



IBM Systems - iSeries
Networking
Network Scenarios

Version 5 Release 4





IBM Systems - iSeries
Networking
Network Scenarios

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in “Notices,” on page 39.

Third Edition (February 2006)

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

© Copyright International Business Machines Corporation 2004, 2006. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Network scenarios	1
Printable PDFs.	1
Network planning work sheet	2
Scenario: Set up iSeries to communicate with LAN	3
Review planning work sheet	4
Install the TCP/IP Connectivity and Utilities licensed program	5
Configure TCP/IP	6
Test TCP/IP	7
Install and configure iSeries Access for Windows on your workstation.	7
Configure printers on the LAN	7
Test network connections	9
Secure your iSeries server	9
Implement system security recommendations	10
Explore TCP/IP services, applications, and protocols	11
Scenario: Enable remote connections	11
Set up Certificate Authority with Digital Certificate Manager.	14
Configure VPN connection between the branch sales office and the corporate office	19
Configure VPN connection to remote users.	22
Scenario: Create a virtual Ethernet for interpartition communications	28

Enable the logical partitions to participate in a virtual Ethernet	29
Create the Ethernet line descriptions	29
Turn on IP datagram forwarding	30
Create the interface to enable proxy ARP	30
Create the virtual Ethernet interface on partition A.	31
Create the virtual Ethernet interface on partition B.	31
Create the virtual Ethernet interface on partition C.	31
Create the virtual Ethernet interface on partition D.	32
Create the routes	32
Verify network communications	32
Scenario: Share a modem between logical partitions using L2TP	32
Scenario details: Share a modem between logical partitions using L2TP	34

Appendix. Notices	39
Programming Interface Information	40
Trademarks	41
Terms and conditions	41

Network scenarios

The subject of networking encompasses an enormous amount of information. The purpose of this topic is not to provide basic networking information, but instead to provide examples of iSeries™ technology used in specific networking environments. The following scenarios are intended to demonstrate how to take advantage of networking services and applications available on your iSeries server.

Printable PDFs

Use this to view and print PDFs of this information.

To view or download the PDF version of this document, select Network scenarios (about 585 KB).

You can view or download these related topics:

- TCP/IP setup (about 666 KB) contains the following topics:
 - Internet Protocol version 6 (IPv6)
 - Plan TCP/IP setup
 - Install TCP/IP
 - Configure TCP/IP
 - Customize TCP/IP
 - TCP/IP techniques over virtual Ethernet
- Remote access services (about 1059 KB) contains the following topics:
 - PPP scenarios
 - PPP concepts
 - Plan PPP
 - Configure PPP
 - Manage PPP
 - Troubleshoot PPP
- Virtual private networking (about 1113 KB) contains the following topics:
 - VPN scenarios
 - VPN concepts
 - Plan VPN
 - Configure VPN
 - Manage VPN
 - Troubleshoot VPN
- TCP/IP troubleshooting (921 KB) contains the following topics:
 - Interactive troubleshooter
 - Troubleshooting tools and techniques
 - Troubleshooting problems related to specific applications


Saving PDF files

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

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

4. Click Save.

Downloading Adobe Reader

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

Network planning work sheet

Read this work sheet to learn basic networking considerations.

Use this work sheet as a supplement to your network planning research. Each scenario includes similar tables with prerequisites and assumptions made about the network environment. The following tables do not cover a complete network design for every environment, but provide you a basis to start thinking about your own environment. For example, before coming to these scenarios, you need to plan for server availability, performance, capability, and more.

Server work sheet	Company answer
Record server model.	
Record operating system version.	
Understand and document the logical partitioning environment.	
Determine client needed to connect to the iSeries server.	
Record the type of communication adapter installed. See Network communications for more information on Ethernet, token ring and others.	
Record the communication resource name.	
Record the IP address for the iSeries server.	
Record the subnet mask for the iSeries server.	
Record the gateway address.	
Record the host name and domain name.	
Record the IP address for the domain name server.	

Network work sheet	Company answer
Establish clear network goals.	
Who are the users and what are their requirements?	
What applications support those requirements?	
What performance is expected from those applications?	
What protocol is required? Keep interoperability in mind. Most networks use TCP/IP; however, there are other alternatives. See Network communications for more information.	
Do some applications require higher priority than others?	
Are the applications sensitive to delay or packet loss?	
What applications have specific security needs? Security planning should be integrated with network planning. See the eServer™ security planner for a resource on planning network security.	
Will this network grow in the future and how quickly? Make sure to consider security in your basic network architecture.	
What technologies should be used for the LAN?	
What other devices will be connected to the network?	

Network work sheet	Company answer
Draw a picture of your network.	

Related reference

“Review planning work sheet” on page 4

Scenario: Set up iSeries to communicate with LAN

As a network administrator, you would like to add a new iSeries server to your local area network (LAN). This scenario provides a network administrator with prerequisite information as well as instructions on how to set up your iSeries server to communicate with the LAN.

Situation

You are the network administrator for a small wholesale company, Sampson Organic Produce. Your customers include area grocery stores and individual families who want organically grown, high-quality produce. Your business has been growing and you have recently purchased a new iSeries server to help manage your inventory more efficiently. In the past, resources and key business applications were stored on individual workstations. As your business changed, it became apparent that data from these applications needed to be shared more easily. For example, employees who took telephone orders need a quicker way to check stock to determine product availability. In the past, they made customers wait while checking with an employee who had access to the in-stock database.

You plan to consolidate all of these key business applications on the new server. You have already completed all the required hardware planning and setup tasks for your new server. You have researched communication and networking and have decided to create an Ethernet local area network (LAN).

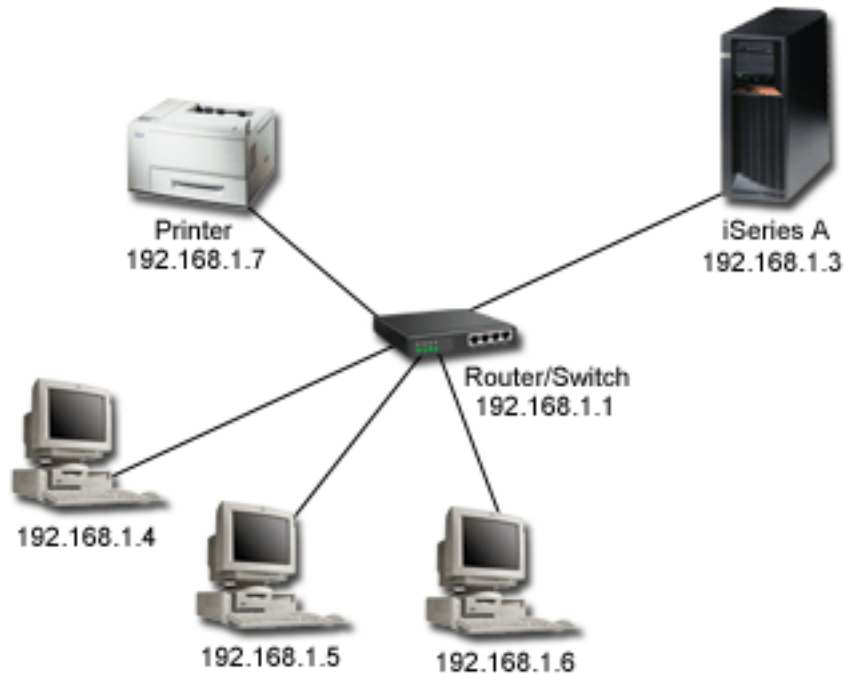
Objectives

After you add your server to the LAN, you would like to have met the following objectives:

- To set up the iSeries to communicate with the LAN.
- To set up a printer for the LAN.
- To ensure that the data stored on the server is protected.
- To locate TCP/IP services to communicate with other hosts.

Details

The following figure shows an iSeries server connected to a router. Three workstations and a printer are also connected to the router depicting the network for a small, fictional company called Sampson Organic Produce.



- iSeries A runs on OS/400® Version 5 Release 2 (V5R2) and contains all pertinent business applications.
- iSeries A has the IP address 192.168.1.3.
- iSeries A has the subnet mask of 255.255.255.128.
- Workstation 1 has the IP address of 192.168.1.4.
- Workstation 2 has the IP address of 192.168.1.5.
- Workstation 3 has the IP address of 192.168.1.6.
- The printer has the IP address of 192.168.1.7.
- The router in the network has the IP address of 192.168.1.1.

Tip: When no external network connection is planned, a hub can be used in place of a router or switch.

Prerequisites and assumptions

This scenario assumes the following prerequisites have been met in this network environment:


- All cabling and hardware setup has been completed for the network.
- If you use a router, the router has been configured. Configuration is not applicable to hubs or switches.

Configuration steps

Complete the following tasks. After each step, there is a link to the next task.

Review planning work sheet

After thorough planning, the network administrator answered the following questions, which directly affect the tasks presented in this scenario. For a blank table (to create your own work sheet), review the “Network planning work sheet” on page 2.

Server work sheet	Company answer
Record the server size.	Model 820
Record the operating system or systems.	i5/OS™
Understand and document the current logical partitioning environment.	No logical partitions
Determine client needed to connect to your iSeries.	IBM®  ® iSeries Access for Windows® which includes iSeries Navigator.
Record the type of communication adapter installed.	Ethernet
Record the communication resource name.	cmn01
Record the IP address for your iSeries server.	192.168.1.3
Record the subnet mask for your iSeries server.	255.255.255.128
Record the gateway address.	192.168.1.1
Record the host name and domain name.	iseriesa.sampson.com
Record the IP address for domain name server.	DNS is not needed because the LAN is not connected to another network. The company adds host table entries for all systems on the network.

Network assumptions	Company decisions
Who are the users and what are their requirements?	3 areas taking customer orders.
What applications support those requirements?	An in-house ordering application that is not web-based.
What protocol is required? Keep interoperability in mind.	TCP/IP
Are your applications sensitive to delay or packet loss?	No
Do your applications need specific security considerations?	Basic system security. Details are integrated into the scenario.
Will this network grow in the future and how quickly? Make sure to consider security in your basic network architecture.	Yes. Not sure.
What other devices will be connected to your network?	Printer—IBM Infoprint® 40
Draw a picture of your network.	See scenario diagram.

Related concepts

“Network planning work sheet” on page 2

Read this work sheet to learn basic networking considerations.

Install the TCP/IP Connectivity and Utilities licensed program

1. Insert your installation media for TCP/IP into your server. The server uses a CD-ROM device as the installation media.
2. At the command line, type G0 LICPGM and press Enter to access the Work with Licensed Programs display.

3. Select option 11 (Install licensed programs) on the Work with Licensed Programs display to see a list of licensed programs and optional features of licensed programs.
4. Type 1 (Install) in the Option column next to 57xxTC1 (TCP/IP Connectivity Utilities for iSeries), 57xxCM1 (Communications Utilities), and 57xxXE1 (iSeries Access for Windows). Press Enter. The Confirm Licensed Programs to Install display shows the licensed programs you select to install.
5. Press Enter to confirm.
6. The network administrator enters the following choices on the Install Options display:
 - Installation device: QOPT (This is for installing from a CD-ROM device.)
 - Objects to install: Both programs and language objects.
 - Automatic Restart: Yes (determines whether the system will automatically restart after the installation has completed successfully.)

When TCP/IP Connectivity Utilities is successfully installed, either the Work with Licensed Programs menu or the Sign On display appears.

7. Select option 50 (Display log for messages) to verify that you have installed the licensed program successfully.

Configure TCP/IP

1. At a command line, type WRKHDWRSC *CMN to display the Work with Communication Resources menu.
2. Type 5 beside the communication resource for the Ethernet port and press Enter.
3. On the Work with Communication Descriptions menu, type 1 and press Enter.
4. The Create Line Description (Ethernet) (CRTLINETH) menu appears.
5. In the **Line Description** field, enter a description for the line. In this example, the network administrator chose Eth01.
6. Enter the information for the **Line speed** and **Duplex** fields. Ensure these values match the port on the switch connecting to the iSeries. In this example, 100M and *HALF are used. Press Enter.
7. Press F10 to view additional parameters. You might have to press Page Down to view them.
8. Change the Link speed field to match the Line Speed you entered previously (In this example, 100M).
9. Accept all other default values and press Enter.
10. Press F3 to return to the Work with Communication Resources menu.
11. Press F3 again to return to the Command entry menu.
12. At the command line, type CFGTCP to display the Configure TCP/IP menu.
13. On the Configure TCP/IP menu, select Option 1 (Work with TCP/IP interfaces).
14. Select option 1 (Add) to show the Add TCP/IP Interface display, and press Enter.
15. Enter the following values to create a new TCP/IP interface and press Enter:
 - Internet address: 192.168.1.3
 - Line description: Eth01
 - Subnet mask: 255.255.255.128

Important: These addresses are used for example purposes only. You need to enter the values that pertain to your own network.

16. Press F3 to return to the Configure TCP/IP menu.
17. On the Configure TCP/IP menu, select option 2 (Work with TCP/IP routes).
18. Select option 1 (Add) to go to the Add TCP/IP Route (ADDTCPRTE) display, and press Enter.
19. Enter the following values to create a route and press Enter:
 - Route destination: *DFTRROUTE
 - Subnet mask: *NONE

- Next hop: 192.168.1.1

Note: If you are not connected to another network, this route is unnecessary. It is added here because this company knows it will connect to the Internet in the future.

20. Select option 10 (Work with TCP/IP Host Table Entries) from the Configure TCP/IP menu, and press Enter.
21. Select option 1 (Add) to go to the Add TCP/IP Host Table Entry display, and press Enter.
22. Enter the following values to add a host table entry and press Enter:
 - IP address: 192.168.1.3
 - Host names: iseriesa.sampson.com
 - Name: iseriesa
23. Repeat Step 22 for each system on your network. Because the server is not configured as a Domain Name System (DNS), each system must have host table entries. For example, to allow iSeries A to communicate with workstation 1 (192.168.1.4/wstn1), add an additional host table entry: **IP address:** 192.168.1.4, **Host name:** wstn1.sampson.com, and **Name:** wstn1. If this is not realistic for your network environment, see the DNS configuration topic in the information center.
24. On the command line, type STRTCP to start TCP/IP. This should also start your interfaces and lines.

Test TCP/IP

After you have successfully installed TCP/IP Connectivity and Utilities licensed program and configured TCP/IP on your iSeries system, you should test your TCP/IP connections.

To test your TCP/IP connection to the network, follow these steps:

1. Verify that TCP/IP communication is configured and started on each of the workstations. Use the documentation provided by your workstation vendor.
2. From workstation 1, open a command prompt and type ping 192.168.1.3. You might receive a message that confirms the packet has been sent to iSeries A. This verifies that the workstation can access the server. If the connection to the network fails, you can see TCP/IP troubleshooting topic in the information center for more information.

Install and configure iSeries Access for Windows on your workstation

During the license program (LP) installation procedure, Sampson Organic Produce installed the LP for iSeries Access for Windows on the server. In order to use iSeries Navigator (a component of iSeries Access for Windows), you must also install the client on your personal computer. See the iSeries Access for Windows instructions for details on how to install the client on your PC.

Configure printers on the LAN

You also need to provide print services to your users by allowing them to share a common printer attached to the office LAN. The printer in your network is compatible with Simple Network Management Protocol (SNMP). You will use your iSeries system as a print server to manage print jobs and to send them to this printer on your LAN. This printer is attached to the LAN with a network adaptor.

To set up the iSeries server as a print server that manages print jobs, complete the following steps:

1. Configure printers
 - a. Ensure that all cabling is complete.
 - b. Ensure the printer is set up using the printer's instructions manual.

- c. On the control panel of the printer, set the Port Timeout to 300 (5 minutes). This timer controls the amount of time in seconds (5 to 300) that the printer waits before printing the last page. The timer does not end with a command to print the page.
2. Create the printer device description
 - a. From a character-based interface, type CRTDEVPRT to create a printer device description. A printer device description should be created when your printer is directly attached to LAN.
 - b. On the Create Device Description (Printer) display, enter the following parameters:

Tip: At times, you might need to press F10 and Enter to view all parameters. You can accept the default values for parameters that you see on the display that are not included in the following list. For a detailed description of each parameter, use the CL command finder in the iSeries Information Center. Search by name for the CRTDEVPRT command and select Create Device Desc (Printer) (CRTDEVPRT) command.

 - Device description: PRINTER1
 - Device class: *LAN
 - Device type: 3812
 - Device model: 1
 - LAN attachment: *IP
 - Port number: 2501
 - Form feed: *AUTOCUT
 - Printer error message: *INFO
 - Manufacturer type and model: *IBM4340
 - Paper source 1: *LETTER
 - Paper source 2: *LETTER
 - Envelope source: *NONE
 - Name or address: 192.168.1.7
 - User-defined options: *IBMSHRCNN
 - System driver program: *IBMSNMPDRV
 - Text description: *LAN 3812 SNMP Device Description for IBM IP40
 - c. From the command line, type VRYCFG to vary on the configuration for PRINTER1.
 - d. On the Vary Configuration (VRYCFG) display, enter the following information:
 - Configuration object: PRINTER1
 - Type: *DEV
 - Status: *ON
 - e. After completing these fields, press Enter.
 - f. On the command line, type STRPRTWTR to start the printer writer.
 - g. On the Start Printer Writer (STRPRTWTR) display, enter PRINTER1 in the **Printer** field. Press Enter.
3. Test the printer connection
 - a. Ensure that the printer is turned on and ready.
 - b. Type WRKWTR (Work will all printers command) to verify that the printer device status is STR.
 - c. Verify that iSeries A can communicate with the printer by typing ping 192.168.1.7. You receive confirmation that the system is connected to the printer.

Related reference

CL command finder

Test network connections

After you have completed the printer configuration for the network, you should test all connections in the network.

To test all your connections in your network, complete the following steps:

1. From a command line, type `ping xx.xx.xx.xx` where `xx.xx.xx.xx` is the IP address of each of the workstations and the printer.
2. From a command prompt on each of the workstations, type `ping xx.xx.xx.xx` where `xx.xx.xx.xx` is the IP address of the iSeries server and the printer.

Tip: You must configure the new printer on each workstation and add the printer IP address to each host table.

3. **Optional:** Print a test page using the following instructions:
 - a. From iSeries Navigator, select **Basic operations** → **Printer Output**.
 - b. Right-click an output name in the right pane, and select **Open** to view the output.
 - c. From the Viewer, select **File** → **Print**.
 - d. Select your print options and click **Print**. This page should be sent to the printer.

If these connections do not work, the network administrator for Sampson Organic can use TCP/IP troubleshooting to locate problems.

Secure your iSeries server

The recommendations in this topic are generated by the IBM eServer Security Planner for the Sampson Organic Produce Company. Complete the IBM eServer Security Planner to review these details.

Tip: The following recommendations do not include full descriptions of security values and operational considerations for these system values.

Table 1. General security recommendations

System value	Recommended value
QSECURITY	40
QINACTITV	60
QINACTMSGQ	*DSCJOB
QDSCJOBITV	240
QSHRMEMCTL	1 (Yes)
QRETSVRSEC	1 (Yes)
QRMTSRVATR	0 (No)
QRMTIPL	*NONE

Table 2. Password policy recommendations

System value	Recommended value
QPWDLVL	0
QPWDEXPITV	90
QPWDMINLEN	8
QPWDRQDDIF	8
QPWDLMTCHR	*NONE

Table 2. Password policy recommendations (continued)

System value	Recommended value
QPWDLMTAJC	0 (allowed)
QPWDLMTREP	0 (characters can be repeated)
QPWDPOSDIF	0 (No)
QPWDRQDDGT	1 (Yes)
QPWDVLDPGM	*NONE

Table 3. Sign-on policy recommendations

System value	Recommended value
QDSPSGNINF	1 (Yes)
QLMTDEVSSN	0 (No)
QLMTSECOFR	1 (Yes)
QMAXSIGN	3
QMAXSGNACN	2 (disable user profile)
QRMTSIGN	*FRCSIGNON (always display sign-on)

Table 4. Restore policy recommendations

System value	Recommended value
QALWOBJRST	*ALWPTF
QVFYOBJRST	3
QFRCCVNRST	3

Table 5. Auditing policy recommendations

System value	Recommended value
QAUDCTL	*AUDLVL,*OBJAUD, *NOQTEMP
QAUDCTL	*NONE

Note: Auditing reports will be scheduled monthly.

Related tasks

“Implement system security recommendations”

Related reference

Security Reference

Security Planner

Related information

i5/OS system value finder

Implement system security recommendations

To protect assets stored on the iSeries server, Sampson Organic Produce used the IBM eServer Security Planner, an interactive planning tool that creates a dynamic set of recommendations based on the system environment. To access this tool, see IBM eServer Security Planner. You can use the security recommendations that the administrator for Sampson Organic Produce generated from the Security Planner as an example for implementing your own security settings.

To implement security on iSeries A, complete the following steps:

1. In iSeries Navigator, expand **iSeries A**. Right-click **Security** and select **Configure**.
2. On the Welcome page, click **Next**.
3. Select **Average** to describe your general security policy. Click **Next**.
4. Select **Running business applications** to describe how your server will be used. Click **Next**.
5. Select **No** and click **Next**.
6. Select **No** for your APPC use and click **Next**.
7. Select **Yes** to indicate that you are using TCP/IP and click **Next**.
8. Select **No** to indicate that you are not connecting to the Internet and click **Next**.
9. Select **No** and click **Next**.
10. Select **No** to indicate that you are not using IBM iSeries NetServer™. Click **Next**.
11. Select **No** and click **Next** twice.
12. Select **Yes** to audit security-related actions on the server. Click **Next**.
13. Select **Yes** to schedule reports to monitor security on the system. Click **Next**.
14. Select **Once a month** for scheduling these reports. Click **Next**.
15. To review the security recommendations, click **Details**. You can change the security values by clearing the appropriate security control. Click **OK**. Then click **Next**.
16. Specify the directory in which you would like to store the Administrator and User Information Reports. Click **Next**. You can review each of these reports.
17. Click **Next** again.
18. Select **Yes, make changes now** and click **Finish**. You have now completed security configuration on iSeries A.

Related reference

“Secure your iSeries server” on page 9
Security Planner

Explore TCP/IP services, applications, and protocols

There are many other TCP/IP services that Sampson Organic Produce can implement in the future. The most common utilities are Telnet and FTP. In addition, the company might want more information about printing, TCP/IP applications, protocols, services, and iSeries Navigator for additional features.

Related reference

TCP/IP applications, protocols, and services
Printing

Scenario: Enable remote connections

Your company has a branch sales office that has several remote sales personnel who need to connect to your iSeries server. You also connect to your corporate office located in another state. Because the information that is transmitted between these areas of your company is sensitive, you are concerned about protecting it as it is sent across the Internet. Use this scenario to configure connections to remote clients and servers.

Situation

You are the network administrator for a branch sales office that manages several mobile sales employees. You also work with the corporate office located in another state. Both the remote sales personnel and the corporate office need access to your internal network; however, you are concerned about protecting information as it is transmitted over the Internet.

The corporate office often needs access to sensitive information like customer accounts and billing statements. Your mobile sales employees transmit information to your branch sales office by dialing an

Internet service provider (ISP) through the Point-to-Point Protocol (PPP). Because they also transmit sensitive information, you need to ensure data integrity and privacy in these communications. You do not want sensitive credit card numbers or customer contact information exposed to the Internet. After researching your options for both groups of users, you have decided to use a virtual private network (VPN) to protect your connections to the corporate office and to use Layer Two Tunnel Protocol (L2TP) protected with a VPN for your remote employees.

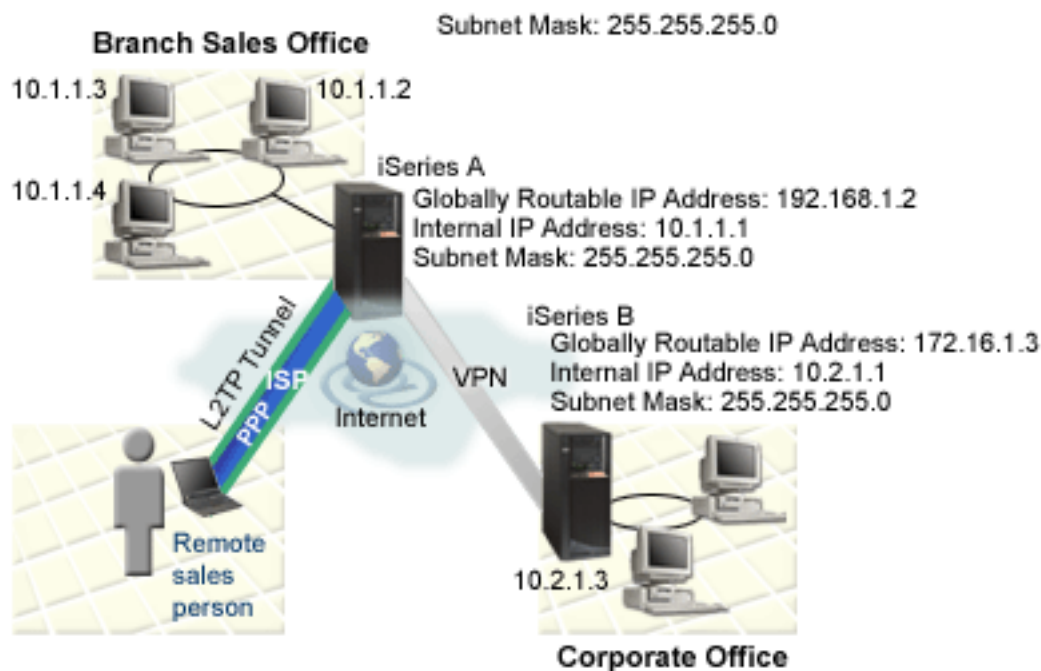
Objectives

The administrators for MyCo, Inc have the following objectives:

- To provide access to remote sales people and the corporate office
- To use existing iSeries servers to support these goals
- To allow remote sales people and the corporate office to access the branch office network

Details

The following network topology shows the connections between a branch sales office and a corporate headquarters and remote sales personnel. Connections to the branch sales office are protected through a VPN. The following descriptions of each part of this network provide details on their configuration.



Branch sale office

- iSeries A runs on OS/400 Version 5 Release 2 (V5R2) and contains all pertinent business applications.
- iSeries A acts as the gateway for the VPN connection with the branch sales office.
- iSeries A has IP address 192.168.1.2, which is globally routable.

Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP address scheme and should not be used in any actual configuration. Use your own IP addresses when completing these tasks.

- Subnet mask is 255.255.255.0.
- iSeries A connects to its subnet with the IP address 10.1.1.1.

- Within the internal network of the branch sales office, all PCs have been configured with a default route that points to iSeries A.
- The fully qualified host name of iSeries A is iseriesa.myco.min.com.
- Both iSeries A and B can initiate connections.
- Remote employees use a pool of IP addresses that range from 10.1.1.100 to 10.1.1.150.

Corporate office

- iSeries B runs on OS/400 Version 5 Release 2 (V5R2) and contains all pertinent business applications.
- iSeries B acts as the gateway for the VPN connection for corporate office.
- iSeries B has the IP address of 172.16.1.3 that is globally routable.

Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.

- Subnet mask is 255.255.255.0.
- iSeries B connects to its subnet with the IP address 10.2.1.1.
- Within the internal network of the corporate office, all PCs have been configured with a default route that points to iSeries B.
- The fully qualified host name of iSeries B is iseriesb.myco.wis.com.

Remote sales personnel

- Laptop with a Microsoft® Windows XP operating system
- Remote employees use a pool of IP addresses that range from 10.1.1.100 to 10.1.1.150.

Prerequisites and assumptions

This scenario provides an example VPN configuration between a branch sales office and a corporate office. It also provides instructions on how to configure remote access for travelling sales people connecting to the branch office. This scenario assumes that several prerequisite steps have been completed and tested, and are operational before beginning these configuration steps. These prerequisites are assumed to have been completed for this scenario:

1. Ensure that the following licensed programs have been installed:

- OS/400 Version 5 Release 2 (5722-SS1)
- Digital Certificate Manager (5722-SS1 Option 34)

Note: This scenario assumes that DCM has been installed on both systems, but it has not been configured on either system.


- TCP/IP Connectivity Utilities for i5/OS (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- IBM eServer iSeries Access for Windows (5722-XE1) and iSeries Navigator
- IBM Developer Kit for Java™ (5722-JV1)
- Ensure that you have the latest PTFs have been installed on your system.

2. Ensure that the following server setup has been completed:

- TCP/IP must be configured, including IP interfaces, routes, local host name, and local domain name.
- Basic system security has been configured and tested.
- The Network component of iSeries Navigator has been installed.
- The retain server security data (QRETSVRSEC *SEC) system value has been set to 1.
- The shared memory (QSHRMEMCTL) system value has been set to 1.

- Normal TCP/IP communications has been established between required endpoints.
3. Ensure that the following requirements are on the PC that is used for remote employees:
- Windows XP client with a Windows 32-bit operating system is properly connected to your iSeries server and configured for TCP/IP.
 - A 233 Mhz processing unit.
 - Windows XP clients must have 64 MB RAM.
 - iSeries Access for Windows and iSeries Navigator have been installed on the client PC.
 - Software must support IP Security (IPSec) protocol.
 - Software must support Layer 2 Tunneling Protocol (L2TP).
 - Connection to an ISP has been established.

In addition to these prerequisites, it is assumed that both networks have set up and activated filter rules on their networks, configured routing, and established an IP addressing scheme. If you have not completed these tasks, see the following topics: IP filtering and network address translation (NAT) and TCP/IP routing and workload balancing.

Tip: This scenario shows the iSeries security gateways attached directly to the Internet. The absence of a firewall is intended to simplify the scenario. It does not imply that the use of a firewall is not necessary. In fact, you should consider the security risks involved anytime you connect to the Internet. Review AS/400® Internet Security Scenarios: A Practical Approach  , for a detailed description of various methods for reducing security risks.

Related reference

- IP filtering and network address translation (NAT)
- TCP/IP routing and workload balancing
- AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00
- DCM scenarios
- VPN scenarios
- PPP scenarios

Set up Certificate Authority with Digital Certificate Manager

Before setting up a Certificate Authority (CA), the administrator for the branch office needed to ensure that several planning tasks were completed. Ensure that all the prerequisites for this scenario have been completed before completing these tasks.

Complete planning work sheets for Digital Certificate Manager

After completing thorough planning, MyCo, Inc completes the following planning work sheets to help set up digital certificates to issue to their business partner.

Table 6. Planning work sheet for creating a Certificate Authority (CA) with Digital Certificate Manager (DCM)

Questions	Answers
What key size do you plan to use for generating the public and private keys for the certificate?	1024
What is the certificate store password?	secret Important: All passwords that are used in this scenario are for example purposes only. Do not use these passwords in any actual configuration.
What is the name of the Certificate Authority?	mycoca

Table 6. Planning work sheet for creating a Certificate Authority (CA) with Digital Certificate Manager (DCM) (continued)

Questions	Answers
What is the name of your organization?	myco
How many days do you want the Certificate Authority to be valid?	1095 (3 years)
What is your browser?	Windows Internet Explorer version 6.0
Will you issue certificates to users on the network?	No

Table 7. Planning work sheet for server certificate for iSeries A

Questions	Answers
What key size do you plan to use for generating the public and private keys for the certificate?	1024
What is the certificate store password?	secret Important: All passwords that are used in this scenario are for example purposes only. Do not use these passwords in any actual configuration.
What is the name of the certificate label?	mycocert
What is the common name for your certificate?	mycocert
What is the name of your organization?	MyCo, Inc
What is the IP address of your iSeries server?	192.168.1.2 Important: IP addresses used in this scenario are meant for example purpose only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.
What is the fully qualified host name of your iSeries server?	iseriesa.myco.min.com

Table 8. Planning work sheet for server certificates for iSeries B

Questions	Answers
What key size do you plan to use for generating the public and private keys for the certificate?	1024
What is the name of the certificate label?	corporatecert
What is the common name for your certificate?	corporatecert
What is the certificate store path and filename?	/tmp/iseriesb.kdb
What is the certificate store password?	secret2 Important: All passwords that are used in this scenario are for example purposes only. Do not use these passwords in any actual configuration.
What is the common name of the server certificate?	corporatecert
What is the organizational name that owns this certificate?	MyCo, Inc

Table 8. Planning work sheet for server certificates for iSeries B (continued)

Questions	Answers
What is the IP address of your iSeries server?	172.16.1.3 Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.
What is the fully qualified host name of your iSeries server?	iseriesb.myco.wis.com

Start IBM HTTP Server for iSeries on iSeries A

To access the Digital Certificate Manager (DCM) interface, you must start the administrative instance of the HTTP Server by completing the following tasks:

1. From iSeries A, sign on to a character-based interface.
2. At the command prompt, type `strtcpsvr server(*HTTP) httpsvr(*admin)`. This will start the administration server of the HTTP Server.

Configure iSeries A as a Certificate Authority

1. In a Web browser, type `http://iseriesa:2001`. This will launch the iSeries Task Page that allows you to access the Digital Certificate Manager (DCM) interface.
2. Log on with your iSeries A user profile name and password.
3. Click **Digital Certificate Manager**.
4. From the left navigation pane, select **Create a Certificate Authority (CA)**.
5. On the Create a Certificate Authority (CA) page, fill in the following required fields with the information from the DCM planning work sheet:
 - **Key size:** 1024
 - **Certificate store password:** secret
 - **Confirm password:** secret

Important: All passwords that are used in this scenario are for example purposes only. Do not use these passwords in any actual configuration.

- **Certificate Authority name:** myco
 - **Organizational name:** MyCo, Inc
 - **State or province:** min
 - **Country or region:** us
 - **Validity period of Certificate Authority (2-7300):** 1095
6. Click **Continue**.
 7. On the **Install Local CA certificate** page, click **Continue**.
 8. On the **Certificate Authority (CA) Policy Data** page, select the following options:
 - **Allow creation of user certificates:** Yes
 - **Validity period of certificates that are issued by this Certificate Authority (1-2000):** 365
 9. On the Policy Data Accepted page, read the messages that are displayed and click **Continue** to create the default server certificate store (*SYSTEM) and a server certificate signed by your Certificate Authority (CA). Read the confirmation message and click **Continue**.
 10. On the Create a Server or Client Certificate page, enter the following information:

- **Key size:** 1024
- **Certificate label:** mycocert
- **Certificate store password:** secret
- **Confirm password:** secret

Important: All passwords that are used in this scenario are for example purposes only. Do not use these passwords in any actual configuration.

- **Common name:** mycocert
- **Organizational name:** myco
- **State or province:** min
- **Country or region:** us
- **IP version 4 address:** 192.168.1.2

Note: IP addresses used in this scenario are meant for example purpose only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.

- **Fully qualified domain name:** iseriesa.myco.min.com
- **E-mail address:** administrator@myco.min.com

11. Click **Continue**.
12. On the Select Application page, click **Continue**.

Tip: The VPN New Connection wizard automatically assigns the certificate you just created to the i5/OS VPN Key Manager application. If you have other applications that might use this certificate, you can select them on this page. Because this scenario only uses certificates for VPN connections, there is no need to select any additional applications.

13. On the Application Status page, read the messages that are displayed and click **Cancel**. This accepts the changes that you created.

Note: If you want to create a certificate store to contain certificates that are used to sign objects, select **Continue**.

14. When the DCM interface is refreshed, select **Select a Certificate Store**.
15. On the Select a Certificate Store page, select ***SYSTEM**. Click **Continue**.
16. On the Certificate Store and Password page, enter secret. Click **Continue**.
17. In the left navigation frame, select **Manage Applications**.
18. On the Manage Applications page, select **Define CA trust list**. Click **Continue**.
19. On the Define CA Trust List page, select **Server**. Click **Continue**.
20. Select **i5/OS VPN Key Manager**. Click **Define CA Trust List**.
21. On the Define CA Trust List page, select **LOCAL_CERTIFICATE_AUTHORITY**. Click **OK**.

Create server certificate for iSeries B

1. In the left navigation pane, click **Create Certificate** and select **Server or client certificate for another iSeries**.
2. Click **Continue**.
3. On the Create Server or Client Certificate for another iSeries page, select **V5R2**. This is the release level for iSeries B. Click **Continue**.
4. On the Create a Server or Client Certificate page, enter the following information:
 - **Key size:** 1024
 - **Certificate label:** corporatecert
 - **Certificate store path and filename:** /tmp/iseriesb.kdb

- **Certificate store password:** secret2
- **Confirm password:** secret2

Note: All passwords that are used in this scenario are for example purposes only. Do not use these passwords in any actual configuration.

- **Common name:** corporatcert
- **Organizational name:** MyCo, Inc
- **State or province:** wis
- **Country or region:** us
- **IP version 4 address:** 172.16.1.3

Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.

- **Fully qualified host name:** iseriesb.myco.wis.com
 - **E-mail address:** administrator@myco.wis.com
5. Click **Continue**. You will receive a confirmation message verifying that a server certificate has been created on iSeries A for iSeries B. As the administrator of the network for the branch sales office, you send these files to the administrator at the corporate office through encrypted e-mail. The administrator at the corporate office must now move and rename the certificate store (.KDB) file and the request (.RDB) file to iSeries B. The administrator at the corporate office will need to move these files to the /QIBM/USERDATA/ICSS/CERT/SERVER directory in the integrated file system (IFS) using binary FTP. After that is completed, the administrator must rename these files in the appropriate directory.

Rename .KDB and .RDB files on iSeries B

Because the *SYSTEM certificate store does not exist on iSeries B, the administrator of the corporate network will need to rename the iseriesb.kdb and iseriesb.RDB files to DEFAULT.KDB and DEFAULT.RDB, thus using these transferred files as the *SYSTEM certificate store on iSeries B.

1. In iSeries Navigator, expand **iSeries B** → **File Systems** → **Integrated File System** → **Qibm** → **UserData** → **ICSS** → **Cert** → **Server** and verify that the files iseriesb.kdb and iseriesb.RDB are listed in this directory.
2. On a command line, type `wrklnk ('/qibm/userdata/icss/cert/server')`.
3. On the Work with Link Objects page, select 7 to rename the iseriesb.kdb file. Press Enter.
4. On the Rename Object page, enter DEFAULT.KDB in the **New Object** field. Press Enter.
5. Repeat Step 3 and Step 4 to rename the iseriesb.RDB file to DEFAULT.RDB.
6. Verify that these files have been changed by refreshing iSeries Navigator and expanding **iSeries B** → **File Systems** → **Integrated File System** → **Qibm** → **UserData** → **ICSS** → **Cert** → **Server**. The DEFAULT.KDB and DEFAULT.RDB files must be listed in the directory.

Change Certificate Store password on iSeries B

Now the network administrator for the corporate office must change the password for the new *SYSTEM Certificate Store that was created when the DEFAULT.KDB and DEFAULT.RDB files were created.

Note: You must change the *SYSTEM Certificate Store password. When you change the password, it is stashed so that the application can automatically recover it and open the Certificate Store to access certificates.

1. In a browser, type `http://iseriesb:2001`. Click **Select a Certificate Store**.
2. Select ***SYSTEM Certificate Store** and enter secret2 for the password. This is the password that the administrator of the branch sales office specified when creating the server certificate for iSeries B. Click **Continue**.

3. In the left navigation frame, select **Manage Certificate Store** and select **Change Password** and click **Continue**.
4. On the Change Certificate Store Password page, enter coporatepwd in the **New password** and **Confirm password** fields.
5. Select **Password does not expire** for the expiration policy. Click **Continue**. A confirmation page is loaded. Click **OK**.
6. On the Change Certificate Store Password confirmation page, read the message on that display and click **OK**.
7. On the Certificate Store and Password page that is reloaded, enter coporatepwd in the **Certificate Store Password** field. Click **Continue**.

Define CA trust for i5/OS VPN Key Manager on iSeries B

1. In the left navigation frame, select **Manage Applications**.
2. On the Manage Applications page, select **Define CA trust list**. Click **Continue**.
3. On the Define CA Trust List page, select **Server**. Click **Continue**.
4. Select **i5/OS VPN Key Manager**. Click **Define CA Trust List**.
5. On the Define CA Trust List page, select **LOCAL_CERTIFICATE_AUTHORITY**. Click **OK**.

Now the administrators for the branch sales office and corporate office can begin VPN configuration.

Configure VPN connection between the branch sales office and the corporate office

The following steps show you how the administrator of the branch sales office configures a VPN connection.

Complete planning work sheets for VPN connection from the branch office to remote sales employees

The administrator for the branch sales office used the VPN planning advisor to create dynamic planning work sheets to help them configure VPN between the branch sales office and the corporate office. The VPN planning advisor is an interactive tool that asks specific questions regarding your VPN needs. Based on your answers, the advisor generates a customized planning work sheet for your environment that can be used when you configure your VPN connection. This work sheet can then be used when configuring a VPN on your iSeries server. Each of the following planning work sheets are generated with the VPN planning advisor and are used to configure a VPN using the VPN New Connection wizard in iSeries Navigator.

Table 9. Planning work sheet for VPN connection between the branch sales office and corporate office

What the VPN wizard asks	What the VPN advisor recommends
What would you like to name this connection group?	SalestoCorporate
What type of connection group would you like to create?	Select Connect your gateway to another gateway
What Internet Key Exchange policy do you want to use to protect your key?	Select Create a new policy , and then select Highest Security, lowest performance
Are you using certificates?	Select Yes and myocert as the certificate Note: This certificate was created during the steps for configuring a Certificate Authority on iSeries A.

Table 9. Planning work sheet for VPN connection between the branch sales office and corporate office (continued)

What the VPN wizard asks	What the VPN advisor recommends
Select the identifier to represent the local connection endpoint.	Select the identifier type IP version 4 address and identifier 192.168.1.2 from the list of identifier types and identifiers that were defined in the certificate you chose. Note: IP addresses used in this scenario are meant for example purpose only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.
What is the identifier of the key server that you want to connect to?	Select the identifier type IP version 4 address and identifier: 172.16.1.3 . Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.
What are the local endpoints of the data that this connection will protect?	Identifier type: IP version 4 subnet Identifier: 10.1.1.0 Mask: 255.255.255.0
What are the remote endpoints of the data that this connection will protect?	Identifier type: IP version 4 subnet Identifier: 10.2.1.0 Mask: 255.255.255.0
What are the ports and protocols of the data that this connection will protect?	Local Port: Any port Remote Port: Any port Protocol: Any protocol
What data policy do you want to use to protect the data?	Select Create a new policy , and then select Highest security, lowest performance
Check the interfaces on the local system that this connection will be applied to.	<ul style="list-style-type: none"> • ETHLINE (branch sales office) • ELINE (corporate office)

Related reference

VPN planning advisor

Configure VPN on iSeries A

After completing your planning for VPN connections, you can now configure iSeries A to use VPN to secure transmission of data between the two networks.

Tip: If VPN server is already started when you run the VPN New Connection wizard, the wizard will not automatically find the certificate store or any of the certificates you just created. If the VPN server is running, you must restart it on iSeries Navigator before running the VPN New Connection wizard.

Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. Use your own IP addresses when completing these tasks.

The administrator for MyCo, Inc used the planning work sheet generated from the VPN planning advisor to configure a VPN on iSeries A:

1. In iSeries Navigator, expand **iSeries A** → **Network** → **IP Policies**.
2. Right-click **Virtual Private Networking** and select **New Connection** to start the Connection wizard. Review the Welcome page for information about what objects the wizard creates.
3. On the Connection Name page, enter SalestoCorporate in the **Name** field. (Optional) Specify a description for this connection group. Click **Next**.
4. On the Connection Scenario page, select **Connect your gateway to another gateway**. Click **Next**.
5. On the Internet Key Exchange Policy page, select **Create a new policy** and then select **Highest security, lowest performance**. Click **Next**.
6. On the Certificate for Local Connection Endpoint page, select **Yes** and select **myocert** from the list of certificates. Click **Next**.
7. On the Local Connection Endpoint Identifier page, select **Version 4 IP address** as the identifier type. The associated IP address should be 192.168.1.2. This information is defined in the certificate that you create in DCM. Click **Next** twice.
8. On the Remote Key Server page, select **Version 4 IP address** in the **Identifier type** field. Enter 172.16.1.3 in the **Identifier** field. This is the IP address for iSeries B in the network of the corporate office. Click **Next**.
9. On the Local Data Endpoint page, select **IP version 4 subnet** as the identifier type, and enter 10.1.1.0 for the identifier, and 255.255.255.0 as the mask.
10. On the Remote Data Endpoint page, select **IP version 4 subnet** as the identifier type, and enter 10.2.1.0 for the identifier, and 255.255.255.0 as the mask.
11. On the Data Services page, select **Any port** for the local port, **Any port** for the remote port, and **Any protocol** for the protocol. Click **Next**.
12. On the Data Policy page, select **Create a new policy**, and then select **Highest security, lowest performance**. Click **Next**.
13. On the Applicable Interfaces page, select **ETHLINE**. Click **Next**.
14. On the Summary page, review the objects that the wizard will create to ensure they are correct.
15. Click **Finish** to complete the configuration. When the Activate Policy Filters dialog box appears, select **No, packet rules will be activated at a later time**, and then click **OK**.

Configure VPN on iSeries B

The administrator for the corporate office follows the same steps that the administrator at the branch sales office used when iSeries A was configured, reversing the IP address when necessary. Use the planning work sheets for guidance.

After this administrator finishes configuring iSeries B, both administrators can activate filter rules on both servers.

Activate filter rules on both servers

The wizard automatically creates the packet rules that this connection requires to work properly. However, you must activate them on both systems before you can start the VPN connection. To do this on iSeries A, follow these steps:

Note: If you lose connection to the iSeries after activating filter rules, you must delete all filter rules currently active on the server. To do this, use the RMVTCPTBL (*ALL) command from a character-based interface.

1. In iSeries Navigator, expand **iSeries A** → **Network** → **IP Policies**.
2. Right-click **Packet Rules** and select **Activate Rules**.
3. On the Activate Packet Rules page, select to **activate only the VPN generated rules** and select **ETHLINE** as the interface on which you would like to activate these filter rules. Click **OK**.
4. Repeat these steps to activate packet rules on iSeries B, using **ELINE** instead of **ETHLINE** for the interface.

Start the VPN connection

Follow these steps to start the SalestoCorporate connection from iSeries A:

1. In iSeries Navigator, expand **iSeries A** → **Network** → **IP Policies**.
2. Right-click **Virtual Private Networking** and select **Start**. This starts the VPN server.
3. Expand **Virtual Private Networking** → **Secure Connections**. Click **All Connections** to display a list of connections in the right pane. Right-click **SalestoCorporate**, and then select **Start**.
4. From the **View** menu, select **Refresh**. If the connection starts successfully, the status changes from idle to enabled. The connection might take a few minutes to start, so periodically click **Refresh** until the status changes to Enabled.
5. Repeat these steps on iSeries B.

Test VPN connection between endpoints

After you finish configuring both servers and have successfully started the connection, you should test the connectivity to ensure that the remote hosts can communicate with each other.

Tip: For any traffic with the destination of the remote network, ensure that the local clients have the appropriate routes configured.

On a Windows XP workstation within the branch sales office, the network administrator should complete these steps:

1. From the command prompt, enter `ping 10.2.1.3`. This is the IP address of one of the workstations in the network of the corporate office.

Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.

2. Repeat these steps, this time testing the connectivity from the corporate office to the branch office.

Configure VPN connection to remote users

The following tasks show you how the administrator for the branch sales office configures a VPN connection to remote users.

Complete planning work sheets for VPN connection from the branch office to remote sales people

The administrator for the branch sales office uses the VPN planning advisor to create dynamic planning work sheets to help them configure VPN on their servers and remote workstations. The VPN planning advisor is an interactive tool that asks specific questions regarding your VPN needs. Based on your answers, the advisor generates a customized planning work sheet for your environment that can be used when you configure your VPN connection. This work sheet can then be used when configuring a VPN on your iSeries server. Each of the following planning work sheets are generated with the VPN planning advisor and are used to configure a VPN using the VPN New Connection wizard in iSeries Navigator.

Table 10. Planning work sheet for VPN connection between branch sales office and remote sales people

What the VPN wizard asks	What the VPN advisor recommends
What would you like to name this connection group?	SalestoRemote
What type of connection group would you like to create?	Select Connect your host to another host
What Internet Key Exchange policy do you want to use to protect your key?	Select Create a new policy and then select highest security, lowest performance
Are you using certificates?	Select No
Enter the identifier to represent the local key server for this connection.	Identifier type: IP version 4 address IP address:192.168.1.2 Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.
What is the identifier of the key server that you want to connect to?	Identifier type: Any IP address Pre-shared key: mycokey Note: The Pre-shared key is a 32-character text string that i5/OS VPN uses to authenticate the connection as well as to establish the keys that protect your data. In general, you should treat a Pre-shared key as you would a password.
What are the ports and protocols of the data that this connection will protect?	Local Port: 1701 Remote Port: Any port Protocol: UDP
What data policy do you want to use to protect the data?	Select Create a new policy and then select highest security, lowest performance
Check the interfaces on the local system that this connection will be applied to.	ETHLINE (Branch sales office)

Related reference

VPN planning advisor

Configure L2TP terminator profile for iSeries A

You want to configure the remote connections to remote workstations. You need to set up iSeries A to accept inbound connections from these clients. To configure a L2TP terminator profile for iSeries A, complete the following steps:

1. In iSeries Navigator, expand **iSeries A** → **Network** → **Remote Access Services**.
2. Right-click **Receiver Connection Profiles** to set the iSeries A as a server that allows incoming connections from remote users , and select **New Profile**.
3. **New Point-to-Point Connection Profile Setup**
 - **Protocol type:** PPP
 - **Connection type:** L2TP (virtual line)

Note: The Operating mode field should automatically display **Terminator (network server)**.

- **Line service type:** Single line
4. Click **OK**. This will launch the New Point-to-Point Profile Properties page.
 5. On the New Point-to-Point Profile Properties page, enter MYCOL2TP in the **Name** field. Click **OK**.
 6. On the Connection tab, select **192.168.1.2** for the **Local tunnel endpoint IP address**.

Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. Use your own IP addresses when completing these tasks.

7. Select **MYCOL2TP** as the **Virtual line name**. Click **OK**. This will launch the New L2TP Properties page.
8. On the Authentication page, enter **iseriesa** as the host name. Click **OK**. This will return you to the Connection page.
9. On the Connection page, select the following options, enter 25 as the **Maximum number of connections**.
10. On the Authentication tab, select **Require this iSeries server to verify the identity of the remote system**.
11. Select **Authenticate locally with validation list**.
12. Enter QL2TP in Validation list name field, enter QL2TP and click **New**.
13. In the Validation list page, select **Add**.
14. Add user names and passwords for each of your remote employees. Click **OK**.
15. On the Password confirmation page, re-enter the password for each remote employees. Click **OK**.
16. On the TCP/IP Setting page, select 10.1.1.1 for **Local IP address**.
17. In the **IP address assignment method** field, select **Address pool**.
18. In the **Starting IP address** field, enter 10.1.1.100 and 49 for the **Number of addresses**.
19. Select **Allow remote system to access other networks (IP forwarding)**. Click **OK**.

Start receiver connection profile

After configuring L2TP receiver connection profile for iSeries A, the administrator needs to start this connection so that it will listen for incoming requests from remote clients.

Note: You might receive an error message that the QUSRWRK subsystem is not started. This message occurs when attempting to start the receiver connection profile. To start the QUSRWRK subsystem, complete these steps:

1. In a character-based interface, enter strsubs.
2. On the Start Subsystem display, enter QUSRWRK in the **Subsystem description** field.

To configure a VPN for remote clients, complete these tasks:

1. In iSeries Navigator, select **Refresh** from the **View** menu. This will refresh your instance of iSeries Navigator.
2. In iSeries Navigator, expand **iSeries A** → **Network** → **Remote Access Services**.
3. Double-click **Receiver Connection Profiles** and right-click **MYCOL2TP** and select **Start**.
4. The **Status** field will display, **Waiting for connection requests**.

Configure a VPN connection on iSeries A for remote clients

After configuring and starting the L2TP receiver connection profile for iSeries A, the administrator needs to configure a VPN to protect the connection between remote clients and the network in branch sales office.

To configure a VPN for remote clients, complete these steps:

Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. Use your own IP addresses when completing these tasks.

1. In iSeries Navigator, expand **iSeries A** → **Network** → **IP Policies**.
2. Right-click **Virtual Private Networking** and select **New Connection** to start the VPN New Connection wizard. Review the Welcome page for information about what objects the wizard creates.
3. Click **Next** to go to the Connection Name page.
4. In the **Name** field, enter **SalesToRemote**.
5. **Optional:** Specify a description for this connection group. Click **Next**.
6. On the Connection Scenario page, select **Connect your host to another host**. Click **Next**.
7. On the Internet Key Exchange Policy page, select **Create a new policy**, and then select **Highest security, lowest performance**. Click **Next**.
8. On the Certificate for Local Connection Endpoint page, select **No**. Click **Next**.
9. On the Local Key Server page, select **Version 4 IP address** as the identifier type. The associated IP address should be 192.168.1.2. Click **Next**.
10. On the Remote Key Server page, select **Any IP address** in the Identifier type field. In the **Pre-shared key** field, enter **mycokey**. Click **Next**.
11. On the Data Services page, enter 1701 for the local port, select 1701 for the remote port, and select **UDP** for the protocol. Click **Next**.
12. On the Data Policy page, select **Create a new policy** and then select **Highest security, lowest performance**. Click **Next**.
13. On the Applicable Interfaces page, select **ETHLINE**. Click **Next**.
14. On the Summary page, review the objects that the wizard will create to ensure they are correct.
15. Click **Finish** to complete the configuration. When the Activate Policy Filters dialog box window appears, select **No, packet rules will be activated at a later time**. Click **OK**.

Update VPN policies for remote connections from Windows XP clients

Because the wizard creates a standard connection that can be used for most VPN configurations, you will need to update the policies that were generated by the wizard to ensure interoperability with Windows XP clients. To update these VPN policies, complete the following tasks:

1. In iSeries Navigator, expand **iSeries A** → **Network** → **IP Policies** → **Virtual Private Networking** → **IP Security Policies**.
2. Double-click **Internet Key Exchange Policies** and right-click **Any IP address** and select **Properties**.
3. On the Transform page, click **Add**.
4. On the Add Internet Key Exchange Transform page, select the following options::

- **Authentication method:** Pre-shared key
 - **Hash algorithm:** MD5
 - **Encryption algorithm:** DES-CBC
5. Click **OK**.
 6. In iSeries Navigator, expand **iSeries A** → **Network** → **IP Policies** → **Virtual Private Networking** → **IP Security Policies**.
 7. Double-click **Data Policies** and right-click **SalestoRemote** and select **Properties**.
 8. On the General page, clear **Use Diffie-Hellman perfect forward secrecy**.
 9. On the Proposal page, click **Add**.
 10. On the New Data Policy Proposal page, select the following options:
 - **Encapsulation mode:** Transport
 - **Key expiration:** 15 minutes
 - **Expire at size limit:** 100000
 11. On the Transform page, click **Add**.
 12. On the Add Data Policy Transform page, select the following options:
 - **Protocol:** Encapsulating security payload (ESP)
 - **Authentication algorithm:** MD5
 - **Encryption algorithm:** DES-CBC
 13. Click **OK**.

Activate filter rules

The wizard automatically creates the packet rules that this connection requires to work properly. However, you must activate them on both systems before you can start the VPN connection.

To activate filter rules on iSeries A, follow these steps:

Important: IP addresses used in this scenario are meant for example purposes only. They do not reflect an IP addressing scheme and should not be used in any actual configuration. You should use your own IP addresses when completing these tasks.

1. In iSeries Navigator, expand **iSeries A** → **Network** → **IP Policies**.
2. Right-click **Packet Rules** and select **Activate Rules**.
3. On the Activate Packet Rules page, select to **activate only the VPN generated rules** and select **ETHLINE** as the interface on which you would like to activate these filter rules. Click **OK**.

Before remote users can configure their Windows XP workstations, the administrator gives them the following information so they can set up their side of the connection. For each of your remote users, give them the following information:

- Name of Pre-shared key: mycokey
- IP address of iSeries A: 192.168.1.2
- User name and password for the connection

Note: These were created when the administrator added the user name and passwords to a validation list during the configuration of L2TP terminator profile.

Configure VPN on Windows XP client

Remote users at MyCo, Inc will need to set up their remote Windows XP client by completing the following steps:

1. In the Windows XP **Start** menu, expand **Programs** → **Accessories** → **Communications** → **New Connection Wizard**.
2. On the Welcome page, read the overview information. Click **Next**.
3. On the Network Connection Type page, select **Connect to the network at my workplace**. Click **Next**.
4. On the Network Connection page, select **Virtual Private Network connection**. Click **Next**.
5. On the Connection Name page, enter Connection to Branch office in the **Company Name** field. Click **Next**.
6. On the Public Network page, select **Do not dial the initial connection**. Click **Next**.
7. On the VPN Server Selection page, enter 192.168.1.2 in the **Host name or IP address** field. Click **Next**.
8. On the Summary page, click **Add a shortcut to this connection to my desktop**. Click **Finish**.
9. Click the **Connect Connection to MyCo** icon that has been created on your desktop.
10. On the Connect Connection to MyCo page, enter the user name and password that the administrator provided.
11. Select **Save this user name and password for the following users and Me only**. Click **Properties**.
12. On the **Security** page, ensure that the following **Security options** are selected:
 - **Typical**
 - **Require secured password**
 - **Require data encryption**
 Click **IPSec Settings**.
13. On the IPSec Settings page, select **Use pre-shared key for authentication** and enter mycokey in the **Pre-shared key** field. Click **OK**.
14. On Networking page, select **L2TP IPSec VPN** as the **Type of VPN**. Click **OK**.
15. Sign on with username and password and click **Connect**.

To start the VPN connection on the client side, click the icon that appears on your desktop after completing the connection wizard.

Test VPN connection between endpoints

After you finish configuring the connection between iSeries A and remote users, and you have successfully started the connection, you should test the connectivity to ensure that the remote hosts can communicate with each other.

To test the connectivity, follow these steps:

1. In iSeries Navigator, expand **iSeries A** → **Network**.
2. Right-click **TCP/IP Configuration** and select **Utilities** and then select **Ping**.
3. From the **Ping from** dialog, enter 10.1.1.101 in the **Ping** field.

Note: 10.1.1.101 represents the IP address dynamically assigned (to the remote sales client) from the address pool specified in the L2TP terminator profile on iSeries A.

4. Click **Ping Now** to verify connectivity from iSeries A to a remote workstation. Click **OK**.

To test the connection from the remote client, the remote employee completes these steps on a workstation that is running Windows:

1. From the command prompt, enter ping 10.1.1.2. This is the IP address of one of the workstations in the network of the corporate office.
2. Repeat these steps, this time testing the connectivity from the corporate office to the branch office.

Scenario: Create a virtual Ethernet for interpartition communications

You are the system administrator for a small company. You use a server that is divided into four logical partitions. You need to allow communication between all four logical partitions. You want to avoid purchasing excess Ethernet cards and cables because money and space is limited in your IT department.

Situation

You are the system administrator for a small company. You use a server that is divided into four logical partitions. You need to allow high-speed communication between all four logical partitions and you need to extend that communication to an external LAN. Your hardware has a limited number of card slots available for LAN cards. Therefore, you must find a solution that does not require additional LAN cards.

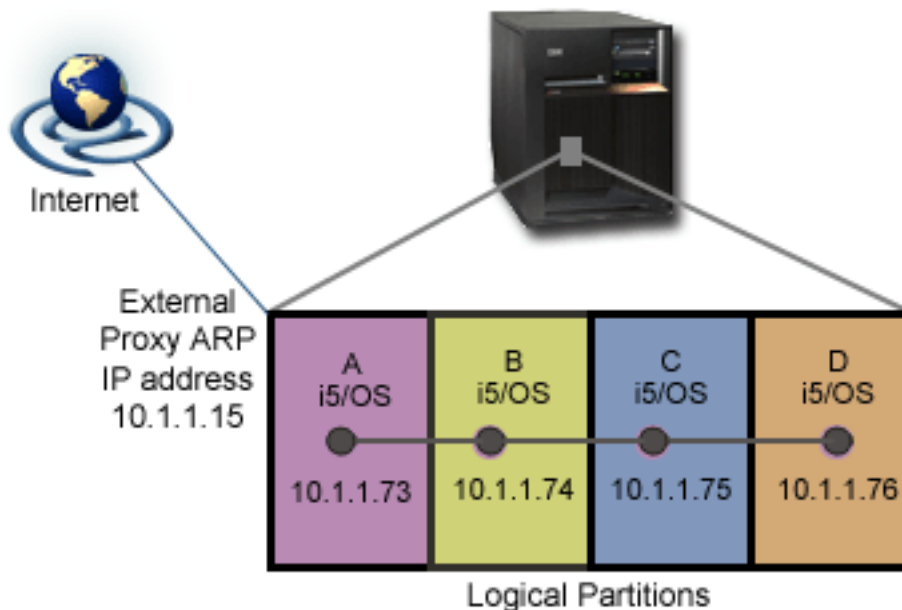
Objectives

As the system administrator for this company, you have the following objectives:

- To create a virtual Ethernet network to allow communications between logical partitions.
- To enable proxy ARP to connect the virtual Ethernet network to an external LAN.
- To configure the necessary lines, interfaces and routes.

Details

This figure shows a virtual Ethernet that enables communication among four logical partitions and uses proxy ARP to allow the data to flow between the virtual Ethernet and the external LAN.



- Four logical partitions have been created on the iSeries server.
- Each partition runs on i5/OS Version 5 Release 3.
- A virtual TCP/IP interface is configured on each partition using these IP addresses:
 - Partition A has the IP address 10.1.1.73.
 - Partition B has the IP address 10.1.1.74.
 - Partition C has the IP address 10.1.1.75.
 - Partition D has the IP address 10.1.1.76.
- An external proxy ARP interface is configured on Partition A using the IP address 10.1.1.15.

Prerequisites and assumptions

Setup requirements include:

- i5/OS Version 5 Release 3 or later installed on the primary logical partition
- IBM 270 and 8xx model servers
- Four logical partitions (LPAR) on the server. The primary logical partition must have i5/OS Version 5 Release 3, or later, installed. The other logical partitions can have i5/OS V5R3 or Linux[®] installed.

In this scenario, all of the logical partitions are using i5/OS.

Configuration Steps

Complete these configuration tasks:

Related reference

Logical partitions

Enable the logical partitions to participate in a virtual Ethernet

To enable virtual Ethernet, follow these steps:

1. At the command line on the primary partition (partition A), type STRSST and press Enter.
2. Type your service tools user ID and password.
3. From the System Service Tools (SST) display, select option 5 (Work with System Partitions).
4. From the Work with System Partitions display, select option 3 (Work with partition configuration).
5. Press F10 (Work with Virtual Ethernet).
6. Type 1 in the appropriate column for the primary partition and the secondary partition to enable the partitions to communicate with one another over virtual Ethernet.
7. Exit System Service Tools (SST) to return to the command line.

Create the Ethernet line descriptions

To configure new Ethernet line descriptions to support virtual Ethernet, follow these steps:

1. At the command line on logical partition A, type WRKHDWRSC *CMN, and press Enter.
2. From the Work with Communication Resources display, select option 7 (Display resource detail) next to the appropriate virtual Ethernet port.
The Ethernet port identified as 268C is the virtual Ethernet resource. There will be one for each virtual Ethernet that is connected to the logical partition.
3. From the Display Resource Detail display, scroll down to find the port address.
The port address corresponds to the virtual Ethernet you selected during the configuration of the logical partition.
4. From the Work with Communication Resources display, select option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet port, and press Enter.
5. From the Work with Configuration Descriptions display, select option 1 (Create), and press Enter to see the Create Line Description Ethernet (CRTLINETH) display.
 - a. For the *Line description* prompt, type VETH0. The name VETH0, although arbitrary, corresponds to the numbered column on the Virtual Ethernet page in which you enabled the logical partitions to communicate. If you use the same names for the line descriptions and their associated virtual Ethernet, you can easily keep track of your virtual Ethernet configurations.
 - b. For the *Line speed* prompt, type 1G.
 - c. For the *Duplex* prompt, type *FULL, and press Enter.
 - d. For the *Maximum frame size* prompt, type 8996, and press Enter.

By changing the frame size to 8996, the transfer of data across the virtual Ethernet is improved.
You will see a message stating the line description has been created.

6. Vary on the line description. Type `WRKCFGSTS *LIN` and select option 1 (Vary on) for VETH0.
7. Repeat steps 1 through 6, but perform the steps from the command lines on logical partitions B, C, and D to create an Ethernet line description for each logical partition.

Although the names of your line descriptions are arbitrary, it is helpful to use the same names for all of the line descriptions associated with the virtual Ethernet. In this scenario, all the line descriptions are named VETH0.

Turn on IP datagram forwarding

You need to turn on IP datagram forwarding on the partition that connects the virtual Ethernet to the external LAN. IP datagram forwarding enables the IP packets to be forwarded among different subnets. For this scenario, you need to turn on IP datagram forwarding on Partition A.

To turn on IP datagram forwarding, follow these steps:

1. At the command line on partition A, type `CHGTCPA` and press F4.
2. For the *IP datagram forwarding* prompt, type `*YES`.

Create the interface to enable proxy ARP

Before you create the TCP/IP interfaces, you need to decide how you want to connect your virtual Ethernet to a physical LAN. To allow your logical partitions to communicate with systems on an external LAN, you need to enable the TCP/IP traffic to travel between the virtual Ethernet and the external LAN. There are three methods for connecting the virtual and external networks: Proxy ARP, network address translation (NAT), and TCP/IP routing. This scenario uses the Proxy ARP method. For more information about all three methods of connecting this network traffic, see TCP/IP techniques connecting virtual Ethernet to external LANs.

To create the TCP/IP interface to enable proxy ARP, complete these steps:

1. Obtain a contiguous block of IP addresses that are routable by your network.

Because you have a total of four logical partitions in this virtual Ethernet, you need a block of eight addresses. The fourth segment of the first IP address in the block must be divisible by eight. The first and last IP addresses of this block are the subnet and broadcast IP addresses and are unusable. The second address can be used for a virtual TCP/IP interface on logical partition A, and the third, fourth, and fifth addresses can be used for the TCP/IP connections on each of the other logical partitions. For this scenario, the IP address block is 10.1.1.72 through 10.1.1.79 with a subnet mask of 255.255.255.248.

You also need a single IP address for your external TCP/IP address. This IP address should not belong to your block of contiguous addresses, but it must be within the same original subnet mask of 255.255.255.0.

2. Create an i5/OS TCP/IP interface for logical partition A. This interface is known as the external, proxy ARP IP interface.

To create the interface, follow these steps:

- a. At the command line on partition A, type `CFGTCP`, and press Enter to see the Configure TCP/IP display.
- b. Select option 1 (Work with TCP/IP Interfaces), and press Enter.
- c. Select option 1 (Add), and press Enter to see the Add TCP/IP Interface (ADDTCPIFC) display.
- d. For the Internet address prompt, type `10.1.1.15`.
- e. For the Line description prompt, type the name of your line description, such as `ETHLINE`.
- f. For the Subnet mask prompt, type `255.255.255.0`.

3. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface you want to start.

Related reference

TCP/IP techniques connecting virtual Ethernet to external LANs

Create the virtual Ethernet interface on partition A

To create the virtual Ethernet interface on partition A, complete these steps:

1. At the command line on partition A, type `CFGTCP`, and press Enter to see the Configure TCP/IP display.
2. Select option 1 (Work with TCP/IP Interfaces), and press Enter.
3. Select option 1 (Add), and press Enter to see the Add TCP/IP Interface (ADDTCPIFC) display.
4. For the Internet address prompt, type `10.1.1.73`.
5. For the Line description prompt, type `VETH0`.
6. For the Subnet mask prompt, type `255.255.255.248`.
7. For the Associated local interface prompt, type `10.1.1.15`. This associates the virtual Ethernet interface to the external interface and enables proxy ARP to forward packets between the virtual Ethernet interface `10.1.1.73` and the external interface `10.1.1.15`.
8. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface you want to start.

Create the virtual Ethernet interface on partition B

To create the virtual Ethernet interface on partition B, complete these steps:

1. At the command line on partition B, type `CFGTCP`, and press Enter to see the Configure TCP/IP display.
2. Select option 1 (Work with TCP/IP Interfaces), and press Enter.
3. Select option 1 (Add), and press Enter to see the Add TCP/IP Interface (ADDTCPIFC) display.
4. For the Internet address prompt, type `10.1.1.74`.
5. For the Line description prompt, type `VETH0`.
6. For the Subnet mask prompt, type `255.255.255.248`.
7. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface you want to start.

Create the virtual Ethernet interface on partition C

To create the virtual Ethernet interface on partition C, complete these steps:

1. At the command line on partition C, type `CFGTCP`, and press Enter to see the Configure TCP/IP display.
2. Select option 1 (Work with TCP/IP Interfaces), and press Enter.
3. Select option 1 (Add), and press Enter to see the Add TCP/IP Interface (ADDTCPIFC) display.
4. For the Internet address prompt, type `10.1.1.75`.
5. For the Line description prompt, type `VETH0`.
6. For the Subnet mask prompt, type `255.255.255.248`.
7. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface you want to start.

Create the virtual Ethernet interface on partition D

To create the virtual Ethernet interface on partition D, complete these steps:

1. At the command line on partition D, type `CFGTCP`, and press Enter to see the Configure TCP/IP display.
2. Select option 1 (Work with TCP/IP Interfaces), and press Enter.
3. Select option 1 (Add), and press Enter to see the Add TCP/IP Interface (ADDTCPIFC) display.
4. For the Internet address prompt, type `10.1.1.76`.
5. For the Line description prompt, type `VETH0`.
6. For the Subnet mask prompt, type `255.255.255.248`.
7. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface you want to start.

Create the routes

To create the default routes to enable the packets to exit the virtual Ethernet, follow these steps:

1. At the command line on partition B, type `CFGTCP`, and press Enter.
2. Select option 2 (Work with TCP/IP Routes), and press Enter.
3. Select option 1 (Add), and press Enter.
4. For the Route destination prompt, type `*DFTRROUTE`.
5. For the Subnet mask prompt, type `*NONE`.
6. For the Next hop prompt, type `10.1.1.73`.
7. Repeat steps 1 through 6 for partitions C and D to create a default route on each of those logical partitions. Specify `10.1.1.73` as the next hop address in each case.

Packets from each of these logical partitions travel over the virtual Ethernet to the `10.1.1.73` interface using these default routes. Because `10.1.1.73` is associated with the external proxy ARP interface `10.1.1.15`, the packets continue out of the virtual Ethernet using the proxy ARP interface.

Verify network communications

Verify your network communications by using the ping command:

- From partitions B, C, and D, ping the virtual Ethernet interface `10.1.1.73` and an external host.
- From an external i5/OS host, ping each of the virtual Ethernet interfaces `10.1.1.73`, `10.1.1.74`, `10.1.1.75`, and `10.1.1.76`.

Related reference

ping command

Scenario: Share a modem between logical partitions using L2TP

You have virtual Ethernet set up across four logical partitions. Use this scenario to enable selected logical partitions to share a modem. These logical partitions will use the shared modem to access an external LAN.

Situation

You are the system administrator at a medium sized company. It's time to update your computer equipment, but you'd like to do more than that; you want to streamline your hardware. You start the process by consolidating the work of three old servers onto one new iSeries server. You create three logical partitions on the iSeries server. The new iSeries server came with a 2793 internal modem. This is

the only input/output processor (IOP) you have that supports PPP. You also have an old 7852-400 electronic customer support (ECS) modem.

Solution

Multiple systems and partitions can share the same modems for dial-up connections, eliminating the need for each system or partition to have its own modem. This is possible by using L2TP tunnels and configuring L2TP profiles which allow outgoing calls. In your network, the tunnels will run over a virtual Ethernet network and a physical network. The physical line connects to another server in your network, which will also share modems.

Details

The following figure illustrates the network characteristics for this scenario:

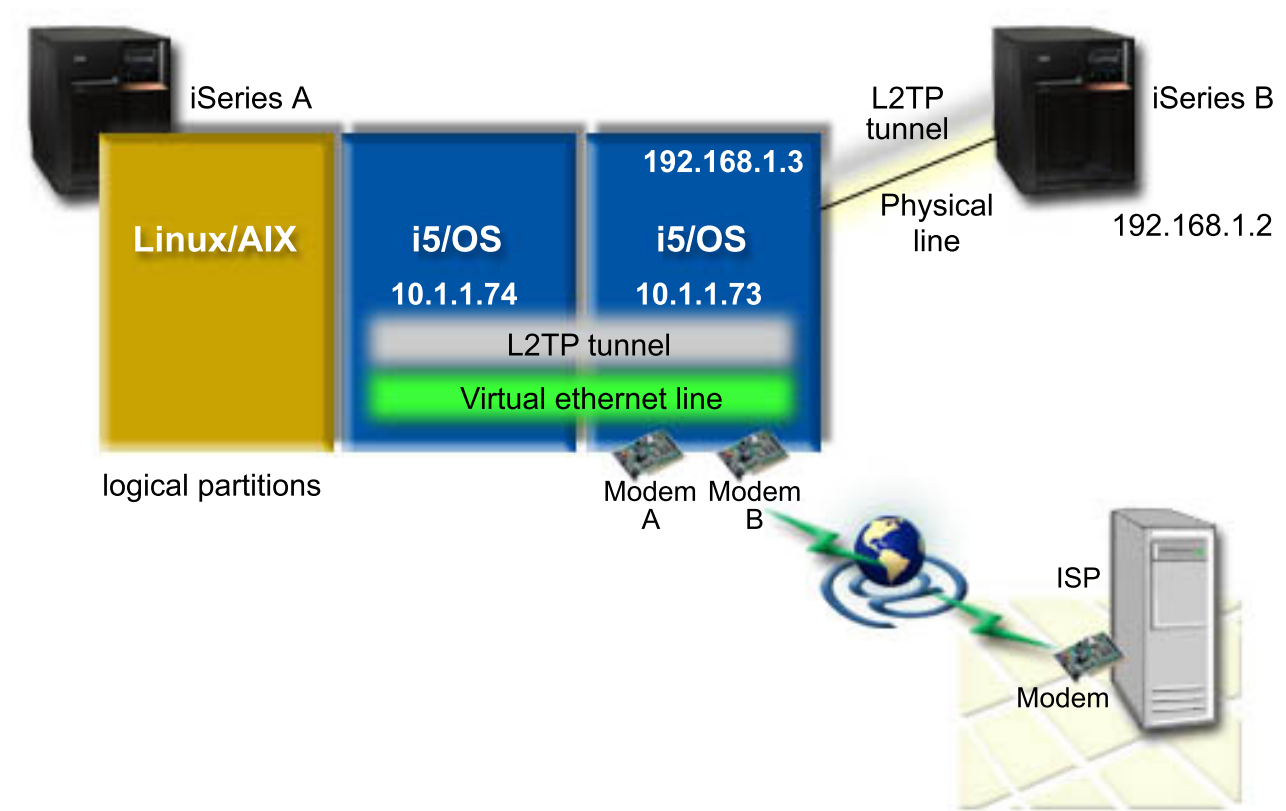


Figure 1. Multiple systems sharing the same modem for dial-up connections

Prerequisites and assumptions

Setup requirements for iSeries-A include:

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

- You have created at least two logical partitions (LPAR) on the server. The partition that owns the modem must have i5/OS Version 5 Release 3 or later installed. The other partitions can have OS/400 V5R2, V5R3, Linux, or AIX® installed. In this scenario, the partitions are either using i5/OS or Linux operating systems.
- You have virtual Ethernet created to communicate across partitions. See the following scenario: Create a virtual Ethernet network for interpartition communication.

Setup requirements for iSeries-B include:

- iSeries Access for Windows and iSeries Navigator (Configuration and Service component of iSeries Navigator), Version 5 Release 2 or later

Scenario details: Share a modem between logical partitions using L2TP

After you complete the prerequisites, you are ready to begin configuring the L2TP profiles.

Step 1: Configure L2TP terminator profile for any interface on the partition, which owns the modems

Follow these steps to create a terminator profile for any interface:

1. In iSeries Navigator, expand *your server* → **Network** → **Remote Access Services**.
2. Right-click **Receiver Connection Profiles**, and select **New Profile**.
3. Select the following options on the Setup page and click **OK**:
 - **Protocol type**: PPP
 - **Connection type**: L2TP (virtual line)
 - **Operating mode**: Terminator (network server)
 - **Type of line service**: Single line
4. On the **New Profile - General** tab, complete the following fields:
 - **Name**: toExternal
 - **Description**: Receiver connection to dial out
 - Select **Start profile with TCP**.
5. On the **New Profile - Connection** tab, complete the following fields.
 - **Local tunnel endpoint IP address**: ANY
 - **Virtual line name**: toExternal. This line has no associated physical interface. The virtual line describes various characteristics of this PPP profile. The L2TP Line Properties window opens. Click the **Authentication** tab and enter your server's host name. Click **OK** to return to the Connection tab on the New PPP Profile Properties window.
6. Click **Allow out-going call establishment**. The **Outgoing call dial properties** dialog appears.
7. On the Outgoing Call Dial Properties page, select a line service type.
 - **Type of line service**: Line pool
 - **Name**: dialOut
 - Click **New**. The **New Line Pool Properties** dialog appears.
8. On the New line pool properties window, select the lines and modems to which you will allow the outgoing calls and click **Add**. If you need to define these lines, select **New Line**. The interfaces on the partition which owns these modems will try to use whichever line is open from this line pool. The new Line Properties window appears.
9. On the **New Line Properties - General** tab, enter information in the following fields:
 - **Name**: line1
 - **Description**: first line and first modem for line pool (2793 internal modem)
 - **Hardware resource**: cmn03 (communication port)

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

Note: These numbers might be something like your ISP which is going to be frequently called by the other systems using these modems. If the other systems specify a telephone number of *PRIMARY or *BACKUP, the actual numbers dialed will be the ones specified here. If the other systems specify an actual telephone number then the telephone number will be used instead.

17. On the **TCP/IP Settings** tab, select the following values:
 - **Local IP address:** None
 - **Remote IP address:** None

Note: If you are also using the profile to terminate L2TP sessions, you will need to pick the local IP address which represents the iSeries server. For Remote IP address, you can select an address pool that is in the same subnet as your server. All L2TP sessions would get their IP addresses from this pool. For other considerations, see Multiple Connection Profile Support.

18. On the **Authentication** tab, accept all default values.

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

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.

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 IP 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 IP 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 IP 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 IP address after creating the interface, you select the option to start the IP address when using the Interface Wizard.

Remote IP address pools for multiple-connection profiles:

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

Line pool restrictions:

These restrictions apply when using line pools for multiple connections:

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

Step 2: Configure a L2TP originator profile on 10.1.1.74

Follow these steps to create a L2TP originator profile:

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

- **Connection type:** L2TP (virtual line)
 - **Operating mode:** Remote dial
 - **Type of line service:** Single line
4. On the **General** tab, complete the following fields:
 - **Name:** toModem
 - **Description:** originator connection going to partition owning modem
 5. On the **Connection** tab, complete the following fields:

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

Note: The protocol should match whatever protocol the server you are dialing also uses.

12. Enter your user name and password.

Note: The user name and password needs to match whatever user name and password is valid on the server to which you are dialing.

13. Go to the **TCP/IP Settings** tab and verify the required fields:
 - **Local IP address:** Assigned by remote system
 - **Remote IP address:** Assigned by remote system
 - **Routing:** No additional routing is required
14. Click **OK** to save the PPP profile.

Step 3: Configure a L2TP remote dial profile for 192.168.1.2

Repeat Step 2. However, change the remote tunnel endpoint address to 192.168.1.3 (the physical interface to which iSeries B connects).

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

Step 4: Test connection

After you finish configuring both servers, you should test the connectivity to ensure that the systems are sharing the modem to reach external networks. To do this, follow these steps:

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

- a. In iSeries Navigator, expand **10.1.1.74** → **Network** → **Remote Access Services** → **Originator Connection Profiles**.
- b. In the right pane, find the required profile (toModem) and verify the **Status** field is *Active*. If not, right-click the profile and select **Start**.
3. Start the Remote dial profile on iSeries B.
 - a. In iSeries Navigator, expand **192.168.1.2** → **Network** → **Remote Access Services** → **Originator Connection Profiles**.
 - b. In the right pane, find the profile you created and verify the **Status** field is *Active*. If not, right-click the profile and select **Start**.
4. If possible, ping the ISP or other destination that you've dialed to verify both profiles are active. You will attempt the ping from both 10.1.1.74 and 192.168.1.2.
5. As an alternative, you can also check the Connection Status.
 - a. In iSeries Navigator, expand *the required server (such as 10.1.1.73)* → **Network** → **Remote Access Services** → **Originator Connection Profiles**.
 - b. In the right pane, right-click the profile you created and select **Connections**. On the Connection Status window you can see which profiles are active, inactive, connecting, and more.

Appendix. Notices

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

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

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

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

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

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

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

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

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

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

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

IBM Corporation

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

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

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

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

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

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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

COPYRIGHT LICENSE:

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

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

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

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

Programming Interface Information

This Network scenarios publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

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

AS/400
eServer
e(logo)server
i5/OS
IBM
IBM (logo)
Infoprint
iSeries
NetServer
OS/400

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

Terms and conditions

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

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

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

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

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

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

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



Printed in USA