to the iSeries server. To provide additional security, filter rules can be applied to the PPPoE virtual line to restrict certain inbound Internet traffic.

Sample Configuration:

1. Configure the connection device for use with your ISP.
2. Configure an Originator Connection Profile on your iSeries server.
   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 will refer to both the connection profile and the virtual PPPoE line.
4. Click 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 will display the line properties dialog.
   a. On the **General** page, enter a meaningful description for the PPPoE virtual line.
   b. Click 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 will display the Ethernet line properties dialog. **Note:** PPPoE requires a type 2838 Ethernet adapter.
      1) On the **General** page, enter a meaningful description for the Ethernet line, and verify that the line definition is using the desired hardware resources.
      2) Click the **Link** page. Enter the properties for the physical Ethernet line. Refer to the documentation for your Ethernet card and the online help for more information.
      3) Click the **Other** page. Specify the level of access and authority other users may 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.
5. If your ISP requires the iSeries server to authenticate itself, or if you want the iSeries to authenticate the remote server, click on the **Authentication** page. For more information, refer to System authentication.
6. Click the **TCP/IP Settings** page, and specify the IP address handling parameters for this connection profile. To allow LAN attached users to connect to the ISP using the IP addresses allocated to the iSeries server, select **Hide addresses (Full masquerading)**.
7. Click 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 the **Other** page.
9. Click **OK** to complete the profile.

For information about restricting users access to external IP address or iSeries resources, refer to IP filtering and Group Access Policies.

Scenario: Connect remote dial-in clients to your iSeries server

Situation: As an administrator of your company's network, you must maintain both your iSeries server and network clients. Instead of coming into work to troubleshoot and fix problems, you would like the capability to do work from a remote location, such as your home. Since your company does not have an Internet bound network connection, you could dial into your iSeries server using a PPP connection. Additionally, the only modem you currently have is your 7852-400 ECS modem and you would like to utilize this modem for your connection.

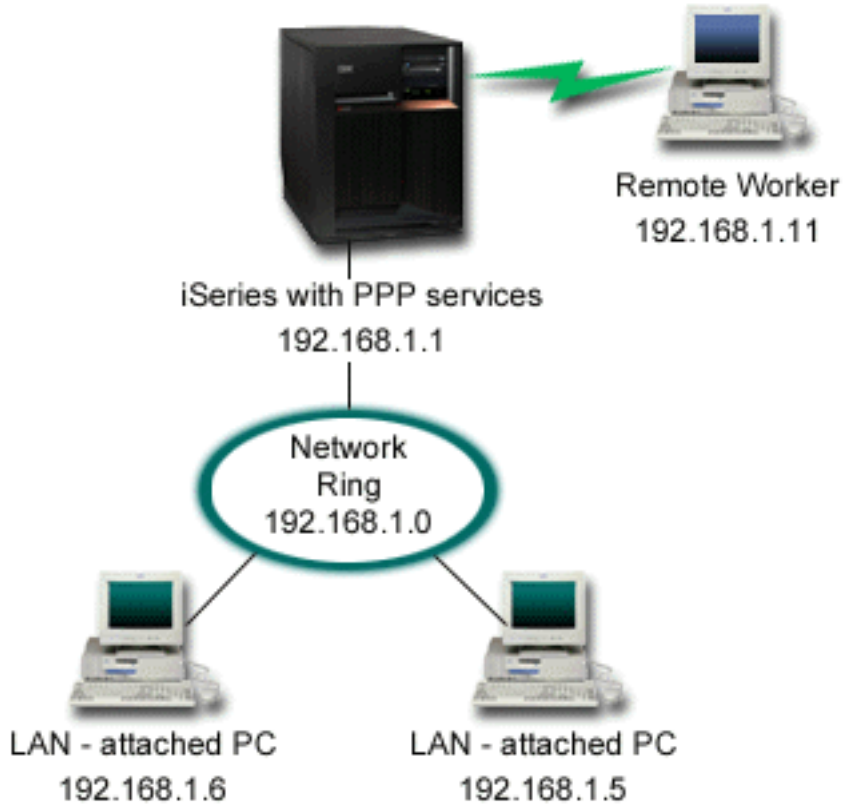

Figure 2. Connecting remote clients to your iSeries server

Solution: You can use PPP to connect your home PC to your iSeries server using your modem. Since you are using your ECS modem for this type of PPP connection, you must ensure that your modem is configured for both synchronous and asynchronous modes. The above illustration depicts an iSeries server with PPP services that is connected to a LAN with two PCs. The remote worker then dials into the iSeries server, authenticates itself, and then 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 CHAP-MD5 to authenticate with the iSeries server. The iSeries cannot use MS_CHAP, so you must make sure your PPP client is set to use 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 above illustration only has one remote dial-in client, because the ECS modem can only handle one connection at a time. If your needs require multiple simultaneous dial-in clients, then see the planning section for both hardware and software considerations.

Sample Configuration:

1. Configure Dial-up Networking and create a dial-up connection on the remote PC.
2. Configure a Receiver Connection Profile on your iSeries server.
   Ensure that you enter the following information:
   - **Protocol type**: PPP

- **Connection type**: Switched-line
- **Operating mode**: Answer
- **Link configuration**: This may 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 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 the **Modem** page. From the Name select list, choose the **IBM 2772** modem.
   c. Click **OK** to return to New Point-to-Point Profile Properties page.
5. Click on 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 on the **TCP/IP Settings** page.
   a. Select the local IP address of `192.168.1.1`.
   b. For the remote address, select **Fixed IP address** with a starting address of `192.168.1.11`.
   c. Select **Allow remote system to access other networks**.
7. Click **OK** to complete the profile.

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

Situation: The corporate application that your company uses now requires your users to access the Internet. Since the application does not require large amounts of data exchange, you would like to be able to use a modem to connect both your iSeries server and LAN-attached PC clients to the Internet. The following illustration describes an example of this situation.

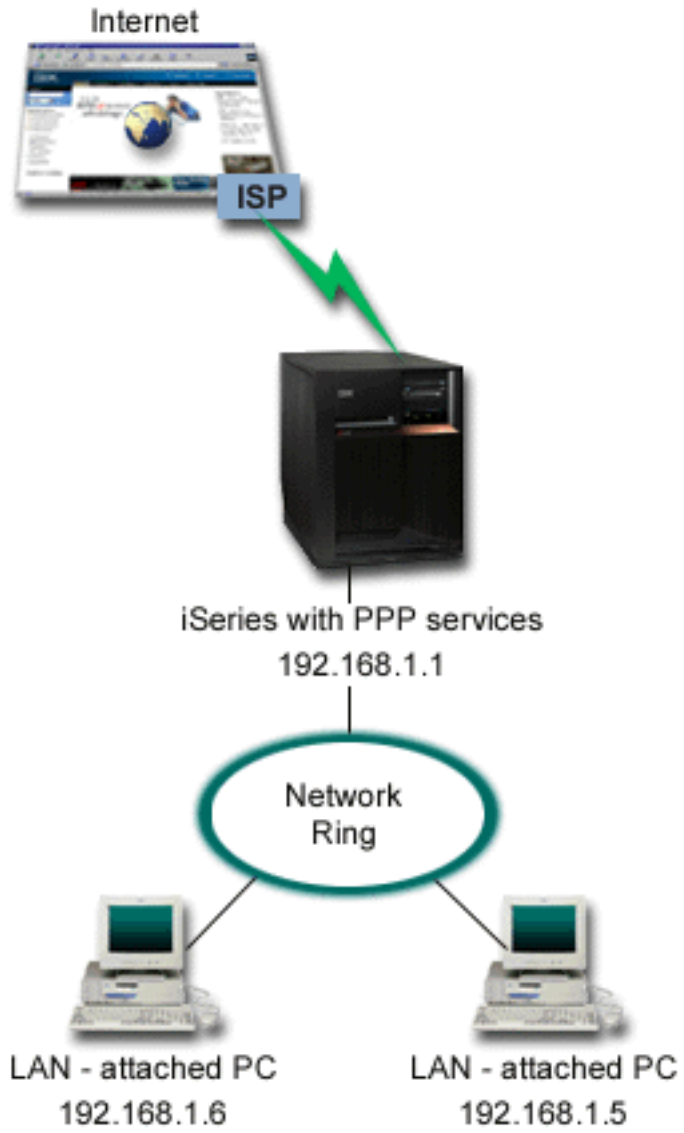

Figure 3. Connecting your office LAN to the Internet with a modem

Solution: You can use your ECS (or other compatible) modem to connect your iSeries to your Internet Service Provider (ISP). You need to create a PPP originator profile on the server to establish the PPP connection to the ISP.

Once you make the connection between the iSeries and the ISP, your LAN-attached PCs can communicate with the Internet using the iSeries as a gateway. In the originator profile, you will want to make sure that Hide addresses option is on, so that the LAN clients, which have reserved IP addresses, can communicate with the Internet.

Now that your iSeries and network is attached to the Internet, you must understand your security risk. Work with your ISP to under to understand their security policy and take further actions to protect your server and network.

If you are using your ECS modem for this type of PPP connection, configure your modem for asynchronous communication. Depending on your Internet usage, bandwidth could become a concern. To learn more about how to increase the bandwidth of your connection, refer to the planning section.

Sample Configuration:

1. Configure an Originator Connection Profile on your iSeries server.

   Ensure that you select the following information:

   - **Protocol type**: PPP
   - **Connection type**: Switched-line
   - **Operating mode**: Dial
   - **Link configuration**: This may 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 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 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 phone number to dial to reach the ISP server. Ensure that you include any required prefix.
5. Click 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 the TCP/IP Settings 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 the **DNS** page, enter the IP address of the DNS server 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 Operations 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 Internet bound TCP/IP traffic from these systems will be sent to the iSeries server.

Scenario: Connect your corporate and remote networks with a modem

Situation: Suppose that you have a branch and corporate networks in two different locations. Everyday 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.

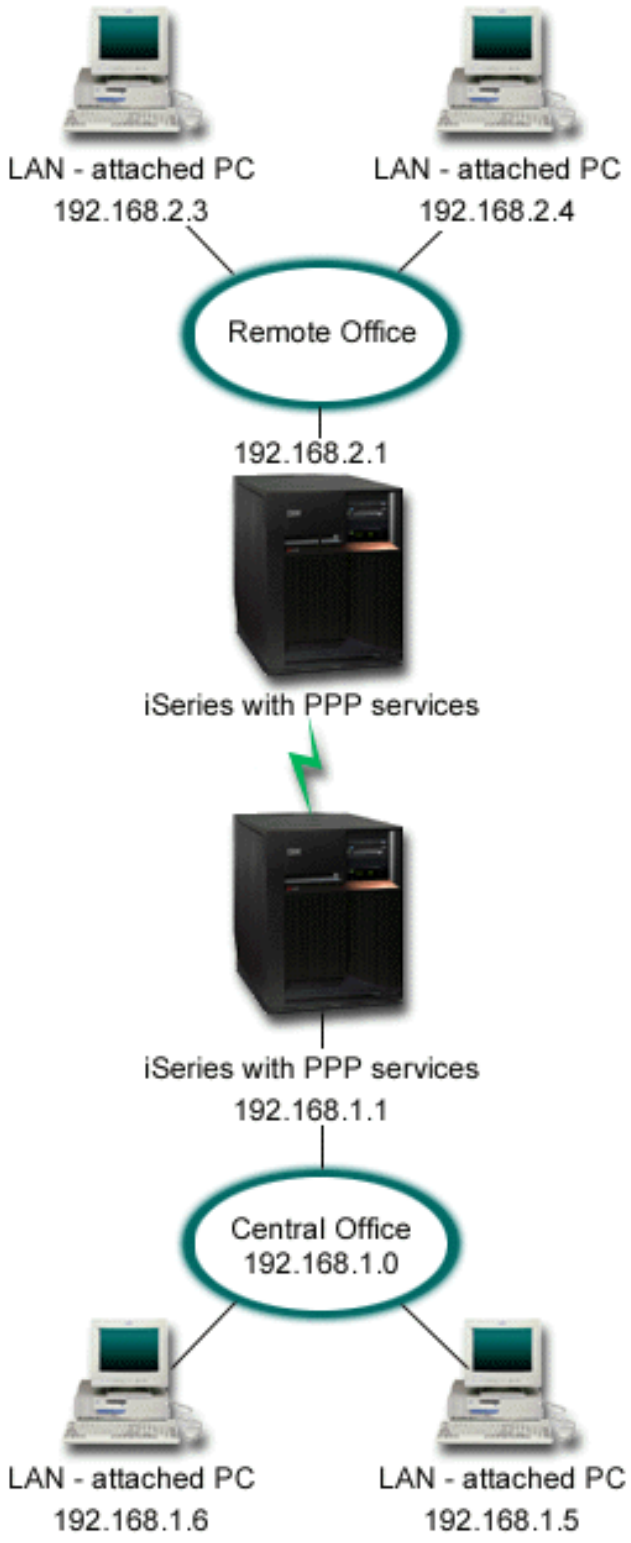

Figure 4. Connecting your corporate and remote networks with a modem

Solution: PPP can connect the two LANs together by establishing a connection between each iSeries server as in the above illustration. In this case, assume that the remote office initiates the connection to the central office. You would configure an originator profile on the remote iSeries and a receiver profile on the central office server.

If the remote office PCs need access to the corporate LAN (192.168.1.0), then the central office receiver profile would 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:

1. Configure an Originator Connection Profile on the Remote Office iSeries server.

   Ensure that you select the following information:

   - **Protocol type**: PPP
   - **Connection type**: Switched-line
   - **Operating mode**: Dial
   - **Link configuration**: This may 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 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 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 phone number to dial to reach the Central Office iSeries server. Ensure that you include any required prefix.
5. Click 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 or password information.
6. Click on 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 iSeries server.

   Ensure that you select the following information:

   - **Protocol type**: PPP
   - **Connection type**: Switched-line
   - **Operating mode**: Answer
   - **Link configuration**: This may 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 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 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 on 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 on 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 would 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 iSeries servers as a gateway.
12. Click **OK** to complete the receiver profile.

Scenario: Authenticate dial up connections with RADIUS NAS

Situation: Your corporate network has remote users dialing into two iSeries servers from a distributed dial-up network. You would like a way to centralize authentication, service and accounting, allowing one server to handle requests for validating user IDs and passwords, and determining which IP addresses are to them.

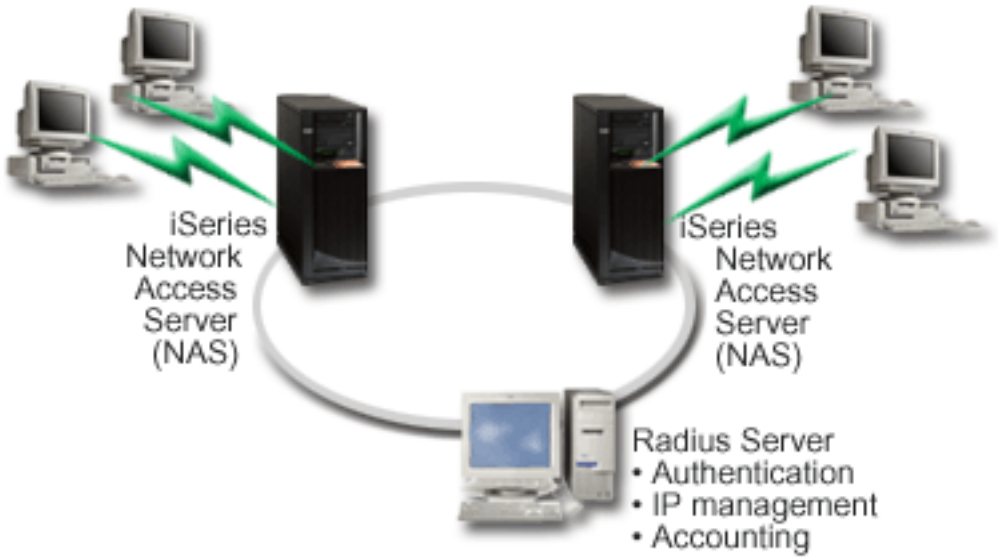

Figure 5. Authenticate dial up connections with a RADIUS server

Solution: When users attempt to connect, the Network Access Server (NAS) running on the iSeries servers 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 iSeries.

Sample Configuration:

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 may 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) page(s), click **Add** and enter the following information:
   a. In the **Local IP address** box, enter the IP address for the iSeries interface used to connect with 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 used to identify the iSeries server to the RADIUS server.
   d. In the **Port** box, enter the port on the iSeries used to communicate with the RADIUS server. Enter 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. (EAP, PAP, or CHAP-MD5) This protocol must also be used by the RADIUS server. Refer to System Authentication for more information.
12. Select **Use RADIUS for connection editing and accounting**.
13. Click **OK** to save the changed 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 iSeries will forward the authentication information to the specified RADIUS server. If the user is validated, the connection will be allowed, and will use any connection restrictions specified in the user's information on the RADIUS server.

Scenario: Manage remote user access to resources using Group Policies and IP filtering

Situation: Your network has several groups of distributed users, each of whom need access to different resources on your corporate LAN. A group of data entry users needs access to the data base and several other applications, while a business partner needs dial-up access to HTTP, FTP and Telnet services, but for security reasons must not be allowed access to other TCP/IP services or traffic. Defining detailed connection attributes and permissions for each user would duplicate your efforts, and providing network

restrictions for all the users of this connection profile won't provide enough control. You'd like a way to define connection setting and permissions for several distinct groups of users who routinely dial into this server.

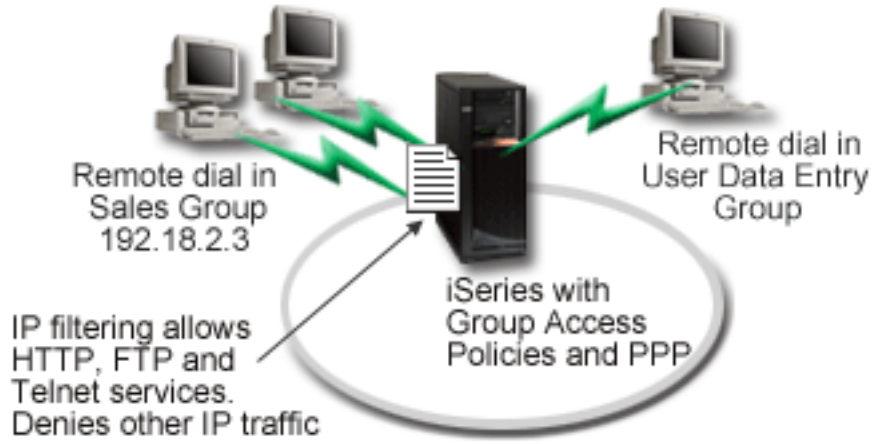

Figure 6. Apply connection settings to dial-up connections based on group policy settings

Solution: You need to apply unique IP filtering restrictions to two different groups of users. To accomplish this, you will create group access policies and IP filter rules. Group access policies reference IP filter rules, so you need to create your filter rules first. In this example, you need to create a PPP filter to include IP filter rules for the ″Business partner″ Group Access Policy. These filter rules will permit HTTP, FTP and Telnet services, but restrict access to all other TCP/IP traffic and services through the iSeries server. This scenario only shows the filter rules needed for the sales group; however, you could 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. Group access policies allow you to define common connection attributes to a group of users. By adding a Group Access Policy to a Validation list on the iSeries server, 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 will restrict the IP addresses, and TCP/IP services available to a user during their session.

Sample Configuration:

1. Create the PPP filter identifier and IP packet rules filters that specify the permissions and restrictions for this Group Access Policy. For more information about IP filtering, see IP packet rules (Filtering and NAT) .
   a. In iSeries Navigator, expand **Network > Remote Access Services**.
   b. Click **Receiver Connection Profiles**, right–click the connection profile for this connection and select **Properties**.
   c. Select the **TCP/IP Settings** tab, and click **Advanced**.
   d. 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.
   e. 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 includes 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

FILTER SET services_rules ACTION = PERMIT DIRECTION = * SRCADDR =  %
        * DSTADDR = * PROTOCOL = ICMP TYPE = * CODE = * 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 = 192.54.5.1 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.54.5.1 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
        = 23 FRAGMENTS = NONE JRN = OFF
```

f. 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

      ```
      permited_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 = permited_services SET = services_rules
      ```

g. Save your changes, and exit. If you need to undo these changes later, use the character-based interface to enter the command:

   ```
   RMVTCPTBL
   ```

   This will remove all filter rules and NAT on the server.

h. 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. For a detailed description of the options for Group Access Policies, see, Configure a Group Access Policy.
   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.

For more information about authenticating users over a PPP connection, see System Authentication.

Chapter 4. PPP concepts

You can use PPP to connect an iSeries server to remote networks, client PCs, another iSeries or an ISP. To fully utilize this protocol, you should understand both the capabilities and iSeries support for this protocol. Refer to the following topics for more information.

What is PPP?
Point-to-Point Protocol (PPP) is a TCP/IP protocol used to connect one computer system to another. See this topic for a more detailed definition.

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

Group Access Policies
These policies define a set of connection and security attributes for a group of users. See this topic for information on defining these on your system.

What is PPP?

Computers use **PPP**, or **Point-to-Point Protocol**, to communicate over the Internet through telephone lines. 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 is an Internet standard. It is the most widely used connection protocol among Internet Service Providers (ISPs). You can use PPP to connect to your ISP; your ISP then gives you connectivity to the Internet.

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 at http://www.rfc-editor.org.

- RFC1661 Point-to-Point Protocol
- RFC1662 PPP on HDLC-like framing
- RFC1994 PPP CHAP

Connection profiles

V5R2 uses two types of profiles to allow you 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 iSeries server 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 iSeries server. You can configure inbound connections using this object.

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

- What type of connection protocol will you use? (PPP or SLIP)
- Does your iSeries server contact the other computer by dialing out (originator)? Does your iSeries server wait to receive a call from the other system (receiver)?
- What communications line will the connection use?

- How should your iSeries server determine which IP address to use?
- How should your iSeries server authenticate another system? Where should your iSeries server store the authentication information?

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

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

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

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

  Connection type specifies the type of line your connections rest on and the whether or not they are **dial** or **answer** (originator or receiver, respectively). You can select among these connection types:
  - Switched line
  - Leased (dedicated) line
  - L2TP (virtual line)
  - PPPoE (virtual line)

  PPPoE is only supported for Originator connection profiles.
- **Operation Mode**. The available operating mode depends on the type of connection. Refer to the following table:

  Refer to the following table for Originator connection profiles:

Table 1. Available operating modes for Receiver 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

Refer to the following table for receiver connection profiles:

Table 2. Available operating modes for Originator connection profiles.

Connection type	Available Operating Modes
Switched line	Answer

Table 2. Available operating modes for Originator connection profiles. (continued)

Connection type	Available Operating Modes
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
  – Integrated ISDN line

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

Group policy support

Group Policy support enables network administrators to define user based group policies to help manage resources and allows access control policies to be assigned to individual users when logging into the network with a PPP or L2TP session. The concept here is that users can be identified as belonging to a specific class of user, where each class would have it's own unique policy. Each unique Group Policy allows definition of resource limits such as number of links allowed in a Multilink bundle, attributes such as IP Forwarding, and identification of what set of IP Packet Filter rules to apply. With Group Policy support network administrators could define for example a Work_at_Home group that allows that class of user full access to the network while a Vendor_Workers group may be restricted to a more limited set of services.

For an example, see Scenario: Manage user access to resources using Group Access Policies and IP address filtering.

Chapter 5. Plan PPP

Creating and administering PPP connections requires familiarity with both PPP support and connection alternatives in the iSeries servers, and also with many of the networking and security plans your business uses. The following topics can help you become familiar with the available options and requirements for iSeries PPP connections.

Software and hardware requirements
iSeries Navigator V4R4 or higher supports PPP connections. See this topic for a list of other requirements.

Connection alternatives
The iSeries supports PPP connections over a variety of media, from analog or digital phone lines, to dedicated or fractional T1 connections. See this topic for a description of supported connection options.

Connection equipment
iSeries servers use modems, ISDN terminal adapters, Token Ring adapters, Ethernet adapters or CSU/DSU devices to handle PPP connections. See this topic for information about supported hardware.

IP address handling
PPP connections have several options for IP address assignment and IP packet filtering during connections. See this topic for descriptions of these options.

System authentication
The iSeries can authenticate dial-up connections using either a validation list and exchange of passwords, or a RADIUS server. It also provides authentication information to systems it is connecting to. See this topic for a description of authentication options.

Bandwidth considerations
The iSeries supports the Multilink protocol for PPP connections. This allows you to use multiple analog phone lines for a single connection to increase the bandwidth. See this topic for an overview of this support.

Software and hardware requirements

A PPP environment requires that you have two or more computers that support PPP. One of these computers, the iSeries server, can either be the originator or receiver. The iSeries server must meet the following prerequisites so remote systems can access it.

- **Operations Navigator** Release 4 Version 4 (V4R4) or higher 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 (95/98/NT/Millenium/2000/XP)** with iSeries Navigator.
- An installed adapter

  You can choose one from the following adapters:
  - 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)
  - 2742*: two line IOA (replaces IOA 2745)
  - 2750: PCI ISDN V.90 Basic Rate Interface U IOA (2-wire interface)
  - 2751: PCI ISDN V.90 Basic Rate Interface U IOA (4-wire interface)
  - 2761: Eight-port analog modem IOA

  - 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
  - 2838: Ethernet adapter for PPPoE connections.
  - 2793*: 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 2793 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 ISDN terminal adapter, and an RS232 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 phone numbers and information for the Internet connection.

Connection alternatives

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 HDLC-like framing for encapsulating datagrams over both asynchronous and synchronous point-to-point telecommunication links.

While PPP supports a wide range of link types, SLIP only supports 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 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 phone lines
- Digital services and DDS
- Switched-56
- ISDN
- T1/E1 and fractional T1
- Frame Relay
- L2TP (tunneling) support for PPP connections
- PPPoE (DSL) support for PPP connections

Analog phone 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-phone lines. The fastest modems today operate at an uncompressed rate of 56Kbps. 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 usually 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 may even increase with V.42bis applied. X2 or 56Flex extends the bps rate to 56k 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 56Kbps 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 RS232 serial interface with an asynchronous protocol at rates up to 115.2Kbps.

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 56Kbps. 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 33.6Kbps. 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 48Kbps. Additionally, connection times may be reduced due to improvements in the hand-shaking process, and modems that support a ″hold″ feature can now remain connected while the phone line accepts in coming call or uses call-waiting.

Digital Services and DDS

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.

DDS

Digital Data Services (DDS) is the most basic of digital services. DDS links are leased, permanent connections, running at fixed rates of up to 56Kbps. 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 the 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 30,000 feet. Telephone companies can accommodate longer distances with signal extenders, but this service comes at 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 may be 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 56Kbps.

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 DDS setup in that the DTE connects to the digital service by way of CSU/DSU. An SW56 CSU/DSU, however, includes a dialing pad from which you enter the phone number of the remote host. SW56 lets you 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 phone 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 a SW56 CSU/DSU over V.35 or RS 449 serial interface with synchronous protocol at rates up to 56Kbps. With a V.25bis call/answer unit, data and call control flow over a single serial interface.

ISDN

Like Switched-56, ISDN also provides switched end-to-end digital connectivity. Unlike other services, however, 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 64Kbps 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 128Kbps. In some areas, the phone company may limit each B channel to either 56Kbps or 112Kbps combined. There is also a physical constraint in that the customer location must be within 18,000 feet 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 RS232 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 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. New technology also enables a terminal adapter to operate as the digital server side for 56K(X2/56Flex) clients.

Typically, you would like to connect to an ISDN terminal adapter over an RS232 serial interface using asynchronous protocol at rates up to 230.4Kbps. However, the maximum iSeries server baud rate for asynchronous over RS232 is 115.2Kbps. Unfortunately, this restricts the maximum byte transfer rate to 11.5k bytes/sec, while the terminal adapter with multi-linking is capable of 14/16k bytes uncompressed. Some terminal adapters support synchronous over RS232 at 128Kbps, but iSeries server maximum baud rate for synchronous over RS232 is 64Kbps.

The iSeries server is capable of running asynchronous over V.35 at rates up to 230.4Kbps, but terminal adapter manufacturers generally do not offer such a configuration. Interface converters that convert RS232 to V.35 interface could be a reasonable solution for the problem, but this approach has not been evaluated for the iSeries server. Another possibility is to use terminal adapters with V.35 interface synchronous protocol at rate of 128Kbps. Although this class of terminal adapters exists, it does not appear that many offer synchronous Multilink PPP.

T1/E1 and fractional T1

T1/E1

A T1 connection bundles together twenty-four 64Kbps (DS0) time division multiplexed (TDM) channels over 4-wire copper circuit. This creates a total bandwidth of 1.544Mbps. An E1 circuit in Europe and other parts of the world bundles together thirty-two 64Kbps channels for a total of 2.048Mbps. TDM allows multiple users to share a digital transmission medium by using pre-allocated time slots. Many digital 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 may 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 CSU/DSU device can be used. Typically, you can connect to a T1/E1 CSU/DSU or multiplexer over V.35 or RS 449 serial interface with synchronous protocol at rates at a multiple of 64Kbps to 1.544Mbps or 2.048Mbps. The CSU/DSU or multiplexer provides the clocking in the network.

Fractional T1

With Fractional T1 (FT1), a customer can lease any 64Kbps sub-multiple of a T1 line. FT1 is useful whenever the cost of dedicated T1 would be prohibitive for the actual bandwidth 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 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 V.35 or RS 449 serial interface with synchronous protocol at some multiple of 64Kbps. With FT1, you are pre-allocated 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 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 T-1 (1.544 Mbps) and T-3 (45 Mbps) speeds. You can think of Frame Relay as a way of utilizing existing T-1 and T-3 lines owned by a service provider. Most telephone companies now provide Frame Relay service for customers who want connections at 56 Kbps to T-1 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 ATM.

L2TP (tunneling) support for PPP connections

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol that extends 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). Using 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, this is why L2TP is also refered to as Virtual PPP. The L2TP protocol is documented as a Request For Comment standard RFC2661. More information about RFCs can be found at http://www.rfc-editor.org A L2TP tunnel can extend across a entire PPP session or only across one segment of a two segment session. This can be represented by four different tunneling models:

- Voluntary tunnel
- Compulsory tunnel-incomming call
- Compulsory tunnel-remote dial
- L2TP Multi-hop Connection.

Voluntary tunnel

In the voluntary tunnel model, a tunnel is created by the user, typically by the use of a L2TP enabled client. As a result, the user will send L2TP packets to the Internet Service Provider (ISP) which will forward them on to the LNS. In voluntary tunneling the ISP does not need to support L2TP, and the L2TP tunnel initiator effectively resides on the same system as the remote client. In this model the tunnel extends across the entire 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 will send PPP packets to the ISP (LAC) which will encapsulate them in L2TP and tunnel them to the LNS. In the compulsory tunneling cases, the ISP must be L2TP capable. In this model the tunnel only extends 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 (LNS) initiates a tunnel to an ISP (LAC) and instructs the ISP to place a local call to the PPP answer client. This model is intended for cases where the remote PPP Answer Client has a permanent established phone 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

An L2TP Multi-hop connection is a way of redirecting L2TP traffic on behalf of client LACs and LNSs. A Multi-hop connection is established using a 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 will act as both a LNS to a set of LACs at the same time as acting as a 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

DSL refers to a class of technology used to obtain more bandwidth over existing copper telephone cabling running between a customer's premises and an ISP provider. It 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 kbit/s) 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 Megabits per second are achievable in some areas - 30 or more times faster than today's fastest modems. PPPoE stands for Point to Point Protocol over Ethernet. PPP is usually used over serial communications like dial-up modem connections. Many DSL Internet service providers now use PPP over Ethernet because of its added login and security features. What is a DSL modem? A DSL ″modem″ is a device that is placed at either end of the copper phone line to allow a computer (or LAN) to be connected to the Internet through a DSL connection. Unlike a dial up connection, it usually does not require a dedicated phone line (a POTS splitter box enables the line to be shared simultaneously). DSL is considered to be the next generation of modem technology. Although DSL modems resemble conventional analogue modems they provide much higher throughput.

Connection Equipment

These are the three kinds of communication equipment that you can use with your PPP environment.

- Modems
- CSU/DSU
- ISDN terminal adapters
- Type 2838 Ethernet adapters (for PPPoE connections).
-

Modems

Both external and internal modems can be used for 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 phone 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 then the modem strings are already defined for their use.

The iSeries server has many modem models predefined, but new models can be defined through Operations 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 shipped 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 (ECS) modem that is shipped with the iSeries server to establish PPP connections. On older systems, the ECS modem was an IBM 7852-400 external modem. On newer systems, the 2771 or 2772 Internal modems may be used as the ECS modem.

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.

ISDN terminal adapters

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.

Verify that your terminal adapter is rated for use on the iSeries server:

- ISDN terminal adapter recommendations list the best terminal adapter to use.
- ISDN terminal adapters restrictions provides information and brief evaluations on various ISDN terminal adapters that have been tested with iSeries server.

Follow these steps to configure your terminal adapter:

1. In iSeries Navigator, select your server 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.

Review the example Configuring an ISDN terminal adapter for sample procedures that use Operations Navigator.

ISDN terminal adapter recommendations

The recommended external 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 iSeries server. 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 iSeries server.** 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 iSeries server. PAP responses do not appear on the ISDN connection.
- **Connections that the iSeries server answers.** The Courier I requires CHAP authentication by the calling side if the iSeries server answer configuration causes the iSeries server to open authentication with a CHAP challenge. If the iSeries server 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 iSeries server 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 , though some may still be from third party suppliers. The RS-232 version is still recommended at somewhat reduced performance on iSeries, since RS-232 connections are limited to 115.2 Kb.

You can also obtain a V.35 to RS-232 adapter from Black Box Corporation. The part number is FA-058.

Be sure to set the V.35 line speed on iSeries server for 230.4 Kbps.

ISDN terminal adapter restrictions

The following terminal adapters have been evaluated. They are recommended only for the origination of ISDN remote connections from the iSeries server.

3Com Impact IQ ISDN:

This terminal adapter is not recommended for iSeries server for the following reasons:

- The terminal adapter does not support V.34 analog modem connections. However, it may 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 may not connect to iSeries server at speeds greater than 115200 bps.
- The terminal adapter does not automatically support Challenge Handshake Authentication Protocol (CHAP). However, setting S84=0 allows the iSeries server CHAP authentication to be performed.
- The iSeries server is unable to determine when the connection ends when monitoring the Data Set Ready signal from the terminal adapter. This results in a potential system security exposure.

Motorola BitSurfr Pro ISDN:

This terminal adapter is not recommended for iSeries server for the following reasons:

- The terminal adapter does not support V.34 analog modem connections. However, it may 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 may not connect to iSeries server at speeds greater than 115200 bps.
- The terminal adapter does not automatically support CHAP authentication. However, setting @M2=C allows iSeries server 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 iSeries server hardware flow control mechanism does not work well with this terminal adapter. This results in degraded performance when the iSeries server is sending data on a Multilink PPP connection.

IP address handling

PPP connections allow several different sets of options for managing IP addresses depending on the type of connection profile which allows the IP address management for the PPP connection to work seamlessly with your existing network architecture. For information about defining an IP address scheme for your network, refer to the following topics:

- DHCP

  DHCP can centrally manage IP address assignments for your network. Learn how to setup and manage DHCP services for your network.
- DNS

  DNS can help you manage host names and their associated IP addresses. Learn how to setup and manage DNS services for your network.
- BOOTP

  BOOTP is used to associate client workstations with your iSeries server, and assign them IP addresses. Learn how to setup and manage BOOTP services for your network.
- IP packet filtering

  Restrict users and groups access to specific IP addresses by creating an IP filter rules file. Learn about IP filtering support, and how to implement this option on your network.

You should be familiar with your network IP address management strategy before configuring a PPP connection profile. This strategy will impact many of the decisions throughout the configuration process including your authentication strategy, security consideration 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 allows 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 then you will have to be sure that the remote system is defined to accept the addresses you have defined. One typical application is to define your local 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 addresses with each other as a way to learn the address of the remote system. This could be useful for one office calling another office for temporary connectivity.

Another consideration is if you want to enable IP Address Masquerading. For example, if the iSeries server connects to the internet via an ISP then this could allow an attached network behind the iSeries server to also access the internet. Basically the iSeries server will 'hide' 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 iSeries server. There are also additional routing considerations for the both the systems on the LAN (to ensure their internet traffic is sent to the iSeries server.) as well as the iSeries server where you will 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 iSeries server. This will become the address that will identify the iSeries server 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 previously existing local IP addresses are present then 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 may 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 address range for LAN attached systems, and verify that IP forwarding has been enabled for both this connection profile and the iSeries system.

Table 3. 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 an unique 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 allow additional routes to be defined for each of these user IDs so 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 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 address assignment methods of Fixed IP address and Address Pool. When a remote user connects to the iSeries server a search will be made to determine if a remote IP address is defined specifically for this user. If it is then that address, mask and set of possible routes will be used for the connection. If the user is not defined then the 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 address then 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.

Table 3. IP address assignment options for receiver profile connections (continued)

Option	Description
IP address routing	The dial-up client and the iSeries must have IP address routing properly configured if the client needs access to any IP addresses on the LAN to which the iSeries belongs.

IP packet filtering

IP Packet Filtering is the mechanism that can limit the services to an individual user when logged into a network. Packet Filtering can ″Permit″ or ″Deny″ access based on destination IP addresses and/or ports. 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 would 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. See the IP Packet Rules Information Center topic for more information.

For L2TP connections, VPN with IP SEc filtering must be used to protect network traffic. See the VPN Information Center topic for more information.

System authentication

PPP connections with an iSeries server support several options for authenticating both remote clients dialing in to the iSeries, and connections to an ISP or other server the iSeries is dialing. The iSeries supports several methods for maintaining authentication information, ranging from simple validation lists on the iSeries that contain lists of authorized users and associated passwords, to support for RADIUS servers that maintain detailed authentication information for your network users. The iSeries also supports several options for encrypting user ID and password information, ranging from a simple password exchange to maceration support with CHAP-MD5. You can specify your preferences for system authentication, including a user ID and password used to validate the iSeries when dialing out, on the **Authentication** tab of the connection profile in iSeries Navigator.

For more information about maintaining validation and authentication information, refer to:

- Remote Authentication Dial In User Service (RADIUS)
- Validation list

For more information about supported password authentication protocols, refer to:

- Challenge Handshake Authentication Protocol (CHAP-MD5)
- Password Authentication Protocol (PAP)
- Extensible Authentication Protocol (EAP)

CHAP-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 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.

EAP

Extensible Authentication Protocol (EAP) allows 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 RAS authentication with third-party security devices. EAP protects secure VPNs from hackers that use dictionary attacks and password guessing. EAP improves on PAP and CHAP.

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

The iSeries server currently only supports a version of EAP that is basically equivalent to CHAP-MD5. You can however use remote authentication using a RADIUS server that may support some of the additional authentication schemes described above.

PAP

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 remove 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 CHAP whenever possible.

RADIUS overview

Remote Authentication Dial In User Service (RADIUS) is an Internet standard protocol which 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 iSeries Server, 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 returns all configuration information necessary, to the NAS, so that the NAS (iSeries Server) can deliver authorized services to the authenticated dial-in user.

If a RADIUS server cannot be reached, the iSeries server 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 being supported. This could be UNIX password files, Kerberos, a commercially security system or even a custom-developed security system.The RADIUS server sends back to the iSeries server any services 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. For an example RADIUS configuration, refer to the Authenticating dial up users with a RADIUS server scenario.

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 may be **encrypted - CHAP-MD5/EAP** or **unencrypted - PAP**.

Refer to the online help for more information.

Bandwidth considerations - Multilink

Often additional bandwidth is required to complete certain tasks but is not required all of the time. In these cases the purchase of specialized hardware and expensive communication lines may 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 phone lines. You may include up to Six links in a 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 RFC1990. More information about RFCs can be found at http://www.rfc-editor.org.

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 a MP bundle. Links may then 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 a MP bundle. RFC2125 documents both the PPP Bandwidth Allocation Protocol (BAP) and Bandwidth Allocation Control Protocol (BACP).

Chapter 6. Configure PPP

Before you can use PPP to set up a point-to-point connection, you must first configure your PPP environment. These sections provide configuration information for PPP environments:

- Creating a connection profile
- Configure your modem
- Configure a remote PC
- Configure Internet access through the AT&T Global Network
- Connection wizards
- Configure a group access policy
- Apply IP packet filtering rules for a PPP connection
- Enable RADIUS and DHCP services for PPP receiver connection profiles

Creating a connection profile

The first step in configuring a PPP connection between systems is to create a connection profile on the iSeries server. The connection profile is the logical representation of the following connection details:

- Line and profile type
- Multilink settings
- Remote phone 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** are outbound point-to-point connections that originate from the iSeries server (local system). These are PPP connections that a remote system receives.
- **Receiver Connection Profiles** are inbound point-to-point connections that originate from a remote system. These are PPP connections that the iSeries server (local system) receives.
- **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 iSeries server as a server that initiates connections.
   - Right-click **Receiver Connection Profiles** to set the iSeries server as a server that allows 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. Refer to the online help for specific information.

Protocol type: PPP or SLIP

Which protocol type should you choose to make a point-to-point connection?

PPP is a standard Internet connection. PPP allows interoperability among the remote access software of different manufacturers. PPP also allows multiple network communication protocols to use the same physical communication line.

PPP replaces SLIP as the protocol of choice for point-to-point connections. The SLIP Request for Comment (RFC) never became 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 is still supported on the iSeries server. However, IBM recommends 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 PPP connection profile include selections for the **connection type** and the **operating mode**. Your mode selections specify how your server 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
   - L2TP (virtual line)
   - 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

Select this connection type if you are using any of the following to connect over a telephone line:

- Modem (internal or external)
- Internal ISDN Basic Rate Interface adapter
- External ISDN terminal adapter

The switched line connection type has the following operating modes:

- **Answer**

  Choose this operating mode type to enable a remote system to dial into the iSeries server.
- **Dial**

  Choose this operating mode to enable the iSeries server to dial out to a remote system.
- **Dial on-demand (dial only)**

Choose this operating mode to enable the iSeries server to automatically dial out to a remote system when TCP/IP traffic 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 iSeries server to answer calls from a dedicated remote system. This operating mode also allows the iSeries server to call the remote system when TCP/IP traffic for the remote system is detected. If both systems are iSeries servers and if both 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 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

Select this connection type if you have a dedicated line between the local iSeries server and the remote system. If you have a leased line, you do not need a modem or an 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 iSeries server through a dedicated line. This operating mode refers to a leased line answer profile.
- **Initiator**

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

L2TP (virtual line)

Select this connection type to provide a connection between systems that use Layer Two Tunneling Protocol (L2TP).

Once an L2TP tunnel is established, a virtual PPP connection is made between your iSeries server 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 iSeries server over an L2TP tunnel.
- **Initiator**

  Choose this operating mode to enable the iSeries server to connect to a remote system over an L2TP tunnel.
- **Remote dial**

  Choose this operating mode to enable the iSeries server to connect to an ISP over a L2TP tunnel, and direct the ISP to dial a remote PPP client.
- **Multi-hop initiator**

Choose this operating mode to enable the iSeries server 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.

Layer 2 Tunneling Protocol (L2TP): L2TP extends PPP to support a link layer tunnel between a requesting L2TP client and the target L2TP server endpoint. By using L2TP tunnels, it is possible to separate the location where the dial-up protocol ends from the location where access to the network is provided.

An Internet Service Provider (ISP) uses the virtual line mode to operate Virtual Private Networks (VPN). See Configuring an L2TP connection protected by VPN for a better understanding of how VPN works with L2TP.

These illustrate three different tunneling implementations of L2TP:

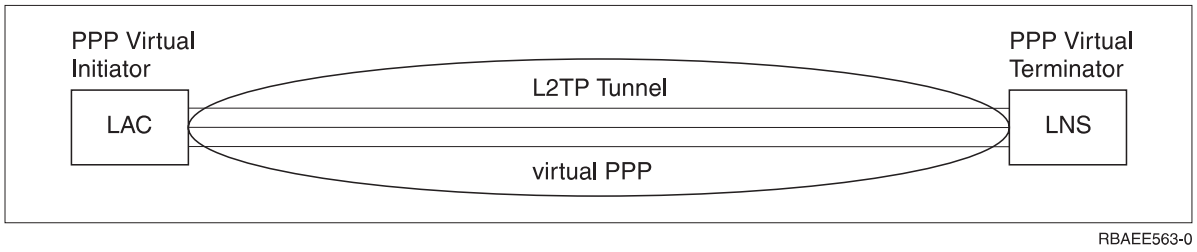

Figure 7. PPP Virtual Initiator or PPP Virtual Terminator

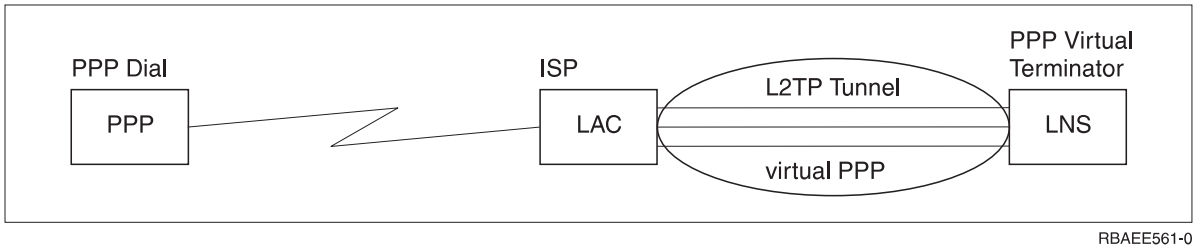

Figure 8. PPP Dial Initiator or PPP Virtual Terminator

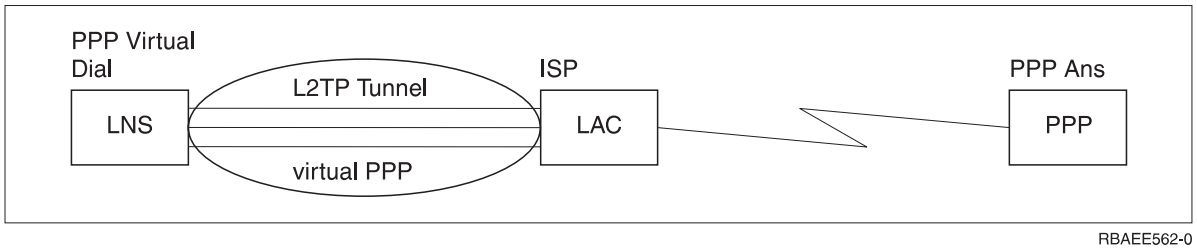

Figure 9. PPP Virtual Dial or PPP Virtual Answer

PPPoE line

PPPoE connections use a virtual line to send PPP data through a type 2838 Ethernet adapter to a DSL modem provided by your ISP that is also connected to the Ethernet-based LAN. This allows high speed internet access for LAN users via PPP sessions through the iSeries server. Once the connection between the iSeries 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, and imply an Initiator operating mode and use only a single line.

Link configuration

Link configuration defines the type of line service that your PPP connection profile uses to establish a connection. The types of line service depend on the connection type that you specify.

- Single line
- Line pool
- Integrated ISDN line

Single line

Select this line service to define a PPP line that is associated with an analog modem. This option is also used for leased lines where a modem is not required. The PPP connection profile always uses the same iSeries server communications port resource.

An analog single line, if desired, 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 it 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. Once 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 than be established. Once 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 on 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

Select this line service to set the PPP connection to use a line from a line pool. When the PPP connection starts, the iSeries server selects an unused line from the line pool. For dial on-demand profiles, the server 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 were 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 iSeries server 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 would 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.

Multiple-connection profile support

Point-to-point connection profiles that support multiple connections allow 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 iSeries server 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 are for use from one adapter, or the 2750 and 2751 adapters, which support eight separate ISDN B-channel connections.

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 iSeries server. You can use the Local IP address pull down list to select the existing address. Remote users can access the resources that are on your local network if you choose the local iSeries server 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 iSeries server IP address or do not want the remote users to access the LAN, you must define a virtual IP address for your iSeries server. 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. Since this address is not tied to a physical network, it will not automatically forward traffic to other networks that are attached to your iSeries server.

To create a Virtual IP address, follow these steps:

1. In iSeries Navigator, expand your server, 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 address with your profile.

   Note: The Virtual IP address must be active prior to starting your multiple-connection profile; otherwise, the profile will not start. To activate the address after creating the interface, you select the option to start the 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. Since 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.

Remote IP address pools: The system can use remote IP address pools for any answering or terminating point-to-point connection profile that is used with multiple incoming connections. This includes L2TP, native ISDN, and line pools with a maximum number of connections greater than one. This function allows 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 address is already in use, the next IP address within the Number of addresses range is given out. For example, assume that the Starting IP address is 10.1.1.1 and the Number of addresses is defined as 5. The 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, once all the addresses in the pool are used, any subsequent connection request is refused until another connection ends and frees up an address.
- To allocate specific addresses to some remote systems while allowing other incoming systems to use an 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 connects, the iSeries server 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 address from the remote IP address pool is returned.

ISDN

Select this line service to define a PPP line that is associated with an ISDN network connection.

Advantages of using ISDN:

- ISDN provides clear communication at faster speeds.
- ISDN aims to provide universal connectivity by using a single interface and a high-speed digital network to transport all types of data.
- ISDN also has the capability of fast connection times for switched connections. Analog modem connections can take up to 30 seconds or more to establish, while an ISDN connection takes only a few seconds.

Configure your modem for PPP

For your analog PPP connections, you can use an external modem, an internal modem or an ISDN terminal adapter. A modem provides you with analog connection capabilities (leased and switched lines). Modem descriptions for the most popular modems have been defined for the iSeries server.

You can complete these modem configuration tasks:

- Configure a new modem
- Associate a modem with a line description
- Set modem command strings

Configure a new modem

1. In iSeries Navigator, select your server, 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.

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

1. In iSeries Navigator, select your server, 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.

To create a modem description, follow these steps:

1. In Operations Navigator, select your server, 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.

Set modem command strings

The table below lists a minimum set of command strings that are used by the modems that are defined on the iSeries server. You can find the equivalent command string in the user manual for your modem. Use the manufacturer's recommended setting in the modem description.

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
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: Configure an ISDN terminal adapter

1. In Operations Navigator, select your server, 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 iSeries server may perform

   Consequently, these commands should include and be limited to the following:

   - 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 may 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 iSeries server 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 phone 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 may 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.

Associate a modem with a line description

1. In iSeries Navigator, select your server, 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 on 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 dialog box.
4. From New Line Properties dialog box, 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, refer to the online help.

For V5R2, 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 dialog. You can configure PPP lines from the Connection tab of Receiver and Originator connection profiles.

Configure a remote PC

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

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

- Type of dial-up connection should be **PPP**.
- If you are using encrypted passwords, ensure that you use MD-5 CHAP (MS-CHAP is NOT supported by the iSeries server). 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, PAP is automatically used. Any other unsecured protocol type will not be supported by the iSeries server.
- Typically, IP addressing is defined by the remote system, or in this case, the iSeries server. If you intend to use alternate IP addressing methods (such as defining your own IP addresses), ensure that the iSeries server is also configured to accept your addressing method.
- Add DNS IP address if appropriate for your environment.

Configure Internet access through the AT&T Global Network

IBM provides internet access through its AT&T Global Network. 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 may cancel the wizard at any time and no existing data is saved.

Two types of applications can use the AT&T Global Network connection:
- **Mail Exchange**: Allows you to periodically retrieve mail from a single AT&T Global Network account and send it to your iSeries server for distribution to your Lotus Mail users or 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 the 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)
- 2761: Eight-port analog modem IOA
- 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 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 server, 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

New Dial Connection Wizard

This wizard guides you through the steps to configure a dial-up connection profile to access your Internet Service Provider (ISP) or Intranet. You may need to get some information from your network administrator or Internet Service Provider (ISP) to complete the wizard. For more information on completing this wizard, refer to the online help.

Universal Connection Wizard

This wizard selection guides you through 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 iSeries server system environment to supply you with recommendations of personalized fixes for your system and situation. For more information on completing this wizard, refer to the online help.

Configure 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:

1. In Operations Navigator, select your server, 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 links per bundle can be between 1 and 16. Since 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 can not 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:
   - Allow remote system to access other networks (IP forwarding)

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

     There may be security reasons why you would not want to allow IP forwarding. In contrast, an Internet Service Provider (ISP) generally always provides IP forwarding. Note that this will only take effect if system wide IP datagram forwarding is enabled, otherwise it will be ignored even if marked. System-wide IP datagram forwarding can be displayed from the Settings tab on the TCP/IP Properties page.
   - Request TCP/IP header compression (VJ)

     This option specifies whether you want Internet Protocol (IP) to compress header information after it establishes a connection. Compressing usually 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 iSeries server 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 let you control what IP traffic you allow in your network. You can use this IP packet filtering component to

protect your system. The IP packet filtering component protects your system by filtering packets according to rules that you specify. The rules are based on packet header information.

For more information on IP Packet rules, see the IP Packet Filtering and NAT topic on the Information Center.

For an example, refer to Managing users access to resources using Group Access Policies and IP Filtering.

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:

1. Click the **Authentication** page.
2. Check **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 pulldown 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 dialog box, complete the following:
   - Select the authentication protocol for which the user name is defined.
   - Enter the user name and password.

     Note: For security purposes, it is recommended that you do not use the same password for a user defined for Challenge Handshake Authentication Protocol22314 (CHAP), Extensible Authentication Protocol (EAP), and Password Authentication Protocol (PAP).
   - Check **Apply a group policy to the user**, select a group policy from the pulldown list, and click **Open**.

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

Apply IP packet filtering rules to a PPP connection

The IP Packet Filtering and NAT Rules topic in the Information Center discusses how to create IP packet rules that you can reference for a PPP connection profile. You can use a packet rules file to restrict a user a groups access to IP addresses on your network. For an example of using a filter rules file with a PPP connection, see the Scenario: Manage remote user access to resources using group policies and IP filtering.

You can reference 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 pulldown 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 pulldown list.
4. Click **OK** to apply the PPP filter.

Enable RADIUS and DHCP services for connection profiles

To enable RADIUS and DHCP services for PPP receiver connection profiles:

1. In Operations Navigator, select your server, 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 may also wish to 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.

For an example RADIUS configuration, refer to the Authenticating dial up users with a RADIUS server scenario.

Chapter 7. Manage PPP

These are the PPP management tasks that you can do on the iSeries server:

- Set properties for connection profiles
- Monitor PPP activity

Set 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 dialog box. After you enter your selections on this dialog box, the connection profile property sheet appears. The selections that you specify on the Point-to-Point Connection Profile Setup dialog box 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** dialog box. 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 appears on the dialog box. You can also refer to the PPP examples and procedures for more information.

Monitor PPP activity

This page explains how to view a connection profile and a session log by using Operations 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 jobs run under the QTCP user profile and are used to handle each individual PPP connection. These jobs run in the QUSRWRK subsystem by default, but can be configured to run in other subsystems. Two PPP connection job names are used:
  - QTPPPSSN - This job is used to handle all non-L2TP PPP connections.
  - QTPPPL2SSN - This job is used to handle virtual PPP data after the QTPPPL2TP jobs successfully negotiates an L2TP tunnel.
- 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 server, 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:
   - **Jobs** opens the job log for QTPP*xxx* jobs.
   - **Connections** opens a dialog box 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 or connection details for each connection is avialable.
   - **Properties** opens the Property pages to display current properties for a connection.

Viewing connection information:

1. In iSeries Navigator, expand your server, 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 will be 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, Local and Remote IP addresses and name of the PPP job may be shown depending on the status of each PPP job.
3. To view job output or details for a connection, right-click a connection and the buttons will be enabled.
4. To view job output, click **Jobs**. From the job log, right-click the job name, and select **Printer output**. The contents of the connection session logs and job logs (for ended sessions) can then be displayed.
5. To view connection details click **Details**. Details can only be displayed for currently active connections. The details dialog will allow you to see additional connection information for this particular connection.

Working with PPP Output from the iSeries server:

To work with PPP output type WRKTCPPTP at the iSeries server 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. The 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 dialog.

Primary status description	**Explanation**
Waiting for connection requests	Receiver profile is ready for a connection
Waiting for incoming call	Server 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 succesfully connected

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 succesfully 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 sucessfully complete
L2TP call established	L2TP tunnel up message

Chapter 8. Troubleshoot PPP

Current and relevant information on program temporary fixes (PTFs) and troubleshooting is documented on the iSeries server TCP/IP home page . This link provides the latest information that supplements and overrides the information that is contained in this topic.

If you experience PPP connection problems, you can use this checklist to gather error information. This checklist can help you identify error symptoms and resolve PPP connection problems.

1. Required supporting material:
   - Remote host type, operating system, and level
   - iSeries server host operating system level
   - Job log of failing session and connection dialog file

     In V5R1, joblogs and connection dialog output are saved in an OUTQ with the same name as the profile.
   - Connection script if 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 TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190) extensively covers the following PPP problems. It also provides detailed problem resolution information.

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 Operations 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.

Problem	Solution
PPP protocol Connection errors can occur due to misconfiguration of the PPP protocol.	Investigating the lower-levels of the PPP protocol may 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.

Chapter 9. Other information about PPP

Other sources of information on PPP:

- Find the latest program temporary fixes (PTFs), and the latest configuration information for PPP and L2TP through the PPP link on the iSeries server TCP/IP home page  . This link provides the latest information that supplements and overrides the information that is contained in the **Remote Access Services: PPP Connections** topic.
- The ITSO Redbook TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  extensively covers TCP/IP services and applications.

IBM Confidential
Printed in U.S.A.