



@server

iSeries

Network scenarios

Version 5 Release 3





@server

iSeries

Network scenarios

Version 5 Release 3

Note

Before using the information and the product it supports, be sure to read the information in "Notices," on page 49.

Second Edition (August 2005)

This edition applies to version 5 release 3 modification 0 of IBM Operating System/400® (product number 5722-SS1), and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2004, 2005. All rights reserved.

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

Contents

Chapter 1. Network scenarios	1	Configure VPN connection between branch sales office and corporate office	28
Chapter 2. What's new for V5R3	3	Configure VPN connection to remote users	31
Chapter 3. Print this topic	5		
Chapter 4. Network planning work sheet	7		
Chapter 5. Scenario: Set up iSeries to communicate with LAN	9		
Scenario details: Set up iSeries to communicate with LAN	11		
Security recommendations	16		
Chapter 6. Scenario: Enable remote connections	19		
Scenario details: Enable remote connections	22		
Set up Certificate Authority (CA) with Digital Certificate Manager	23		
		Chapter 7. Scenario: Create a virtual Ethernet for interpartition communications	37
		Scenario details: Create a virtual Ethernet for interpartition communications	38
		Chapter 8. Scenario: Share a modem between logical partitions using L2TP	43
		Scenario details: Share a modem between logical partitions using L2TP	44
		Appendix. Notices	49
		Trademarks	50
		Terms and conditions for downloading and printing publications	51

Chapter 1. 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. See the Network planning work sheet to read some basic networking considerations.

Print this topic

This page provides instructions on how to download and print a PDF version of this information.

Scenario: Set up the iSeries server to communicate with the 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.

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. Since 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.

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.

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.

Chapter 2. What's new for V5R3

Network scenarios provides a starting place for network administrators who are interested in using common TCP/IP technologies in the networks that they manage. Each scenario provides a complete task and points to additional information and resources within the Information Center. The following scenarios can help you to design and implement similar network topologies in your network environment:

New network scenarios

- Scenario: Set up the iSeries server to communicate with the LAN
- Scenario: Enable remote connections
- Scenario: Create a virtual Ethernet interpartition communications
- Scenario: Share a modem across logical partitions using L2TP

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

Chapter 3. Print this topic

To view or download the PDF version of this document, select Network scenarios (about 242 KB).

You can view or download these related topics:


- TCP/IP setup (456 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 (277 KB) contains the following topics:
 - PPP scenarios
 - PPP concepts
 - Plan PPP
 - Configure PPP
 - Manage PPP
 - Troubleshoot PPP
- Virtual private networking (509 KB) contains the following topics:
 - VPN scenarios
 - VPN concepts
 - Plan VPN
 - Configure VPN
 - Manage VPN
 - Troubleshoot VPN
- TCP/IP troubleshooting (235 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:

- Right-click the PDF in your browser (right-click the link above).
- Click **Save Target As...** if you are using Internet Explorer. Click **Save Link As...** if you are using Netscape Communicator.
- Navigate to the directory in which you would like to save the PDF.
- Click **Save**.

Downloading Adobe Acrobat Reader

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

Chapter 4. Network planning work sheet

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 tables below do not cover a complete network design for every environment, but provide a basis to start you thinking about your own environment. For example, before coming to these scenarios, you need to plan for server availability, performance, capability, and much more.

See Plan for hardware and software: View entire planning checklist to review more thorough considerations. Ultimately, your business objectives determine which applications and networking solutions your company needs.

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?	
Draw a picture of your network.	

Chapter 5. Scenario: Set up iSeries to communicate with 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).

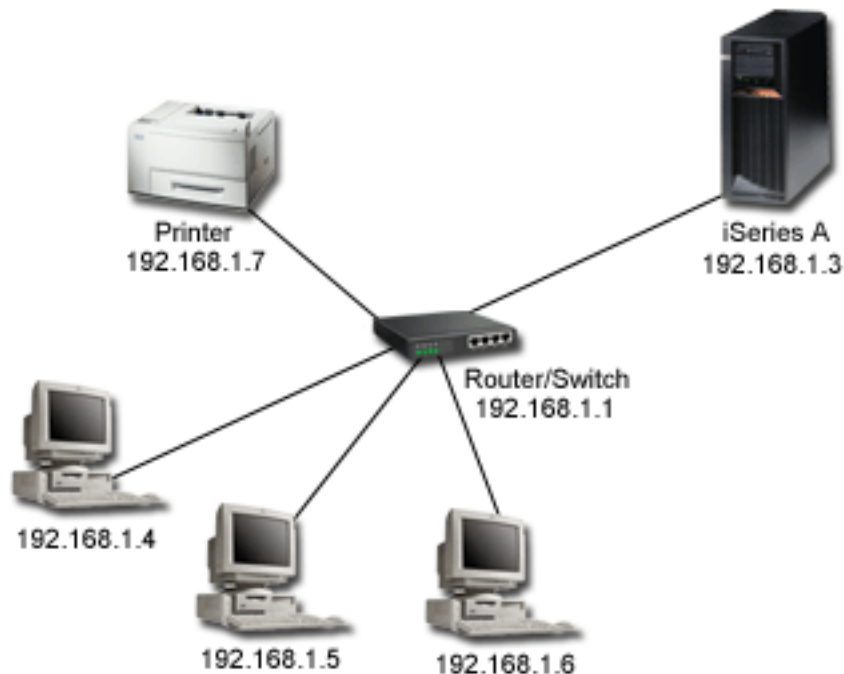
Objectives

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 also are 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 an IP address of 192.168.1.1.

Note: When no external network connection is planned, a hub may be used in place of a router/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 using 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 will be a link to the next task.


1. Review planning work sheets
2. Set up TCP/IP
3. Test TCP/IP
4. Configure printers on the LAN (optional)
5. Test network connections
6. Implement system security recommendations
7. Explore TCP/IP applications, protocols, and services

Scenario details: Set up iSeries to communicate with LAN

The following steps show how the network administrator configured an iSeries server to communicate with an existing LAN for the fictional company, Sampson Organic Produce. Before completing these tasks, the network administrator completed all the necessary prerequisites.

Step 1: 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.

Server work sheet	Company answer
Record the server size.	Model 820
Record the operating system or systems.	OS/400
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 since the LAN is not connected to another network. The company added 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

Network assumptions	Company decisions
Draw a picture of your network.	See scenario diagram.

Step 2: Set up TCP/IP

After you have completed the network planning work sheets, you must set up TCP/IP on your iSeries system.

Complete the following steps to set up TCP/IP on your network:

1. Install the TCP/IP Connectivity and Utilities licensed program

- a. Insert your installation media for TCP/IP into your server. The server uses a CD-ROM device as the installation media.
- b. At the command line, type G0 LICPGM and press Enter to access the Work with Licensed Programs display.
- c. 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.
- d. 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 selected to install.
- e. Press Enter to confirm.
- f. The network administrator entered 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.

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

2. Configure TCP/IP

- a. At a command line, type WRKHDWRSC *CMN to display the Work with Communication Resources menu.
- b. Type 5 beside the communication resource for the Ethernet port and press Enter.
- c. On the Work with Communication Descriptions menu, type 1 and press Enter.
- d. The Create Line Description (Ethernet) (CRTLINETH) menu appears.
- e. In the Line Description field, enter a description for the line. In this example, the network administrator chose Eth01.
- f. Enter the accurate information for the Line speed and Duplex fields. These values should match the port on the switch connecting to the iSeries. In this example, we entered 100M and *HALF respectively. Press Enter.
- g. Press F10 to view additional parameters. You may have to press Page Down to view them.
- h. Change the Link speed field to match the Line Speed you entered previously (In this example, 100M).
- i. Accept all other default values and press Enter.
- j. Press F3 to return to the Work with Communication Resources menu.
- k. Press F3 again to return to the Command entry menu.
- l. At the command line, type CFGTCP to display the Configure TCP/IP menu.

- m. On the Configure TCP/IP menu, select Option 1 (Work with TCP/IP interfaces).
- n. Select option 1 (Add) to show the Add TCP/IP Interface display, and press Enter.
- o. 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

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

- p. Press F3 to return to the Configure TCP/IP menu.
- q. On the Configure TCP/IP menu, select option 2 (Work with TCP/IP routes).
- r. Select option 1 (Add) to go to the Add TCP/IP Route (ADDTCP RTE) display, and press Enter.
- s. 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, since this company knows it will connect to the Internet in the future.

- t. Select option 10 (Work with TCP/IP Host Table Entries) from the Configure TCP/IP menu, and press Enter.
- u. Select option 1 (Add) to go to the Add TCP/IP Host Table Entry display, and press Enter.
- v. 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
- w. Repeat the above step for each system on your network. Since the server is not configured as a domain name server (DNS), each system needs to 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 topic in the Information Center for configuring DNS.
- x. On the command line, type STRTCP to start TCP/IP. This should also start your interfaces and lines.

Step 3: 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:

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 receive a message that confirms the packet has been sent to iSeries A. This verifies that the workstation can access the server.

Step 4: 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 PC. See the iSeries Access for Windows instructions for more detail. Once you have iSeries Navigator working, you will have the ability to perform step 7.

Step 5: 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.

Note: This is an optional step that may not be appropriate for your own network set-up.

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

1. Configure printers

- a. Ensure that all cabling is complete.
- b. Ensure the printer is setup 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 that 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 the LAN.
- b. On the Create Device Description (Printer) display, enter the following:

Note: At times, you will need to press F10 and Enter to view all parameters. You can accept the default values on any parameters seen on the display that are not listed below. For a detailed description of each parameter, see the CL command finder in the iSeries Information Center. Search by name for the CRTDEVPRT command and select Create Device Description (Printer) command. These descriptions will enable you to make the best selection for your particular situation.

- 1) Device description: PRINTER1
 - 2) Device class: *LAN
 - 3) Device type: 3812
 - 4) Device model: 1
 - 5) LAN attachment: *IP
 - 6) Port number: 2501
 - 7) Form feed: *AUTOCUT
 - 8) Printer error message: *INFO
 - 9) Manufacturer type and model: *IBM4340
 - 10) Paper source 1: *LETTER
 - 11) Paper source 2: *LETTER
 - 12) Envelope source: *NONE
 - 13) Name or address: 192.168.1.7
 - 14) User-defined options: *IBMSHRCNN
 - 15) System driver program: *IBMSNMPDRV
 - 16) Text description: *LAN 3812 SNMP Device Description for IBM IP40
- c. After completing these fields, press Enter.
 - d. From the command line, type VRYCFG to vary on the configuration for PRINTER1.

- e. On the Vary Configuration (VRYCFG) display, enter the following:
 - 1) Configuration object: PRINTER1
 - 2) Type: *DEV
 - 3) Status: *ON
 - f. After completing these fields, press Enter.
 - g. On the command line, type STRPRTWTR to start the printer writer.
 - h. 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.

Step 6: Test network connections

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

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

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. **Note:** You will need to configure the new printer on each workstation and add the printer IP address to each host table.

If you want to print a test page, use the following instructions to print a job log from iSeries A:

1. From iSeries Navigator, select **Basic operations ->Printer Output**.
2. Right-click an output name in the right pane, and select **Open** to view the output.
3. From the Viewer, select **File—>Print**.
4. Select your print options and click **Print**. This page should be sent to the printer.

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

Step 7: Implement system security recommendations

To protect assets stored on the iSeries server, Sampson Organic Produce used the IBM® **@server** Security Planner, an interactive planning tool that creates a dynamic set of recommendations based on the system environment. To access this tool, see IBM **@server** 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**.
12. Select **No** and click **Next**.
13. Select **Yes** to audit security-related actions on the server. Click **Next**.
14. Select **Yes** to schedule reports to monitor security on the system. Click **Next**.
15. Select **Once a month** for scheduling these reports. Click **Next**.
16. To review the security recommendations, click **Details...** You can change security values by deselecting the appropriate security control. Click **OK**. Click **Next**.
17. 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.
18. Click **Next** again.
19. Select **Yes, make changes now** and click **Finish**. You have now completed security configuration on iSeries A.



Step 8: 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, they may want more information on printing. Use the following links to explore more TCP/IP applications, protocols, and services:

- [TCP/IP applications, protocols, and services](#)
- [Printing](#)

Note: You can also explore iSeries Navigator for additional features.

Security recommendations

The following recommendations were generated by the IBM  Security Planner for the Sampson Organic Produce Company. Complete the IBM  Security Planner to review these details.

Note: The following recommendations do not include full descriptions of security values and operational considerations for these system values. You can use either Chapter 3, "Security System Values" of the Security Reference manual or the OS/400 system value finder in the Information Center to find more information about specific system values and their options.

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
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.	

Chapter 6. Scenario: Enable remote connections

Situation

You are the network administrator for a branch sales office that manages several mobile sales people. 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 people transmit information to your branch sales office by dialing-up to an ISP through the Point-to-Point Protocol (PPP). Since 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 public 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.

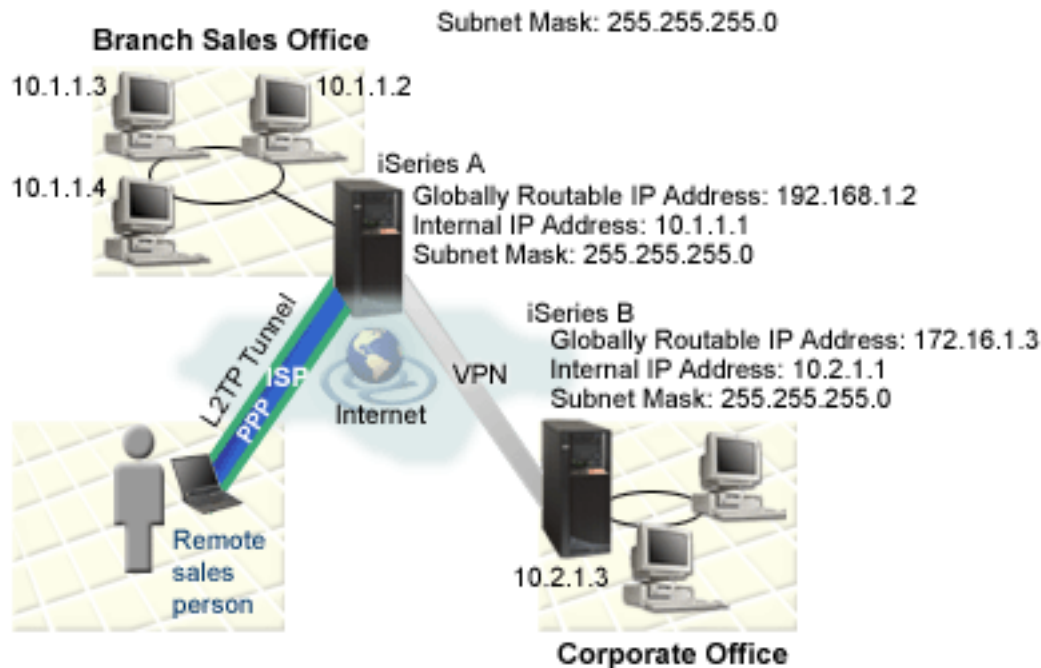
Objectives

The administrators for MyCo, Inc have the following objectives for this scenario:

- 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 the IP address 192.168.1.2 which is globally routable.

Note: IP addresses used in this scenario are meant for example purpose only. They do not reflect an IP address 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 A connects to its subnet with 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.
- iSeries A fully qualified host name is iseriesa.myco.min.com.
- Both iSeries A and B can initiate connections.
- Remote employees use a pool of IP addresses that have the range of 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 which is globally routable.

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.

- Subnet mask is 255.255.255.0.
- iSeries B connects to its subnet with 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.
- iSeries B fully qualified host name is iseriesb.myco.wis.com.

Remote sales personnel

- Laptop with a Windows XP operating system
- Remote employees use a pool of IP addresses that have the range of 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 prior to 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.

- Cryptographic Access Provider (5722-AC3)
- TCP/IP Connectivity Utilities for OS/400 (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- IBM

server

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)
- TCP/IP routing and workload balancing

Note: 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 any time you connect to the Internet. Review this redbook, *AS/400 Internet Security Scenarios: A Practical Approach*, SG24-5954-00  , for a detailed description of various methods for reducing these risks.

Configuration Tasks

Complete the following tasks to enable remote connections to the MyCo, Inc branch sales office:

1. **Set up Certificate Authority (CA) with Digital Certificate Manager**
 - a. Complete planning work sheets for DCM
 - b. Start IBM HTTP Server for iSeries on iSeries A
 - c. Configure iSeries A as a Certificate Authority (CA)
 - d. Create server certificate for iSeries B
 - e. Rename .KDB and .RDB files on iSeries B
 - f. Change *SYSTEM Certificate Store password on iSeries B
 - g. Define CA trust for OS/400 VPN Key Manager on iSeries B
2. **Configure VPN connection between branch sales office and corporate office**
 - a. Complete planning work sheets for VPN connection between branch sales office and corporate office
 - b. Configure VPN on iSeries A
 - c. Configure VPN on iSeries B
 - d. Activate filter rules on both servers
 - e. Start VPN connection
 - f. Test VPN connection between endpoints
3. **Configure VPN connection to remote users**
 - a. Complete planning work sheets for VPN connection from the branch office to remote sales people
 - b. Configure L2TP terminator profile for iSeries A
 - c. Start receiver connection profile
 - d. Configure a VPN connection on iSeries A for remote clients
 - e. Update VPN policies for remote connections from Windows XP clients
 - f. Activate filter rules
 - g. Configure VPN on Windows XP client
 - h. Test connection between endpoints

In addition to this scenario, several other scenarios can be helpful for setting remote connections. See the following topics in the Information Center for more examples of using these technologies:

- DCM scenarios
- VPN scenarios
- PPP scenarios

Scenario details: Enable remote connections

The MyCo, Inc company wants to use VPN connections to protect data transmission between a branch sales office and their corporate headquarters and remote sales representatives.

After completing thorough planning, the administrator for the branch sales office completed the following tasks to set up secure connections between their corporate office and their remote employees. Several

planning tasks must be completed to ensure proper setup. Ensure that all the prerequisites for this scenario have been completed prior to completing these tasks:

1. Set up Certificate Authority (CA) with Digital Certificate Manager (DCM)
2. Configure VPN connection between branch sales office and corporate office
3. Configure VPN connection to remote users

Set up Certificate Authority (CA) 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 prior to completing these tasks.

Step 1: Complete planning work sheets for DCM

After completing thorough planning, MyCo, Inc completed the following planning work sheets to aid them in setting 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 Note: 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
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 Note: 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

Table 7. Planning work sheet for server certificate for iSeries A (continued)

Questions	Answers
What is the IP address of your iSeries server?	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.
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 Note: 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
What is the IP address of your iSeries server?	172.16.1.3 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 fully qualified host name of your iSeries server?	iseriesb.myco.wis.com

Step 2: 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.

Step 3: Configure iSeries A as a Certificate Authority (CA)

1. In a Web browser, type `http://iseriesa:2001`. This will launch the iSeries Task Page which allow 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

Note: 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

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:** 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**.

Note: The VPN New Connection Wizard will automatically assign the certificate you just created to the OS/400 VPN Key Manager application. If you have other applications that would use this certificate, you can select them on this page. Since this scenario will only be using 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 **OS/400 VPN Key Manager**. Click **Define CA Trust List**.
21. On the **Define CA Trust List** page, select **LOCAL_CERTIFICATE_AUTHORITY**. Click **OK**

Step 4: 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/iserieb.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:** corporatecert
- **Organizational name:** MyCo, Inc
- **State or province:** wis
- **Country or region:** us
- **IP version 4 address:** 172.16.1.3

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 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 sent 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. Once that is completed, the administrator must rename these files in the appropriate directory.

Step 5: 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 should be listed in the directory.

Step 6: 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 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 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**.

Step 7: Define CA trust for OS/400 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 **OS/400 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 branch sales office and corporate office

The following steps show you how the administrator on the branch sales office configured a VPN connection.

Step 1: Complete planning work sheets for VPN connection between branch sales office and corporate office

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 will generate 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 were generated with the VPN advisor and will be used to configure a VPN using the VPN New Connection Wizard in iSeries Navigator. To use the VPN advisor, see VPN planning advisor in the Virtual private networking Information Center topic.

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.
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.

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
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 . 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 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)

Step 2: 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.

Note: 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, prior to running the VPN New Connection Wizard.

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 **mycocert** 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. Again, this information is defined in the certificate that you create in DCM.

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.

Click **Next**.

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**.

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.

9. On the **Local Data Endpoint** page, select **IP version 4 subnet** as the identifier type, 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, 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 appears, select **No, packet rules will be activated at a later time**, and then click **OK**.

Step 3: Configure VPN on iSeries B

The administrator for the corporate office followed 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 worksheets for guidance. After this administrator finishes configuring iSeries B, both administrators can activate filter rules on both servers.

Step 4: 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.

Step 5: 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 select **Start**.
4. From the **View** menu, select **Refresh**. If the connection starts successfully, the status should change from Idle to Enabled. The connection may take a few minutes to start, so periodically refresh until the status changes to Enabled.
5. Repeat these steps on iSeries B.

Step 6: 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.

Note: 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 completed 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.

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.

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

Now the administrator can configure the VPN connection to remote users.

Configure VPN connection to remote users

After the VPN connection between the branch sales office and the corporate office has been configured, the administrator of the branch offices wants to set up secure connections to remote sales people.

Step 1: Complete planning work sheets for VPN connection from the branch office to remote sales people

The administrator for the branch sales office used 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 will generate 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 were generated with the VPN advisor to be used with the VPN wizard in iSeries Navigator. To use the VPN advisor, see VPN planning advisor in the Virtual private networking topic.

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

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

What the VPN wizard asks:	What the VPN advisor recommends
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 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?	Identifier type: Any IP address Pre-shared key: mycokey Note: The Pre-shared key is a 32-character text string that OS/400 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)

Step 2: 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. On the **New Point-to-Point Connection Profile Setup** page, and select the following options:
 - **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**.

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.

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**.

Step 3: 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 may receive an error message when attempting to start the receiver connection profile that the QSYSWRK subsystem is not started. To start the QUSRWRK subsystem, complete these tasks:

1. In a character-based interface, enter **strsbs**.
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**.

Step 4: 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 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**.

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.

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 appears, select **No, packet rules will be activated at a later time** Click **OK**.

Step 5: 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 and click **OK**:
 - **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, unselect **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 and click **OK**:
 - **Protocol:** Encapsulating security payload (ESP)
 - **Authentication algorithm:** MD5
 - **Encryption algorithm:** DES-CBC
13. Click **OK**.

Step 6: 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 do this on iSeries A, follow these steps:

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

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.

- 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.

Step 7: 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.

Step 8: 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 do this, 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 complete these steps on a Windows XP workstation:

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.

Chapter 7. Scenario: Create a virtual Ethernet for interpartition communications

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.

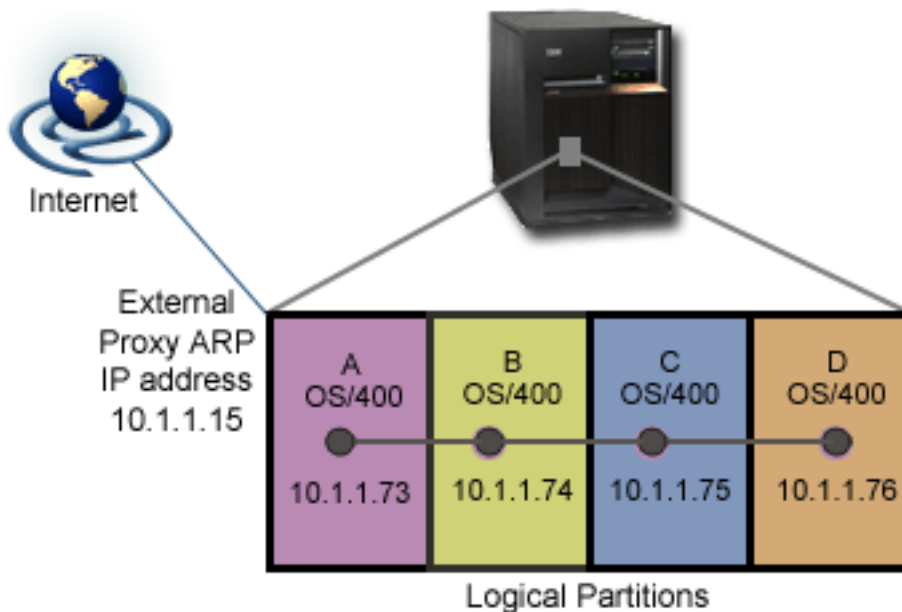
Objectives

The objectives of this scenario are as follows:

- 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 OS/400 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 IP address 10.1.1.15.

Prerequisites and assumptions

Setup requirements include:

- OS/400 Version 5 Release 3 or later installed on the primary logical partition
- IBM 270 and 8xx model servers
- In this case, four logical partitions (LPAR) on the server. The primary logical partition must have OS/400 Version 5 Release 3 or later installed. The other logical partitions may have OS/400 V5R3 or Linux installed.

In this scenario, all of the logical partitions are using OS/400.

Configuration steps

Complete these configuration tasks:

1. Enable the logical partitions to participate in a virtual Ethernet
2. Create the Ethernet line descriptions
3. Turn on IP datagram forwarding
4. Create the interface to enable proxy ARP
5. Create the virtual Ethernet interface on partition A
6. Create the virtual Ethernet interface on partition B
7. Create the virtual Ethernet interface on partition C
8. Create the virtual Ethernet interface on partition D
9. Create the routes
10. Verify network communications

Scenario details: Create a virtual Ethernet for interpartition communications

The following tasks show how the network administrator creates a virtual Ethernet network and enables the network to communicate with an external LAN using proxy ARP.

Step 1: 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.

Step 2: 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.

Step 3: 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.

Step 4: 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 on 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.
Since 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 OS/400 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.

Step 5: Create the virtual Ethernet interface on partition A

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.

Step 6: Create the virtual Ethernet interface on partition B

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.

Step 7: Create the virtual Ethernet interface on partition C

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.

Step 8: Create the virtual Ethernet interface on partition D

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.

Step 9: 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. Since 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.

Step 10: 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 OS/400 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.

Chapter 8. Scenario: Share a modem between logical partitions using L2TP



Situation

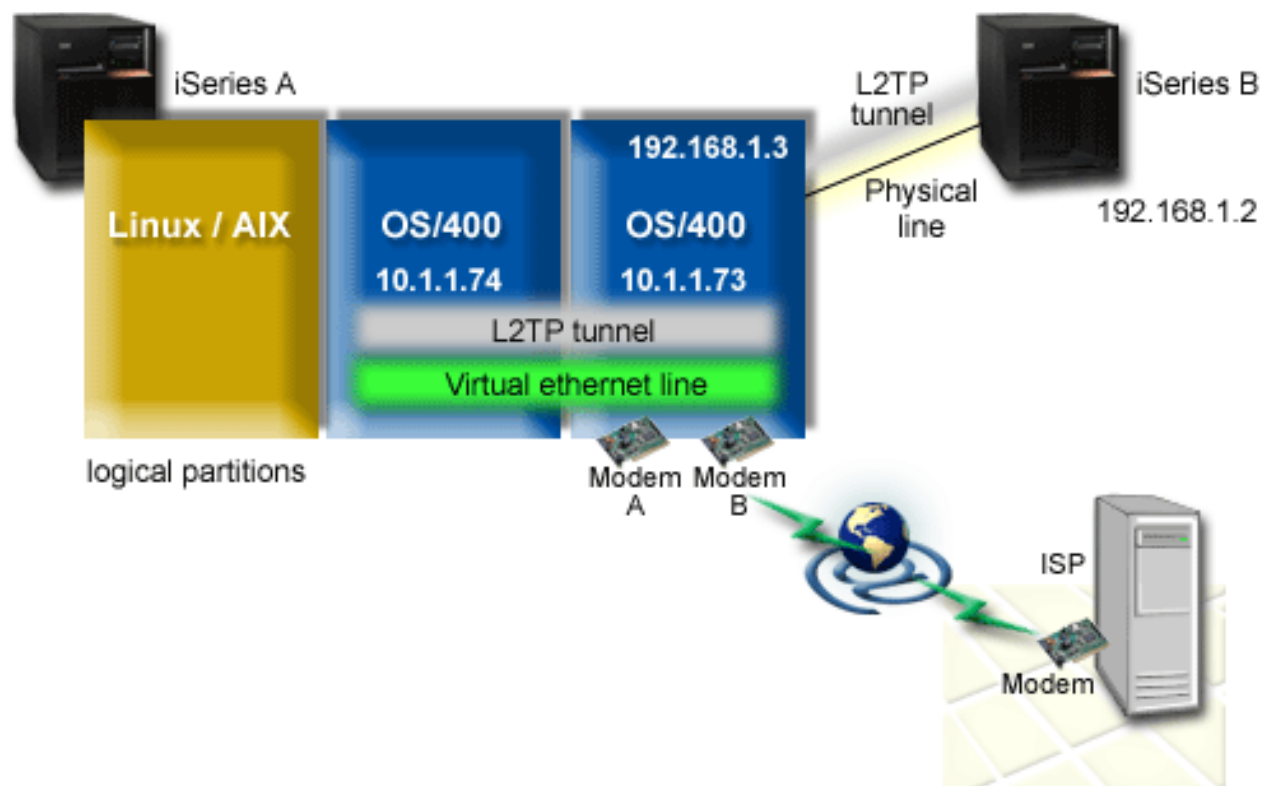
You are the system administrator at a medium sized company. It's time to update your computer equipment, but you'd like to do more than that; you want to streamline your hardware. You start the process by consolidating the work of three old servers onto one new iSeries server. You create three logical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



Prerequisites and assumptions

| Setup requirements for iSeries-A include:

- | • OS/400 Version 5 Release 3 or later, installed on the partition which owns the ASYNC capable modems
- | • Hardware which 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 which owns the modem must have OS/400 Version 5 Release 3 or later installed. The other partitions may have OS/400 V5R2 or V5R3, Linux, or AIX installed. In this scenario, the partitions are either using OS/400 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

| **Configuration steps**

| Complete these configuration tasks:

- | 1. Create a L2TP terminator profile for any interface on the partition which owns the modem
- | 2. Create a L2TP remote dial profile on 10.1.1.74
- | 3. Create a L2TP remote dial profile on 192.168.1.2
- | 4. Test the connection

| **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 dialog 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 outgoing 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 dialog, 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 dialog, 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 could 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 phone number of *PRIMARY or *BACKUP, the actual numbers dialed will be the ones specified here. If the other systems specify an actual phone number then the phone 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 could 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.

| **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**: toModem
 - | This line has no associated physical interface. The virtual line describes various characteristics of this PPP profile. The L2TP Line Properties dialog 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 phone numbers** field, add *PRIMARY and *BACKUP. This allows the profile to use the same phone 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 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-hand pane, find the desired 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-hand pane, find the desired 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-hand 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 desired server (such as 10.1.1.73)--> **Network --> Remote Access Services-->Originator Connection Profiles**.
 - | b. In the right-hand 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 responsibility of the user 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 give 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 49XA
| 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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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.

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

Trademarks

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

e (logo)Server
IBM
iSeries
Operating System/400
OS/400
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.

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

Terms and conditions for downloading and printing publications

- | Permissions for the use of the information you have selected for download are granted subject to the following terms and conditions and your indication of acceptance thereof.
- | **Personal Use:** You may reproduce this information for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of this information, or any portion thereof, without the express consent of IBM.
- | **Commercial Use:** You may reproduce, distribute and display this information solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of this information, or reproduce, distribute or display this information 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 information or any 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 information 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 THIS INFORMATION. THE INFORMATION IS 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.

All material copyrighted by IBM Corporation.

- | By downloading or printing information from this site, you have indicated your agreement with these terms and conditions.



Printed in USA