IBM

@server

iSeries

Networking
TCP/IP setup

Version 5 Release 3

IBM

@server

iSeries

Networking
TCP/IP setup

Version 5 Release 3

> **Note**
>
> Before using this information and the product it supports, be sure to read the information in "Notices," on page 57.

Contents

Part 1. TCP/IP setup

Your server has arrived, and you are ready to put it to use. This topic provides tools and procedures for configuring TCP/IP on OS/400®. For example, you can use this information to create a line description, a TCP/IP interface, and a route. Find out how to customize your TCP/IP configuration using iSeries™ Navigator, and learn about various TCP/IP techniques that enable you to direct the data that flows in and out of your network.

Before you use this information to configure TCP/IP, see Hardware installation and use to ensure you have installed all the necessary hardware components. After you complete the initial tasks for configuring TCP/IP, you are ready to expand the capabilities of your server with TCP/IP applications, protocols, and services to meet your unique needs.

What's new for V5R3
Find out about new and changed TCP/IP function.

Print this topic
Use this topic to print or download a Portable Document Format (PDF) version of the TCP/IP setup documentation.

Internet Protocol version 6 (IPv6)
The new Internet Protocol, IPv6, plays a key role in the future of the Internet, and you can use IPv6 on the iSeries server. This topic provides general information about IPv6 and how it is being implemented on the iSeries server.

Plan TCP/IP setup
This topic helps you prepare for installation and configuration of TCP/IP on the iSeries server. Basic requirements for the installation and configuration are provided so that you have all the necessary information at hand when you begin configuring TCP/IP. References to related terms and concepts are provided.

Install TCP/IP
This topic guides you through the installation of products that prepare your iSeries server for operation.

Configure TCP/IP
This topic shows you how to engage your iSeries and configure TCP/IP. In addition, see instructions for configuring IPv6.

Customize TCP/IP with iSeries Navigator
This topic provides customizing options by using iSeries Navigator.

TCP/IP techniques over virtual Ethernet
Find out how to take advantage of virtual Ethernet on OS/400.

Troubleshoot TCP/IP
If you encounter any problems with TCP/IP connections or traffic, see TCP/IP troubleshooting to help you find the solutions. This troubleshooting guide helps you solve problems related to both IPv4 and IPv6.

Related information for TCP/IP setup
This topic answers the question, "What more can it do?" Find references to services and applications that enhance your server's performance.

Chapter 1. What's new for V5R3

Enhancements to TCP/IP setup

If you are using a virtual Ethernet network to allow your partitions to communicate with one another, you may need to extend that communication to an external, physical LAN. See TCP/IP techniques connecting virtual Ethernet to external LANs to learn how to connect your virtual Ethernet network to an external LAN. Use this information to review examples illustrating three different methods for bridging your network traffic from the virtual Ethernet network to an external LAN.

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

How to see what's new or changed

To help you see where technical changes have been made, this information uses:
- The ≫ image to mark where new or changed information begins.
- The ≪ image to mark where new or changed information ends.

Chapter 2. Print this topic

To view or download the PDF version of this document, select TCP/IP setup (about 362 KB).

Other information

You can also view or print any of the following PDFs:
*   Manuals:

    –   **TCP/IP Configuration and Reference** (592 KB)
        This book provides information on configuring Transmission Control Protocol/Internet Protocol (TCP/IP) and operating and managing your network.

    –   **Tips and Tools for Securing your iSeries** (1 MB)
        This book provides basic recommendations for using the security features of the iSeries to protect your server and its associated operations.
*   Redbooks™:

    –   **TCP/IP Tutorial and Technical Overview** (7 MB)
        This redbook provides information on the basics of TCP/IP.

    –   **TCP/IP for AS/400®: More Cool Things Than Ever** (9 MB)
        This redbook includes an extensive list of common TCP/IP applications and services.

Saving PDF files

To save a PDF on your workstation for viewing or printing:
1.   Right-click the PDF in your browser (right-click the link above).
2.   Click **Save Target As...** if you are using Internet Explorer. Click **Save Link As...** if you are using Netscape Communicator.
3.   Navigate to the directory in which you would like to save the PDF.
4.   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 3. Internet Protocol version 6 (IPv6)

Internet Protocol version 6 (IPv6) is the updated version of Internet Protocol version 4 (IPv4) and is gradually replacing IPv4 as the Internet standard.

You may wonder how you can use IPv6 to improve your company's e-business, or you may be a programmer who wants to create IPv6 applications so your firm can benefit from this enhanced Internet Protocol. Read these topics to find basic information about IPv6 and how to use IPv6 on the iSeries server:

What is IPv6?
Find out why IPv6 is replacing IPv4 as the Internet standard, and how you can use it to your advantage.

What IPv6 functions are available?
Learn how IPv6 is currently being implemented on the iSeries server.

IPv6 scenarios
See examples to help you understand situations in which you would use IPv6 for your business.

IPv6 concepts
Learn basic IPv6 concepts. If you aren't sure what the differences are between IPv4 and IPv6, see detailed comparisons, such as how the IPv4 and IPv6 addresses compare to one another, or how IPv4 packet headers differ from IPv6 packet headers.

Configure IPv6
Find hardware and software requirements and instructions for configuring IPv6 on the server.

Troubleshoot IPv6
Find solutions to IPv6 problems.

Related information for IPv6
Find links to resources that help you understand IPv6.

What is IPv6?

Internet Protocol version 6 (IPv6) is the next evolution in Internet Protocol. Most of the Internet currently uses IPv4, and this protocol has been reliable and resilient for over 20 years. However, IPv4 has severe limitations that are causing more problems as the Internet expands.

In particular, there is a growing shortage of IPv4 addresses, which are needed for all new devices added to the Internet. The key to IPv6 enhancement is the expansion of the IP address space from 32 bits to 128 bits, enabling virtually unlimited unique IP addresses. The new IPv6 address text format is:

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

where each x is a hexadecimal digit representing 4 bits.

The expanded addressing capability of IPv6 provides a solution to the address depletion problem. This is especially important as more people use mobile computers, such as mobile telephones and handheld computers. The increasing demands of wireless users contribute to the depletion of IPv4 addresses. The expanded IP address capability of IPv6 solves this problem by providing enough IP addresses for the growing number of wireless devices.

In addition to this addressing capability, IPv6 provides new functions that simplify the tasks of configuring and managing the addresses on the network. Configuring and maintaining networks is a labor intensive activity. IPv6 reduces some of the workload by automating several of the network administrator's tasks.

If you use IPv6, you will not have to renumber your device addresses when you change to a different Internet Service Provider (ISP). You can keep the same addresses because they are globally unique addresses.

The IPv6 autoconfiguration feature automatically configures interface and router addresses for you. In stateless autoconfiguration, IPv6 takes the machine's MAC address and a network prefix provided by a local node and combines these two addresses to create a new, unique IPv6 address. This feature eliminates the need for a DHCP server, which saves time for the administrator and saves money for your company.

For more information sources about IPv6, see Related information for IPv6

See What IPv6 functions are available? for IPv6 information related specifically to the iSeries server.

What IPv6 functions are available?

IBM® is implementing IPv6 for the iSeries server over several software releases. IPv6 is currently implemented in an application development platform for the purpose of developing and testing IPv6 applications. IPv6 functions are transparent to existing TCP/IP applications and coexist with IPv4 functions.

These are the main iSeries server functions that are affected by IPv6:

- **Configuration**
  Be aware that the configuration process for IPv6 is different from the process for IPv4. To use the IPv6 function, you must change the server's TCP/IP configuration by configuring a line for IPv6. You may configure IPv6 on an Ethernet line or on a tunnel line.

  If you configure an Ethernet line for IPv6 traffic, you are sending IPv6 packets over an IPv6 network. See Create an IPv6 local area network (LAN) for a scenario that describes a situation in which you would configure an Ethernet line for IPv6.

  If you configure tunnel lines, you are sending IPv6 packets over an existing IPv4 network. See Send IPv6 packets over an IPv4 local area network (LAN) and Send IPv6 packets over an IPv4 wide area network (WAN) for scenarios that describe two situations in which you would create a configured tunnel line for IPv6.

  See Configure IPv6 to configure your network for IPv6.

- **Sockets**
  Develop and test sockets applications using IPv6 APIs and tools. IPv6 enhances sockets so that applications can use IPv6 using a new address family: AF_INET6. These enhancements do not affect existing IPv4 applications. You may create applications that support concurrent IPv4 and IPv6 traffic or IPv6-only traffic. See Use AF_INET6 address family for more information on IPv6 for sockets.

- **DNS**
  Domain Name System (DNS) supports AAAA addresses and a new domain for reverse lookups: IP6.ARPA. While it is true that DNS retrieves IPv6 information, the server must use IPv4 to communicate with the DNS.

- **Troubleshoot TCP/IP**
  Use standard troubleshooting tools such as PING, netstat, trace route and communications trace for IPv6 networks and tunnels. These tools now support the IPv6 address format. See TCP/IP troubleshooting to solve problems for both IPv4 and IPv6 networks.

See Related information for IPv6 for resources on IPv6.

Scenarios: IPv6

Review the following scenarios to understand why you would implement IPv6 and how to set up your network in each of these situations:

- Create an IPv6 local area network (LAN)
- Send IPv6 packets over an IPv4 local area network (LAN)
- Send IPv6 packets over an IPv4 wide area network (WAN)

Note: In the scenarios, the IP addresses 10.x.x.x represent public IP addresses. All addresses used in these scenarios are for example purposes only.

See Configure IPv6 to configure your server for IPv6.

See IPv6 concepts for definitions of basic IPv6 concepts.

Create an IPv6 local area network (LAN)

Situation

IPv6 will eventually replace IPv4 as the Internet standard. Consequently, your company decides to implement IPv6 for its financial operations and purchases a new accounting application that uses IPv6 for connectivity. The application needs to connect to another instance of the application that is located on a different server connected to the site Ethernet local area network (LAN). Your job is to configure your server for IPv6 so that your firm may start using the accounting application. The following figure illustrates the network setup in this scenario.
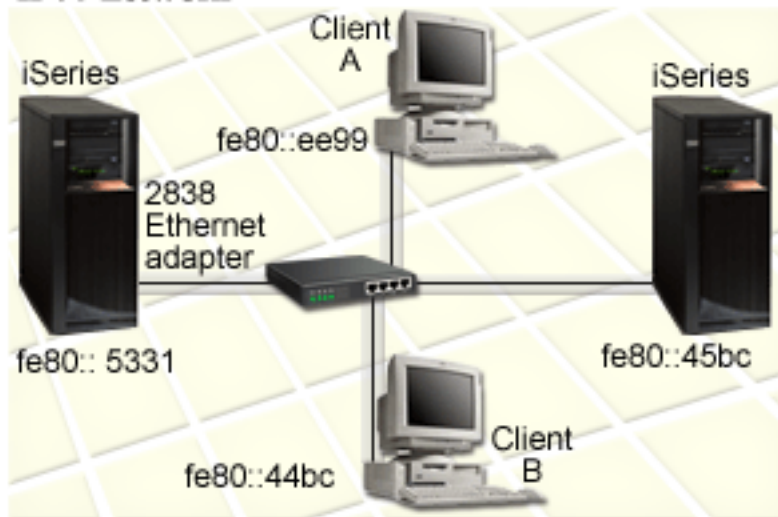
Solution

To create an IPv6 LAN, you must configure an Ethernet line description for IPv6. IPv6 packets travel between iSeries servers and clients on the network as employees use the accounting application.

Setup requirements include:

- OS/400 Version 5 Release 2 or later
- 2838 or 2849 Ethernet adapters, as these are the only types of hardware resources currently supported for IPv6.
- iSeries Access for Windows® and iSeries Navigator (Network component of iSeries Navigator)
- The server must have a separate IPv4 physical interface configured before you configure the Ethernet line for IPv6 because TCP/IP must be running on your server. If you have not configured the server for IPv4, see Configure TCP/IP for the first time before configuring the line for IPv6.

Configuration

To configure an Ethernet line description for IPv6, you must use the **IPv6 Configuration** wizard in iSeries Navigator. IPv6 may only be configured from iSeries Navigator, and may not be configured from the character-based interface.

The wizard requires the name of the hardware communications resource on the server on which you will configure IPv6; for example, CMN01. This must be either a 2838 or 2849 Ethernet adapter that is not currently configured for IPv4.

To use the **IPv6 Configuration** wizard, follow these steps:

1. In iSeries Navigator, select your **server —> Network —> TCP/IP Configuration**.
2. Right-click **IPv6**, select **IPv6 Configuration**, and follow the wizard's instructions to configure an Ethernet line for IPv6.

Send IPv6 packets over an IPv4 local area network (LAN)

Situation

Your firm has written a new IPv6 accounting application. This is a server-to-client application that you will use locally. The application communicates with other instances of itself that are located at the same site, but in other buildings and LANs. Although your firm wants to use IPv6 for this application, it is not ready to change its entire IPv4 infrastructure to IPv6. Your job is to configure IPv6 tunnel lines that allow IPv6 packets to run over the local IPv4 networks. The following figure illustrates the network setup in this scenario.

Accounts Receivable
IPv4 network
Building 1

iSeries A

Client A

Client B

10.1.1.1
fec0:: 1

IPv4 Router
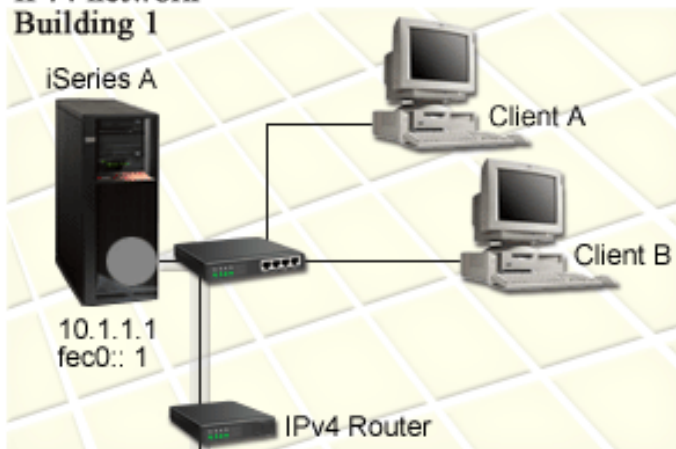
Red configured tunnel
Local endpoint = 10.1.1.1
Remote endpoint = 10.1.2.1
Local IPv6 address = fec0::1

Blue configured tunnel
Local endpoint = 10.1.1.1
Remote endpoint = 10.1.2.2
Local IPv6 address = fec0::1

Accounts Payable
IPv4 network
Building 2

10.1.2.1
fec0::2

Client C

IPv4 Router

Client D

10.1.2.2
fec0::3
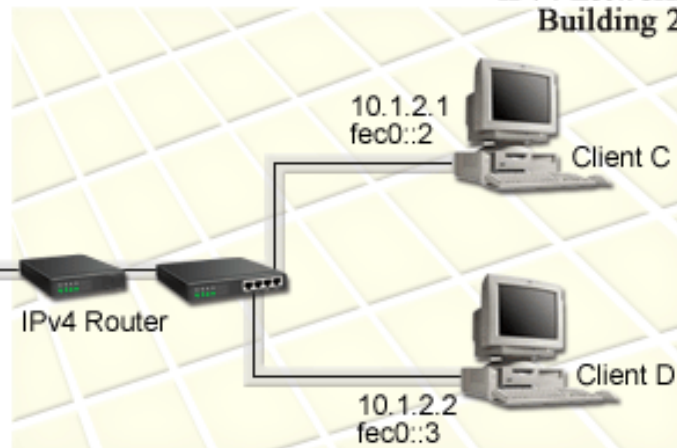
Solution

To use IPv6 over these local IPv4 networks, you must create two configured tunnels and several associated routes. One tunnel is depicted in red and the other tunnel is depicted in blue, for example purposes.

First, consider the red tunnel:
- The red tunnel begins at iSeries A (local endpoint 10.1.1.1) in Building 1 and ends at Client C (remote endpoint 10.1.2.1) in Building 2.
- iSeries A encapsulates an IPv6 packet within an IPv4 packet and sends the IPv4 packet over the tunnel to Client C, which decapsulates the IPv6 packet so it may connect to another instance of the IPv6 application.

Next, consider the blue tunnel:
- The blue tunnel begins at iSeries A (local endpoint 10.1.1.1) in Building 1, like the red tunnel; however, the blue tunnel ends at Client D (remote endpoint 10.1.2.2) in Building 2.
- iSeries A encapsulates an IPv6 packet within an IPv4 packet and sends the IPv4 packet over the tunnel to Client D, which decapsulates the IPv6 packet so it may connect to another instance of the IPv6 application.

Each tunnel connection is point-to-point, so you must define a remote endpoint for each tunnel. This is accomplished by creating two routes. Each route is associated to the same tunnel line, but defines a different remote endpoint as the next hop. In other words, you define the remote endpoints of each tunnel as you create the routes.

In addition to creating the initial routes that define the tunnel endpoints and permit the packets to reach the clients in Building 2, you must create two more routes so the packets may return to the server in Building 1.

Setup requirements include:
- OS/400 Version 5 Release 2 or later
- iSeries Access for Windows and iSeries Navigator (Network component of iSeries Navigator)
- TCP/IP (using IPv4) must be configured on the server before you create the configured tunnel line. If you have not configured the server for IPv4, see Configure TCP/IP for the first time before configuring the tunnel line for IPv6.

Configuration

To create a configured tunnel line, you must use the **IPv6 Configuration** wizard and the **New IPv6 Route** wizard in iSeries Navigator. IPv6 may only be configured from iSeries Navigator, and may not be configured from the character-based interface.

To use the **IPv6 Configuration** wizard to create the red tunnel line, follow these steps:
1. In iSeries Navigator, select your **server —> Network —> TCP/IP Configuration**.
2. Right-click **IPv6**, select **IPv6 Configuration** wizard, and follow the wizard's instructions to configure a tunnel line for IPv6. After you complete the **IPv6 Configuration** wizard, it prompts you to create a new route for the configured tunnel line, and the **New IPv6 Route** wizard dialog will appear. You must create a new route to permit IPv6 packets to travel through the red tunnel.
3. From the **New IPv6 Route** wizard, create a route for the red tunnel. Specify the remote endpoint 10.1.2.1 as the next hop and specify fec0::2 as the destination address.

Use the **New IPv6 Route** wizard again to create a route for the blue tunnel. Note that it is not necessary to create the blue tunnel using the **IPv6 Configuration** wizard. The blue tunnel is created when you define its remote endpoint using the **New IPv6 Route** wizard. To use the **New IPv6 Route** wizard, follow these steps:
1. In iSeries Navigator, select your **server —> Network —> TCP/IP Configuration —> IPv6**.
2. Right-click **Routes**, select **New Route**, and follow the wizard's instructions to configure an IPv6 route for the blue tunnel. Specify the remote endpoint 10.1.2.2 as the next hop and specify fec0::3 as the destination address.

After you create the configured tunnel lines and the routes that define the tunnel endpoints, you must create a route on Client C and a route on Client D that permit the packets to travel back to the server in Building 1. For each of these routes, you should specify 10.1.1.1 as the next hop and specify fec0::1 as the destination address.

Send IPv6 packets over an IPv4 wide area network (WAN)

Situation

Your firm uses an accounting application for accounts receivable on the server in its Chicago office. You need to connect the application to a server in the Dallas office. This application uses IPv6 addressing on the servers in both cities. Because your ISP cannot provide IPv6 routers between your two sites, you need

to configure a tunnel between your two servers. The application packets travel through the tunnel, across the IPv4 wide area network between your two servers. The following figure illustrates the network setup in this scenario.

Note: In this scenario, the IP addresses 10.x.x.x represent public IP addresses that can be globally routed. All addresses used are for example purposes only.
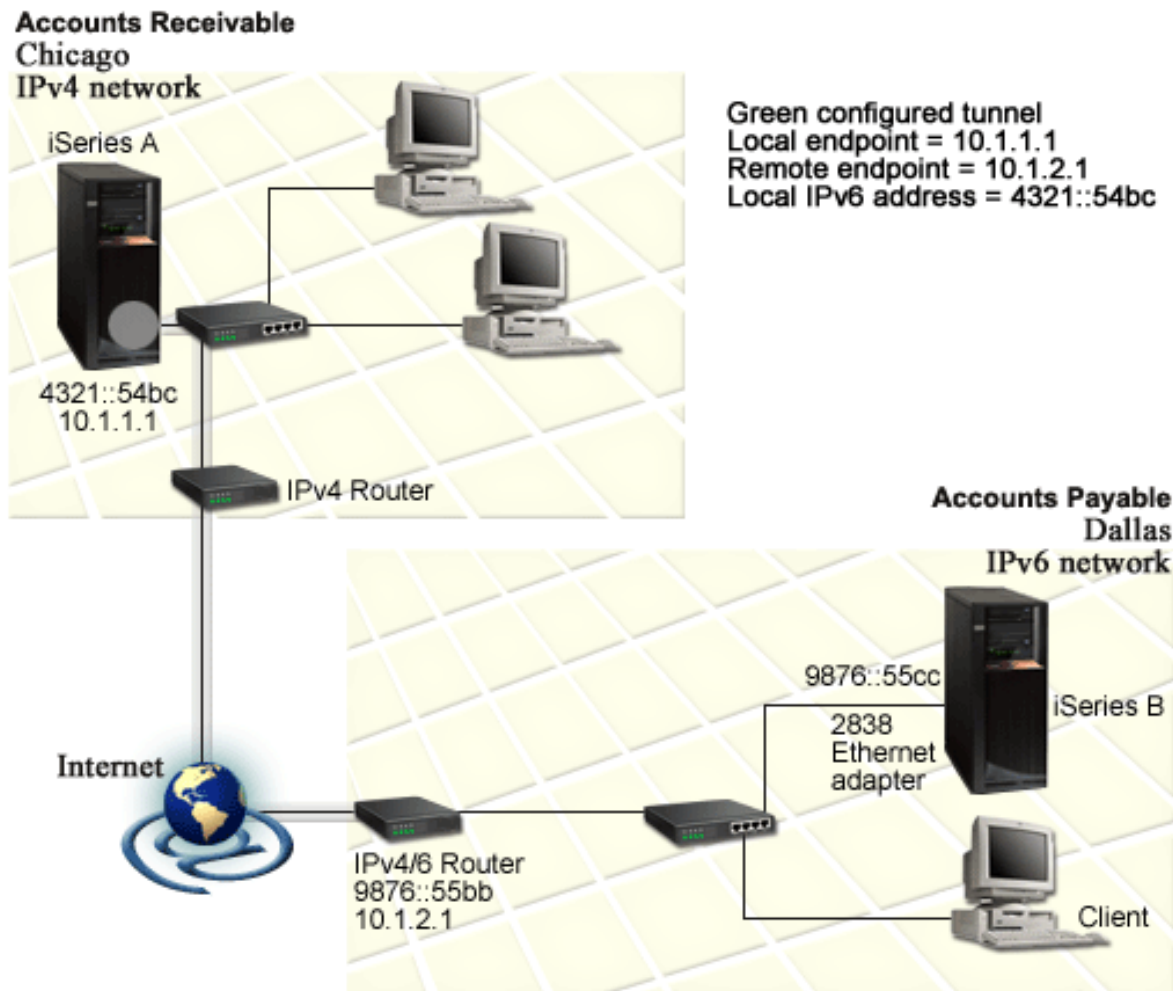
Solution

To use IPv6 across a wide area network that consists of an IPv4 infrastructure, you must create a configured tunnel line and several associated routes. This is how it works:

*   The tunnel begins at iSeries A (local endpoint 10.1.1.1) in Chicago and ends at the IPv4/6 router (remote endpoint 10.1.2.1) in Dallas.
*   The application that resides on iSeries A needs to connect to the application that resides on iSeries B. iSeries A encapsulates the IPv6 packet within an IPv4 packet and sends it over the tunnel to the IPv4/6 router, which decapsulates the IPv6 packet and forwards the IPv6 packet to iSeries B.
*   The packet returns to Chicago by taking the reverse path.

The tunnel connection is point-to-point, so you must define the remote endpoint of the tunnel. This is accomplished by creating a route that is associated with this tunnel line. The route defines the remote

endpoint (10.1.2.1) as the next hop. In other words, you define the remote endpoint as you create the route. In addition, the route defines the destination address as 9876::55cc (the IPv6 address associated with iSeries B).

In addition to creating the initial route that defines the tunnel endpoint and permits the packet to travel to iSeries B in Dallas, you must create two more routes so the packet may return to iSeries A in Chicago.

Setup requirements include:
* OS/400 Version 5 Release 2 or later
* iSeries Access for Windows and iSeries Navigator (Network component of iSeries Navigator)
* TCP/IP (using IPv4) must be configured on the server before you create the configured tunnel line. If you have not configured the server for IPv4, see Configure TCP/IP for the first time before configuring the tunnel line for IPv6.

Configuration

To create a configured tunnel line, you must use the **IPv6 Configuration** wizard and the **New IPv6 Route** wizard in iSeries Navigator. Configured tunnels may only be configured from iSeries Navigator, and may not be configured from the character-based interface.

To use the **IPv6 Configuration** wizard to create the tunnel line, follow these steps:
1. In iSeries Navigator, select your **server —> Network —> TCP/IP Configuration**.
2. Right-click **IPv6**, select **IPv6 Configuration**, and follow the wizard's instructions to configure a tunnel line for IPv6. After you complete the **IPv6 Configuration** wizard, it prompts you to create a new route for the configured tunnel line, and the **New IPv6 Route** wizard dialog will appear. You must create a new route to allow IPv6 packets to travel through the tunnel.
3. From the **New IPv6 Route** wizard, create a host route for the tunnel. Specify the remote endpoint 10.1.2.1 as the next hop and specify 9876::55cc as the destination address.

After you create the configured tunnel line and the route that defines the tunnel endpoint, you must create routes on iSeries B and on the IPv4/6 router that permit the packets to travel back to Chicago. For the route on iSeries B, you should specify 9876::55bb as the next hop and 4321::54bc as the destination address. For the route on the IPv4/6 router, you should specify 10.1.1.1 as the next hop and 4321::54bc as the destination address.

Note: The IPv4/6 router in Dallas should have a direct route to 9876::55cc, but since this route is created automatically no manual configuration is necessary.

Concepts: IPv6

Read descriptions of these IPv6 concepts to better understand how IPv6 works:

Compare IPv4 to IPv6
Find out how IPv4 attributes compare to IPv6 attributes. This table allows you to quickly look up specific functions and compare their usage in each Internet protocol.

IPv6 address formats
Find out about the size and format of the IPv6 address.

IPv6 address types
Find out about new types of addresses within the scope of IPv6.

IPv6 tunneling
Find out how IPv6 tunneling allows IPv6 packets to travel over an IPv4 network.

Neighbor discovery
Find out how neighbor discovery allows hosts and routers to communicate with one another.

Stateless address autoconfiguration
Find out how stateless address autoconfiguration automates some of the network administrator's tasks.

IPv6 address formats

The IPv6 address size is 128 bits. The preferred IPv6 address representation is:
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where each x is a hexadecimal digit representing 4 bits. IPv6 addresses range from 0000:0000:0000:0000:0000:0000:0000:0000 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

In addition to this preferred format, IPv6 addresses may be specified in two other shortened formats:
- **Omit leading zeros**
  Specify IPv6 addresses by omitting leading zeros. For example, IPv6 address 1050:0000:0000:0000:0005:0600:300c:326b may be written as 1050:0:0:0:5:600:300c:326b.
- **Double colon**
  Specify IPv6 addresses by using double colons (::) in place of a series of zeros. For example, IPv6 address ff06:0:0:0:0:0:0:c3 may be written as ff06::c3. Double colons may be used only once in an IP address.

An alternative format for IPv6 addresses combines the colon and dotted notation, so the IPv4 address may be embedded in the IPv6 address. Hexadecimal values are specified for the left-most 96 bits, and decimal values are specified for the right-most 32 bits indicating the embedded IPv4 address. This format ensures compatibility between IPv6 nodes and IPv4 nodes when you are working in a mixed network environment.

These two types of IPv6 addresses use this alternative format:
- **IPv4–mapped IPv6 address**
  This type of address is used to represent IPv4 nodes as IPv6 addresses. It allows IPv6 applications to communicate directly with IPv4 applications. For example, 0:0:0:0:0:ffff:192.1.56.10 and ::ffff:192.1.56.10/96 (shortened format).
- **IPv4–compatible IPv6 address**
  This type of address is used for tunneling. It allows IPv6 nodes to communicate across an IPv4 infrastructure. For example, 0:0:0:0:0:0:192.1.56.10 and ::192.1.56.10/96 (shortened format).

All of these formats are valid IPv6 address formats. Specify any one of these IPv6 address formats in iSeries Navigator.

IPv6 address types

IPv6 addresses are categorized into three basic types:

Unicast address
The unicast address specifies a single interface. A packet sent to a unicast address destination travels from one host to the destination host.

Three types of unicast addresses include:

Link-local address
Link-local addresses are designed for use on a single local link (local network). Link-local addresses are automatically configured on all interfaces. The prefix used for a link-local address is fe80::/10. Routers do not forward packets with a destination or source address containing a link-local address.

Site-local address

Site-local addresses are designed for use in a specific site. The prefix used for a site-local address is `fec0::/10`. Routers do not forward packets with a source address containing a site-local address outside of a specific site.

Global address

Global addresses are designed for use on any network. The prefix used for a global address begins with binary `001`.

Two special types of unicast addresses include:

Unspecified address

The unspecified address is `0:0:0:0:0:0:0:0` or may be abbreviated with two colons (`::`). The unspecified address indicates the absence of an address, and it may never be assigned to a host. It may be used by an IPv6 host that does not yet have an address assigned to it. For example, when the host sends a packet to discover an address from another node, the host uses the unspecified address as its source address.

Loopback address

The loopback address is `0:0:0:0:0:0:0:1` or may be abbreviated as `::1`. The loopback address is used by a node to send a packet to itself.

Anycast address

The anycast address specifies a set of interfaces, possibly at different locations, that all share a single address. A packet sent to an anycast address goes only to the nearest member of the group. The iSeries server does not currently support anycast addressing.

Multicast address

The multicast address specifies a set of interfaces, possibly at multiple locations. The prefix used for a multicast address is `ff`. If a packet is sent to a multicast address, one copy of the packet is delivered to each member of the group. The iSeries server currently provides basic support for multicast addressing. Multicast interface creation and application support are currently not supported.

IPv6 tunneling

IPv6 tunneling enables the iSeries server to connect to IPv6 nodes (hosts and routers) across IPv4 domains. Tunneling permits isolated IPv6 nodes or networks to communicate without changing the underlying IPv4 infrastructure. Tunneling allows IPv4 and IPv6 protocols to cooperate, and thereby provides a transitional method of implementing IPv6 while retaining IPv4 connectivity.

A tunnel consists of two dual-stack (IPv4 and IPv6) nodes on an IPv4 network. These dual-stack nodes are capable of processing both IPv4 and IPv6 communications. One of the dual-stack nodes on the edge of the IPv6 infrastructure inserts an IPv4 header in front of (encapsulates) each IPv6 packet that arrives and sends it as though it were normal IPv4 traffic, through existing links. IPv4 routers continue to forward this traffic. On the other side of the tunnel, another dual-stack node removes the extra IP header from the IPv6 packet (decapsulates) and routes it to the ultimate destination using standard IPv6.

IPv6 tunneling for the iSeries server runs over configured tunnel lines, which are virtual lines. Configured tunnel lines provide IPv6 communications to any node with a routable IPv4 address that supports IPv6 tunnels. These nodes may exist anywhere, that is, within the local IPv4 domain or within a remote domain.

Configured tunnel connections are point-to-point. To configure this type of tunnel line, you must specify the local tunnel endpoint (IPv4 address), such as `124.10.10.150`, and the local IPv6 address, such as `1080:0:0:0:8:800:200c:417a`. You must also create an IPv6 route to enable traffic to travel through the

tunnel. As you create the route, you will define one of the tunnel's remote endpoints (IPv4 address) as the route's next hop. You may configure an unlimited number of endpoints for an unlimited number of tunnels.

See Send IPv6 packets over an IPv4 local area network (LAN) and Send IPv6 packets over an IPv4 wide area network (WAN) for scenarios and figures that demonstrate IPv6 tunneling.

Neighbor discovery

Neighbor discovery functions are used by IPv6 nodes (hosts or routers) to discover the presence of other IPv6 nodes, to determine the link-layer addresses of nodes, to find routers that are capable of forwarding IPv6 packets, and to maintain a cache of active IPv6 neighbors. IPv6 nodes use these five Internet Control Message Protocol version 6 (ICMPv6) messages to communicate with other nodes:

Router solicitation
Hosts send these messages to request routers to generate router advertisements. A host sends an initial router solicitation when the host first becomes available on the network.

Router advertisement
Routers send these messages either periodically or in response to a router solicitation. The information provided by router advertisements are used by hosts to automatically create site-local interfaces, global interfaces, and associated routes. Router advertisements also contain other configuration information used by a host such as maximum transmission unit and hop limit.

Neighbor solicitation
Nodes send these messages to determine the link-layer address of a neighbor, or to verify that a neighbor is still reachable.

Neighbor advertisement
Nodes send these messages in response to a neighbor solicitation or as an unsolicited message to announce an address change.

Redirect
Routers use these messages to inform hosts of a better first hop for a destination.

See RFC 2461 for more information about neighbor discovery and router discovery. To view RFC 2461, see RFC Editor (http://www.rfc-editor.org/rfcsearch.html) .

Stateless address autoconfiguration

Stateless address autoconfiguration is the process that IPv6 nodes (hosts or routers) use to automatically configure IPv6 addresses for interfaces. The node builds various IPv6 addresses by combining an address prefix with either the MAC address of the node or a user-specified interface identifier. The prefixes include the link-local prefix (`fe80::/10`) and prefixes of length 64 advertised by local IPv6 routers (if any exist). Stateless address autoconfiguration also creates appropriate multicast interfaces when the link-type is multicast-capable.

The node performs duplicate address detection to verify the uniqueness of the address before assigning it to an interface. The node sends out a neighbor solicitation query to the new address and waits for a response. If the node does not receive a response, then the address is assumed to be unique. If the node receives a response in the form of a neighbor advertisement, the address is already in use. If a node determines that its tentative IPv6 address is not unique, then autoconfiguration stops and manual configuration of the interface is required.

Compare IPv4 to IPv6

IBM is implementing IPv6 for the iSeries server over several software releases. IPv6 is currently implemented in an application development platform for the purpose of developing and testing IPv6 applications.

You may be wondering how the details of IPv6 differ from IPv4. This table allows you to quickly glance at familiar attributes associated with IPv4 and compare them to similar attributes in IPv6. Select an attribute from this list to link to the comparison in the table.

- "virtual private networking (VPN)" on page 23

	IPv4	IPv6
address	32 bits long (4 bytes). Address is composed of a network and a host portion, which depend on address class. Various address classes are defined: A, B, C, D, or E depending on initial few bits. The total number of IPv4 addresses is 4 294 967 296. The text form of the IPv4 address is nnn.nnn.nnn.nnn, where 0<=nnn<=255, and each n is a decimal digit. Leading zeros may be omitted. Maximum number of print characters is 15, not counting a mask.	128 bits long (16 bytes). Basic architecture is 64 bits for the network number and 64 bits for the host number. Often, the host portion of an IPv6 address (or part of it) will be a MAC address or other interface identifier. Depending on the subnet prefix, IPv6 has a more complicated architecture than IPv4. The number of IPv6 addresses is 10^{28} (79 228 162 514 264 337 593 543 950 336) times <u>larger</u> than the number of IPv4 addresses.The text form of the IPv6 address is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where each x is a hexadecimal digit, representing 4 bits. Leading zeros may be omitted. The double colon (::) may be used once in the text form of an address, to designate any number of 0 bits. For example, ::ffff:10.120.78.40 is an IPv6 IPv4-mapped address. (See RFC 2373 for details. To view this RFC, see RFC Editor (http://www.rfc-editor.org/rfcsearch.html).
address allocation	Originally, addresses were allocated by network class. As address space is depleted, smaller allocations using Classless Inter-Domain Routing (CIDR) are made. Allocation has not been balanced among institutions and nations.	Allocation is in the earliest stages. The Internet Engineering Task Force (IETF) and Internet Architecture Board (IAB) have recommended that essentially every organization, home, or entity be allocated a /48 subnet prefix length. This would leave 16 bits for the organization to do subnetting. The address space is large enough to give every person in the world their own /48 subnet prefix length.
address lifetime	Generally, not an applicable concept, except for addresses assigned using DHCP.	IPv6 addresses have two lifetimes: preferred and valid, with the preferred lifetime always <= valid. After the preferred lifetime expires, the address is not to be used as a source IP address. After the valid lifetime expires, the address is not used (recognized) as a valid destination IP address for incoming packets. Some IPv6 addresses have, by definition, infinite preferred and valid lifetimes; for example link-local (see "address scope").
address mask	Used to designate network from host portion.	Not used (see "address prefix").
address prefix	Sometimes used to designate network from host portion. Sometimes written as /nn suffix on presentation form of address.	Used to designate the subnet prefix of an address. Written as /nnn (up to 3 decimal digits, 0 <= nnn <= 128) suffix after the print form. An example is fe80::982:2a5c/10, where the first 10 bits comprise the subnet prefix.
Address Resolution Protocol (ARP)	Address Resolution Protocol is used by IPv4 to find a physical address, such as the MAC or link address, associated with an IPv4 address.	IPv6 embeds these functions within IP itself as part of the algorithms for stateless autoconfiguration and neighbor discovery using Internet Control Message Protocol version 6 (ICMPv6). Hence, there is <u>no</u> such thing as ARP6.
address scope	For unicast addresses, the concept does not apply. There are designated private address ranges and loopback. Outside of that, addresses are assumed to be global.	In IPv6, address scope is part of the architecture. Unicast addresses have 3 defined scopes, including link-local, site-local and global; and multicast addresses have 14 scopes. Default address selection for both source and destination takes scope into account. A scope zone is an instance of a scope in a particular network. As a consequence, IPv6 addresses sometimes have to be entered or associated with a zone ID. The syntax is %zid where zid is a number (usually small) or a name. The zone ID is written after the address and before the prefix. For example, 2ba::1:2:14e:9a9b:c%3/48.
address types	Unicast, multicast, and broadcast.	Unicast, multicast, and anycast. See IPv6 address types for descriptions.
communications trace	A tool to collect a detailed trace of TCP/IP (and other) packets that enter and leave an iSeries server.	Same for IPv6, and IPv6 is supported, including ICMPv6 and IPv6 packets tunneled in IPv4.

	IPv4	IPv6
configuration	Configuration must be done on a newly installed system before it can communicate; that is, IP addresses and routes must be assigned.	Configuration is optional, depending on functions required. An appropriate Ethernet or tunnel interface must be designated as an IPv6 interface, using iSeries Navigator. Once that is done, IPv6 interfaces are self-configuring. So, the system will be able to communicate with other IPv6 systems that are local and remote, depending on the type of network and whether an IPv6 router exists.
Domain Name System (DNS)	Applications accept host names and then use DNS to get an IP address, using socket API gethostbyname(). Applications also accept IP addresses and then use DNS to get host names using gethostbyaddr(). For IPv4, the domain for reverse lookups is in-addr.arpa.	Same for IPv6. Support for IPv6 exists using AAAA (quad A) record type and reverse lookup (IP-to-name). An application may elect to accept IPv6 addresses from DNS (or not) and then use IPv6 to communicate (or not). The socket API gethostbyname() is unchanged for IPv6 and the getaddrinfo() API can be used to obtain (at application choice) IPv6 only, or IPv4 and IPv6 addresses. For IPv6, the domain used for reverse nibble lookups is ip6.arpa, and if not found then ip6.int (see API getnameinfo()).
Dynamic Host Configuration Protocol (DHCP)	Used to dynamically obtain an IP address and other configuration information.	Currently, DHCP does not support IPv6.
File Transfer Protocol (FTP)	File Transfer Protocol allows you to send and receive files across networks.	Currently, FTP does not support IPv6.
fragments	When a packet is too big for the next link over which it is to travel, it can be fragmented by the sender (host or router).	For IPv6, fragmentation can only occur at the source node, and reassembly is only done at the destination node. Currently, the fragmentation extension header is not supported.
host table	On iSeries Navigator, a configurable table that associates an Internet address with a host name; for example, 127.0.0.1, loopback. This table is used by the sockets name resolver, either before a DNS lookup or after a DNS lookup fails (determined by host name search priority).	Currently, this table does not support IPv6. Customers need to configure a AAAA record in a DNS for IPv6 domain resolution. You may run the DNS locally on the same system as the resolver, or you may run it on a different system.
interface	The conceptual or logical entity used by TCP/IP to send and receive packets and always closely associated with an IPv4 address, if not named with an IPv4 address. Sometimes referred to as a logical interface. Can be started and stopped independently of each other and independently of TCP/IP using STRTCPIFC and ENDTCPIFC commands and using iSeries Navigator.	Same concept as IPv4. Can be started and stopped independently of each other and independently of TCP/IP using iSeries Navigator only.
Internet Control Message Protocol (ICMP)	ICMP is used by IPv4 to communicate network information.	Used similarly for IPv6; however, Internet Control Message Protocol version 6 (ICMPv6) provides some new attributes. Basic error types remain, such as destination unreachable, echo request and reply. New types and codes are added to support neighbor discovery and related functions.
Internet Group Management Protocol (IGMP)	IGMP is used by IPv4 routers to find hosts that want traffic for a particular multicast group, and used by IPv4 hosts to inform IPv4 routers of existing multicast group listeners (on the host).	Replaced by MLD (multicast listener discovery) protocol for IPv6. Does essentially what IGMP does for IPv4, but uses ICMPv6 by adding a few MLD-specific ICMPv6 type values.
IP header	Variable length of 20-60 bytes, depending on IP options present.	Fixed length of 40 bytes. There are no IP header options. Generally, the IPv6 header is simpler than the IPv4 header.
IP header options	Various options that may accompany an IP header (before any transport header).	The IPv6 header has no options. Instead, IPv6 adds additional (optional) extension headers. The extension headers are AH and ESP (unchanged from IPv4), hop-by-hop, routing, fragment, and destination. Currently, IPv6 does not support any extension headers.

	IPv4	IPv6
IP header protocol byte	The protocol code of the transport layer or packet payload; for example, ICMP.	The type of header immediately following the IPv6 header. Uses the same values as the IPv4 protocol field. But the architectural effect is to allow a currently defined range of next headers, and is easily extended. The next header will be a transport header, an extension header, or ICMPv6.
IP header Type of Service (TOS) byte	Used by QoS and differentiated services to designate a traffic class.	Designates the IPv6 traffic class, similarly to IPv4. Uses different codes. Currently, IPv6 does not support TOS.
iSeries Navigator support	iSeries Navigator provides a full configuration function for TCP/IP.	The optional configuration for IPv6 is provided in full by iSeries Navigator, including the **IPv6 Configuration** wizard.
LAN connection	Used by an IP interface to get to the physical network. Many types exist; for example, token ring, Ethernet, and PPP. Sometimes referred to as the physical interface, link, or line.	IPv6 has the same concept. Currently, only the 2838 and 2849 Ethernet cards and tunnel lines are supported.
Layer 2 Tunnel Protocol (L2TP)	L2TP can be thought of as virtual PPP, and works over any supported line type.	Currently, L2TP does not support IPv6.
loopback address	An interface with address of 127.*.*.* (typically 127.0.0.1) that can only be used by a node to send packets to itself. The physical interface (line description) is named *LOOPBACK.	The concept is the same as in IPv4, and the single loopback address is 0000:0000:0000:0000:0000:0000:0000:0001 or ::1 (shortened version). The virtual physical interface is named *LOOPBACK6.
Maximum Transmission Unit (MTU)	Maximum transmission unit of a link is the maximum number of bytes that a particular link type, such as Ethernet or modem, supports. For IPv4, 576 is the typical minimum.	IPv6 has an architected lower bound on MTU of 1280 bytes. That is, IPv6 will not fragment packets below this limit. To send IPv6 over a link with less than 1280 MTU, the link-layer must transparently fragment and defragment the IPv6 packets.
netstat	A tool to look at status of TCP/IP connections, interfaces, or routes. Available using iSeries Navigator and 5250.	Same for IPv6, and IPv6 is supported for both 5250 and iSeries Navigator.
Network Address Translation (NAT)	Basic firewall functions integrated into TCP/IP, configured using iSeries Navigator.	Currently, NAT does not support IPv6. More generally, IPv6 does not require NAT. The expanded address space of IPv6 eliminates the address shortage problem and enables easier renumbering.
network table	On iSeries Navigator, a configurable table that associates a network name with an IP address without mask. For example, host Network14 and IP address 1.2.3.4.	Currently, no changes are made to this table for IPv6.
node info query	Does not exist.	A simple and convenient network tool that should work like ping, except with content: an IPv6 node may query another IPv6 node for the target's DNS name, IPv6 unicast address, or IPv4 address. Currently, not supported.
packet filtering	Basic firewall functions integrated into TCP/IP, configured using iSeries Navigator.	Currently, packet filtering does not support IPv6. However, IPv4 filtering can be applied to tunneled IPv6 traffic.
packet forwarding	The iSeries server can be configured to forward IP packets it receives for nonlocal IP addresses. Typically, the inbound interface and outbound interface are connected to different LANs.	Currently, IPv6 packets are not forwarded.
packet tunneling	In IPv4, tunneling occurs in VPN for tunnel-mode VPN connections (IPv4 tunneled in IPv4) and in L2TP.	For IPv6, tunneling in IPv4 packets is expected to be a major part of its evolution. Currently, at least 5 different types of 6-in-4 tunneling are defined by IETF, each with different attributes and advantages. A basic and flexible type of IPv6-in-IPv4 tunneling is supported to allow IPv6 nodes to communicate across the existing IPv4 Internet. Called **configured tunneling**, it provides a virtual point-to-point link between two IPv6 nodes and uses a new type of tunnel line called *TNLCFG64.
PING	Basic TCP/IP tool to test reachability. Available using iSeries Navigator and 5250.	Same for IPv6, and IPv6 is supported, for both 5250 and iSeries Navigator.
Point-to-Point Protocol (PPP)	PPP supports dial-up interfaces over various modem and line types.	Currently, PPP does not support IPv6.

	IPv4	IPv6
port restrictions	These iSeries panels allow a customer to configure selected port number or port number ranges for TCP or UDP so that they are only available for a specific profile.	Not supported for IPv6. Configured restrictions apply only to IPv4.
ports	TCP and UDP have separate port spaces, each identified by port numbers in the range 1-65535.	For IPv6, ports work the same as IPv4. Because these are in a new address family, there are now four separate port spaces. For example, there are two TCP port 80 spaces to which an application can bind, one in AF_INET and one in AF_INET6.
private and public addresses	All IPv4 addresses are public, except for three address ranges that have been designated as private by IETF RFC 1918: 10.*.*.* (10/8), 172.16.0.0 through 172.31.255.255 (172.16/12) , and 192.168.*.* (192.168/16). Private address domains are commonly used within organizations. Private addresses cannot be routed across the Internet.	IPv6 has an analogous concept, but with important differences. Addresses are public or temporary, previously termed anonymous. See RFC 3041. Unlike IPv4 private addresses, temporary addresses can be globally routed. The motivation is also different; IPv6 temporary addresses are meant to shield the identity of a client when it initiates communication (a privacy concern). Temporary addresses have a limited lifetime, and do not contain an interface identifier that is a link (MAC) address. They are generally indistinguishable from public addresses. IPv6 has the notion of limited address scope using its architected scope designations (see "address scope" on page 19).
protocol table	On iSeries Navigator, a configurable table that associates a protocol name with its assigned protocol number; for example, UDP, 17. The system is shipped with a small number of entries: IP, TCP, UDP, ICMP.	The table supports IPv6 without change.
Quality of service (QoS)	Quality of service allows you to request packet priority and bandwidth for TCP/IP applications.	Currently, QoS does not support IPv6. However, when IPv6 is tunneled in IPv4, existing iSeries QoS facilities can be applied to the IPv4 traffic, which will then transparently handle the IPv6 payloads.
renumbering	Done by manual reconfiguration, with the possible exception of DHCP. Generally, for a site or organization, a difficult and troublesome process to avoid if possible.	Is an important architectural element of IPv6, and is supposed to be largely automatic especially within the /48 prefix.
route	Logically, a mapping of a set of IP addresses (may contain only 1) to a physical interface and a single next hop IP address. IP packets whose destination address is defined as part of the set are forwarded to the next hop using the line. IPv4 routes are associated with an IPv4 interface, hence, an IPv4 address. The default route is *DFTROUTE.	Conceptually, the same as IPv4. One important difference: IPv6 routes are associated (bound) to a physical interface (a link, such as *TNLCFG64 or ETH03) rather than an interface. There are various reasons for this. One reason is that source address selection functions differently for IPv6 than for IPv4. See "source address selection" on page 23. Duplicate routes are allowed to improve robustness, but they are ignored during route lookup.
Routing Information Protocol (RIP)	RIP is a routing protocol supported by the routed daemon.	Currently, RIP does not support IPv6. IPv6 routing uses static routes.
services table	On the iSeries server, a configurable table that associates a service name with a port and protocol; for example, service name FTP-control, port 21, TCP and UDP. A large number of well-known services are listed in the services table. Many applications use this table to determine which port to use.	No changes are made to this table for IPv6.
Simple Network Management Protocol (SNMP)	SNMP is a protocol for system management.	Currently, SNMP does not support IPv6. IPv6 routing uses static routes.

	IPv4	IPv6
sockets API	These APIs are the way applications use TCP/IP. Applications that do not need IPv6 are not affected by sockets changes to support IPv6.	IPv6 enhances sockets so that applications can now use IPv6, using a new address family: AF_INET6. The enhancements have been designed so that existing IPv4 applications are completely unaffected by IPv6 and API changes. Applications that want to support concurrent IPv4 and IPv6 traffic, or IPv6-only traffic, are easily accommodated using IPv4-mapped IPv6 addresses of the form `::ffff:a.b.c.d`, where `a.b.c.d` is the IPv4 address of the client. The new APIs also include support for converting IPv6 addresses from text to binary and from binary to text. See Use AF_INET6 address family for more information on sockets enhancements for IPv6.
source address selection	An application may designate a source IP (typically, using sockets `bind()`) . If it binds to INADDR_ANY, a source IP is chosen based on the route.	As with IPv4, an application may designate a source IPv6 address using `bind()`. Similarly to IPv4, it can let the system choose an IPv6 source address by using in6addr_any. But since IPv6 lines have many IPv6 addresses, the internal method of choosing a source IP is different.
starting and stopping	Use STRTCP and ENDTCP to start or end TCP/IP.	Same as IPv4. IPv4 and IPv6 are not started or stopped independently of one another or independently of TCP/IP. That is, you start and stop all of TCP/IP, not just IPv4 or IPv6. Any IPv6 interfaces are automatically started if the AUTOSTART parameter = `*YES` (the default). IPv6 cannot be used or configured without IPv4, and IPv6 must have IPv6 loopback configured (`::1`).
Telnet	Telnet allows you to log on and use a remote computer as though you were connected to it directly.	Currently, Telnet does not support IPv6.
trace route	Basic TCP/IP tool to do path determination. Available using iSeries Navigator and 5250.	Same for IPv6, and IPv6 is supported for both 5250 and iSeries Navigator.
transport layers	TCP, UDP, RAW. A new transport, Stream Control Transmission Protocol (SCTP), aims to offer the best features of TCP and UDP, that is, guaranteed connectionless communication. SCTP is in the earliest stage of use, and is not supported on iSeries.	Same three transports exist and are functionally unchanged for IPv6.
unspecified address	Apparently, not defined, as such. Socket programming uses `0.0.0.0` as INADDR_ANY.	Defined as `::/128` (128 0 bits). It is used as the source IP in some neighbor discovery packets, and various other contexts, like sockets. Socket programming uses `::/128` as in6addr_any.
virtual private networking (VPN)	Virtual private networking (using IPsec) allows you to extend a secure, private network over an existing public network.	Currently, VPN does not support IPv6. However, when IPv6 is tunneled in IPv4, existing iSeries VPN facilities can be applied to the IPv4 traffic, which then transparently handles the IPv6 payloads.

Troubleshoot IPv6

If you have IPv6 configured on the server, you may use several of the same troubleshooting tools as you do for IPv4. For example, tools such as trace route and PING accept both the IPv4 and IPv6 address formats, so you may use them to test connections and routes for both types of networks. In addition, you may use the communications trace function to trace data on both IPv4 and IPv6 communications lines.

See TCP/IP troubleshooting for a general troubleshooting guide that provides techniques for solving problems related to IPv4 and IPv6.

Related information for IPv6

For more information on IPv6, see these sources of information:

The Internet Engineering Task Force (IETF) (http://www.ietf.cnri.reston.va.us/)
Learn about the group of individuals that develops Internet protocol, including IPv6.

IP Version 6 (IPv6) (http://playground.sun.com/pub/ipng/html/ipng-main.html)
Find current IPv6 specifications and references to several sources on IPv6.

IPv6 Forum (http://www.ipv6forum.com/)
Find news articles and events that communicate the latest IPv6 developments.

Chapter 4. Plan TCP/IP setup

Before you begin to install and configure your iSeries server, take a few moments to plan the operation. See the topics below for planning guidelines. These planning guidelines pertain to basic TCP/IP setup using IPv4. If you intend to configure IPv6, see Configure IPv6 for setup requirements and configuration instructions.

TCP/IP setup requirements
Gather and record basic configuration information that is required for TCP/IP setup.

TCP/IP security considerations
Consider your security needs as a new member of a network.

TCP/IP setup requirements

Print this page and record the configuration information about your server and the TCP/IP network to which you are connecting. You will need to refer to this information later when you configure TCP/IP. Use the instructions following the table to help you determine the values for the first two rows. If you are unfamiliar with any of these terms, see IBM redbook TCP/IP for AS/400: More Cool Things Than

Ever , and refer to Chapter Two, "TCP/IP: Basic Installation and Configuration."

Required information	For your system	Example
Type of communications adapter installed in your system (see instructions below)		Ethernet
Resource name		CMN01
IP address for your iSeries server		199.5.83.158
Subnet mask for your iSeries server		255.255.255.0
Gateway address		199.5.83.129
Host name and domain name for your system		sys400.xyz.company.com
IP address for domain name server		199.4.191.76

To find your communications adapter information, follow these steps:

1. At the server command line, type `go hardware`, and press **Enter**.
2. To select Work with communication resources (Option 1), type 1, and press **Enter**.

   Your communication resources will be listed by resource name. Follow the display instructions if you want to work with your resources or view more details.

What to do next:
Install TCP/IP

TCP/IP security considerations

When planning your TCP/IP configuration, you should consider your security needs. These strategies can help limit your TCP/IP exposure:

- **Start only those TCP/IP applications that you need.**
  Each TCP/IP application has its own unique security exposures. Do not depend on a router to reject requests for a particular application. As a secondary defense, set the autostart values of applications that are not required to N0.

- **Limit the hours during which TCP/IP applications run.**
  Limit your exposure by reducing the hours that your servers are running. If possible, stop TCP/IP servers such as FTP and Telnet during off-hours.

- **Control who can start and change your TCP/IP applications.**
  By default, *IOSYSCFG authority is required to change TCP/IP configuration settings. A user without *IOSYSCFG authority needs *ALLOBJ authority or explicit authority to the TCP/IP start commands. Giving special authorities to users represents a security exposure. Evaluate the need for any special authorities for each user and keep special authorities to a minimum. Keep track of which users have special authorities and periodically review their requirement for the authority. This also limits the possibility of server access during off-hours.

- **Control your TCP/IP routing:**
  - Disallow IP forwarding so that hackers cannot use your Web server to attack other trusted systems.
  - Define only one route on your public Web server: the default route to your Internet Service Provider.
  - Do not configure host names and IP addresses of internal secure systems in your Web server's TCP/IP host table. Only put the name of other public servers that you need to reach in this table.

- **Control TCP/IP servers designed for remote, interactive sign-on.**
  Applications such as FTP and Telnet are more vulnerable to outside attack. For details on how to control your exposure, read the chapter on tips for controlling interactive sign-on in Tips and Tools for

  Securing Your iSeries .

For more information about security and the options available to you, refer to iSeries and Internet security.

Chapter 5. Install TCP/IP

Base TCP/IP support comes with OS/400 and allows you to connect an iSeries server to a network. However, if you want to use any TCP/IP applications such as Telnet, FTP, and SMTP, you also need to install TCP/IP Connectivity Utilities. This is a separately installable licensed program that is included with your operating system.

To install TCP/IP Connectivity Utilities on your iSeries server, follow these steps:

1. Insert your installation media for TCP/IP into your server. If your installation media is a CD-ROM, insert it into your optical device. If your installation media is a tape, insert it into your tape drive.

2. At the command line, type `GO LICPGM` and press **Enter** to access the Work with Licensed Programs display.

3. Select option **11** (Install licensed programs) on the Work with Licensed Programs display to see a list of licensed programs and optional parts of licensed programs.

4. Type **1** (Install) in the Option column next to 57*xx*TC1 (TCP/IP Connectivity Utilities for iSeries). Press **Enter**. The Confirm Licensed Programs to Install display shows the licensed program you selected to install. Press **Enter** to confirm.

5. Fill in the following choices on the Install Options display:

Installation device	Type `QOPT` if installing from a CD-ROM device.
	Type `TAP01` if installing from a tape drive.
Objects to install	This option allows you to install both programs and language objects, only programs, or only language objects.
Automatic restart	This option determines whether the system automatically starts when the installation process has completed successfully.

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

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

   If an error occurs, you will see the message `Work with licensed program function not complete` on the bottom of the Work with Licensed Programs display. Should a problem occur, try to re-install TCP/IP Connectivity Utilities. If the problem is not resolved, you may need to contact support.

Note:

   Other licensed programs that you may want to install include:

   - iSeries Access for Windows 95/NT (5769–XD1 V3R1M3 or later) provides iSeries Navigator support that is used to configure some of the TCP/IP components.
   - IBM HTTP Server for iSeries (57*xx*–DG1) provides Web server support.
   - Some TCP/IP applications require installation of additional licensed programs. To find out which programs you need, review the setup instructions for the specific application you want.

Chapter 6. Configure TCP/IP

You may be configuring TCP/IP for the first time, or you may be changing an existing configuration to use the IPv6 function. This topic provides instructions for configuring TCP/IP in each of these situations. See the options below for instructions on how to configure TCP/IP on your server:

Configure TCP/IP for the first time
Use these instructions if you are setting up a new server. You will establish a connection and configure TCP/IP for the first time.

Configure IPv6
Use these instructions to configure your server for IPv6 function. You will benefit from the enhanced addressing capability and the robust features of this Internet Protocol. If you are unfamiliar with IPv6, see Internet Protocol version 6 (IPv6) for an overview. You must have TCP/IP configured on the server before you may configure IPv6.

Configure TCP/IP when the operating system is in restricted state
Use this method if you need to run TCP/IP while the operating system is in restricted state.

Configure TCP/IP for the first time

Select one of the following methods for setting up TCP/IP on your new server:

Configure TCP/IP using the EZ-Setup wizard
Use this preferred method if your PC is equipped to use the EZ-Setup wizard. The EZ-Setup wizard is packaged with your iSeries server.

Configure TCP/IP using the character-based interface
Use this method if you are unable to use the EZ-Setup wizard. For example, if you want to use iSeries Navigator from a PC that requires basic TCP/IP configuration before iSeries Navigator will run, then you should use this method.

Configure TCP/IP using the EZ-Setup wizard

iSeries Navigator is a graphical user interface that provides concise dialog boxes and wizards to configure TCP/IP. For initial setup, use the iSeries Navigator's EZ-Setup wizard to establish a connection and to configure TCP/IP for the first time. This is the preferred method for working with your server because the interface is easy to use. The CD-ROM containing the EZ-Setup wizard is packaged with your iSeries server.

To configure your server, follow these steps:
1. Use the EZ-Setup wizard. Access the wizard from the CD-ROM that is packaged with your server. Follow the wizard's instructions to configure TCP/IP.
2. Start TCP/IP
   a. In iSeries Navigator, expand your **server –> Network**.
   b. Right-click **TCP/IP configuration** and select **Start**. All interfaces and servers that were set to start automatically when TCP/IP is started will be started at this time.

You have finished configuring TCP/IP on your server. Use iSeries Navigator to modify the configuration as your networking needs change. See Customize TCP/IP with iSeries Navigator to add routes and interfaces or Configure IPv6 to use Internet Protocol version 6 on your network.

Configure TCP/IP using the character-based interface

If you are unable to use the iSeries Navigator's EZ-Setup wizard, use the character-based interface instead. For example, if you want to use iSeries Navigator from a PC that requires basic TCP/IP configuration before iSeries Navigator will run, then you should use the character-based interface to perform the basic configuration.

To perform the configuration steps discussed in this section, you need *IOSYSCFG special authority in your user profile. For more information on this type of authority, see the chapter on user profiles in iSeries

Security Reference .

To configure TCP/IP using the character-based interface, follow these steps:

1. At the command line, type GO TCPADM to display the TCP/IP Administration menu, and press Enter.
2. Specify option 1 (Configure TCP/IP) to display the Configure TCP/IP menu (CFGTCP), and press Enter. Use this menu to select configuration tasks. Take a few moments to review the menu before starting to configure your server.

Perform the following steps to configure TCP/IP on your server.

1. Configure a line description
2. Turn on IP datagram forwarding
3. Configure an interface
4. Configure a route
5. Define local domain and host names
6. Define a host table
7. Start TCP/IP

Configure a line description (Ethernet)

These instructions pertain to configuring TCP/IP over an Ethernet communications adapter. However, if you are using a different type of adapter, such as a token-ring, see TCP/IP Configuration and Reference, *Appendix A*, for a command specific to your adapter.

To configure a line description, follow these steps:

1. At the command line, type CRTLINETH to access the Create Line Desc (Ethernet) (CRTLINETH) menu, and press Enter.
2. Specify your line name, and press Enter. (Use any name.)
3. Specify your resource name, and press Enter.

What to do next:
Turn on IP datagram forwarding

Turn on IP datagram forwarding

Turn on IP datagram forwarding so that the packets can be forwarded among different subnets.

To turn on IP datagram forwarding, follow these steps:

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

What to do next:
Configure an interface

Configure an interface

To configure an interface, follow these steps:

1. At the command line, type `CFGTCP` to access the Configure TCP/IP menu, and press Enter.
2. Select option 1 (Work with TCP/IP interfaces) on the Configure TCP/IP menu, and press Enter.
3. Specify option 1 (Add) to show the Add TCP/IP Interface display, and press Enter.
4. Specify the address value that you want to represent your iSeries server, the subnet mask address, and the line description name you previously defined, and then press Enter.

To start the interface, specify option 9 (Start) for the interface you configured, and press Enter.

What to do next:
Configure a route

Configure a route

To reach remote networks, at least one routing entry is required. If no routing entries are manually added, your server cannot reach systems that are not on the same network to which the server is attached. You must also add routing entries to allow TCP/IP clients that are attempting to reach your server from a remote network to function correctly.

You should plan to have the routing table defined so that there is always an entry for at least one default route (`*DFTROUTE`). If there is no match on any other entry in the routing table, data is sent to the IP router specified by the first available default route entry.

To configure a default route, follow these steps:

1. Select option 2 (Work with TCP/IP Routes) on the Configure TCP/IP menu, and press Enter.
2. Specify option 1 (Add) to go to the Add TCP/IP Route (`ADDTCPRTE`) display, and press Enter.
3. Specify `*DFTROUTE` for the route destination, specify `*NONE` for the subnet mask, specify the IP address for the next hop, and press Enter.

What to do next:
Define local domain and host names

Define local domain and host names

To define local domain and host names, follow these steps:

1. Select option 12 (Change TCP/IP domain) from the Configure TCP/IP menu, and press Enter.
2. Specify the names you selected to be your local host name and local domain name, leaving the other parameters at the default values, and press Enter.

What to do next:
Define a host table

Define a host table

To define a host table, follow these steps:

1. Select option 10 (Work with TCP/IP Host Table Entries) from the Configure TCP/IP menu, and press Enter.
2. Specify option 1 (Add) to go to the Add TCP/IP Host Table Entry display, and press Enter.
3. Specify the IP address, the associated local host name and the fully qualified host name, and then press Enter.
4. Specify a plus sign (+) to make space available for more than one host name, if necessary.
5. Repeat these steps for each of the other hosts on the network to which you want to communicate with by name, and add an entry for each.

What to do next:
Start TCP/IP

Start TCP/IP

TCP/IP services are not available until you start TCP/IP.

To start TCP/IP, type STRTCP at the command line.

The Start TCP/IP (STRTCP) command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the server jobs. Only TCP/IP interfaces and servers with AUTOSTART *YES are started with the STRTCP command.

You have finished configuring TCP/IP on your server. Use iSeries Navigator to modify the configuration as your networking needs change. See Customize TCP/IP with iSeries Navigator to add routes and interfaces or Configure IPv6 to use Internet Protocol version 6 on your network.

Configure IPv6

You are ready to take advantage of the next generation Internet by using IPv6 on your network. To use the IPv6 function, you need to change your TCP/IP configuration by configuring a line that is dedicated to IPv6. You must configure either a line on a 2838 or 2849 Ethernet adapter or on a configured tunnel line (virtual line). Read these topics for instructions on configuring IPv6:

Setup requirements
This topic lists the hardware and software requirements for configuring the server for IPv6.

Configure IPv6 using the IPv6 Configuration wizard
See instructions for using the **IPv6 Configuration** wizard to configure IPv6 on your server.

Setup requirements

Determine which of these two types of IPv6 configurations is appropriate for your situation. If you are not sure which type to choose, see IPv6 scenarios for examples.

Meet these requirements to allow IPv6 to function on your server:

For configuring an Ethernet line for IPv6:
- OS/400 Version 5 Release 2 or later
- iSeries Access for Windows and iSeries Navigator
  - Network component of iSeries Navigator
- 2838 or 2849 Ethernet adapter to be dedicated to IPv6.
- IPv6–capable router is required only if you want to send IPv6 traffic beyond the immediate LAN.
- TCP/IP (using IPv4) must be configured on a separate physical adapter because TCP/IP must be running on the server. If you have not configured your server for IPv4, see Configure TCP/IP for the first time before configuring the line for IPv4.

For creating a configured tunnel line (TNLCFG64):
- OS/400 Version 5 Release 2 or later
- iSeries Access for Windows and iSeries Navigator
  - Network component of iSeries Navigator
- TCP/IP (using IPv4) must be configured on the server before you configure the tunnel line for IPv6. If you have not configured your server for IPv4, see Configure TCP/IP for the first time.

Go to Configure IPv6 using the IPv6 Configuration wizard for directions on accessing the wizard.

Configure IPv6 using the IPv6 Configuration wizard

To configure IPv6 on the server, you must change the server's configuration using the **IPv6 Configuration** wizard in iSeries Navigator. IPv6 may only be configured from iSeries Navigator, and may not be configured from the character-based interface.

Note: You may configure the IPv6 ethernet line description by using the Create Line Desc (Ethernet) CRTLINETH command in the character-based interface; however, you must specify the hexadecimal multicast group address 333300000001. Then, you must use the **IPv6 Configuration** wizard to finish configuring IPv6.

The wizard will require the following input:

For configuring an Ethernet line for IPv6:
This configuration allows you to send IPv6 packets over an IPv6 local area network (LAN). The wizard requires the name of the hardware communications resource on the server on which you will configure IPv6; for example, CMN01. This must be either a 2838 or 2849 Ethernet adapter that is not currently configured for IPv4. See Create an IPv6 local area network (LAN) for a scenario that shows a situation in which you would configure an Ethernet line for IPv6.

For creating a configured tunnel line (TNLCFG64):
This type of configuration allows you to send IPv6 packets over IPv4 networks. The wizard requires the IPv4 address for the local endpoint and the IPv6 address for the local interface associated with the tunnel. See Send IPv6 packets over an IPv4 local area network (LAN) and Send IPv6 packets over an IPv4 wide area network (WAN) for scenarios that show two situations in which you would create the configured tunnel lines for IPv6.

To use the **IPv6 Configuration** wizard, follow these steps:

1. In iSeries Navigator, expand your **server —> Network —> TCP/IP Configuration**.
2. Right-click **IPv6** and select **IPv6 Configuration**.
3. Follow the wizard's instructions to configure IPv6 on your server.

Configure TCP/IP when the operating system is in restricted state

Situation

As the network administrator, you need to obtain backup status reports for your server. When you are running backup procedures, the operating system must be in restricted state to prevent users from changing any configuration. Since you are remote, you access status reports using a PDA device (or any TCP/IP networking device). The PDA uses a sockets-enabled application that requires an active TCP/IP interface available to communicate with the server. To allow this communication, you must first start TCP/IP using special parameters. After you start TCP/IP, you will need to start a specific TCP/IP interface to allow access to the system. The information below provides more detail.

Prerequisites

Your iSeries server is running on OS/400(R) V5R2 or later.

Restrictions

The following restrictions apply when the operating system is running in restricted state:
- Cannot start TCP/IP servers (STRTCPSRV CL command), since they require active subsystems.
- Can only start one interface for a specific line type (Ethernet, token-ring, or DDI) that is not attached to a network server description (NWSD) or a network interface description (NWID).

Configuration steps

1. Start TCP/IP using special parameters

   When the iSeries system is in restricted state, process the following command from the command line interface: STRTCP STRSVR(*NO) STRIFC(*NO). These are the only parameters accepted when the operating system is in restricted state. The above command will start TCP/IP; however, it will not and cannot start TCP/IP application servers or IP interfaces.

2. Start a specific TCP/IP interface

   After you start TCP/IP in restricted state, you can start the specific interface needed for your sockets-enabled application.

   a. Verify that the interface you want to start uses a line description of *ELAN, *TRLAN, or *DDI.

      To view the line type for your interface, at a command line interface enter CFGTCP and select option 1 - Work with TCP/IP interfaces.

   b. Verify that the interface is not attached to an NWID or NWSD. Any other attempts will prompt an error message.

      To verify the interface is not attached to a NWID or NWSD, from a command line interface enter DSPLIND abc (where abc is the name of your line description). Verify that the Resource name is not *NWID or *NWSD.

      Note: If the interface is attached to an NWID or a NWSD, then it is recommended you select a different interface.

   c. Finally, start the interface. At a command line interface, enter the following: STRTCPIFC INTNETADR('a.b.c.d'). Replace a.b.c.d with your interface IP address.

      Note: Verify that STRTCPIFC INTNETADR(*AUTOSTART) is not specified.

3. Verify that the interface is active.

   Ping the specific interface for your application. There are very few TCP/IP related utilities that will operate in restricted state. However, Ping and Netstat can be used. For more information about using the ping and netstat commands, please review Tools to verify your network structure within TCP/IP troubleshooting.

Chapter 7. Customize TCP/IP with iSeries Navigator

Once you have configured TCP/IP, you may decide to customize your configuration. As your network grows, you may need to change properties, add interfaces, or add routes to your server. You may need to configure the server for IPv6 (Internet Protocol version 6) to use IPv6 applications. Use wizards in iSeries Navigator to quickly accomplish many of these tasks.

Choose any of the topics below to customize your configuration using iSeries Navigator. These topics provide a starting point for you to manage your TCP/IP configuration with iSeries Navigator.

> Change TCP/IP settings
>
> Configure IPv6
>
> Add IPv4 interfaces
>
> Add IPv6 interfaces
>
> Add IPv4 routes
>
> Add IPv6 routes

Change TCP/IP settings

You can view and change your TCP/IP settings using iSeries Navigator. For instance, you may change properties for host or domain names, name server, host table entries, system attributes, port restrictions, servers, or client connections. You may change general properties or properties that are specific to either IPv4 or IPv6, such as transports.

To access the general TCP/IP property pages, follow these steps:

1. In iSeries Navigator, select your **server —> Network** .
2. Right-click **TCP/IP Configuration** and select **Properties** to open the **TCP/IP Properties** dialog.
3. Select the tabs at the top of the dialog to view and edit TCP/IP information.

To add and change host table entries, follow these steps:

1. In iSeries Navigator, select your **server —> Network** .
2. Right-click **TCP/IP Configuration** and select **Host Table** to open the **Host Table** dialog.
3. Use the **Host Table** dialog to add, edit, or remove host table entries.

To access property pages that are specific to IPv4, follow these steps:

1. In iSeries Navigator, select your **server —> Network** .
2. Right-click **IPv4** and select **Properties** to open the **IPv4 Properties** dialog.
3. Select the tabs at the top of the dialog to view and edit the IPv4 property settings.

To access property pages that are specific to IPv6, follow these steps:

1. In iSeries Navigator, select your **server —> Network** .
2. Right-click **IPv6** and select **Properties** to open the **IPv6 Properties** dialog.
3. Select the tabs at the top of the dialog to view and edit the IPv6 property settings.

Configure IPv6

If you are unfamiliar with IPv6, see Internet Protocol version 6 (IPv6) for an overview.

To configure IPv6, you must change the server's configuration by using the **IPv6 Configuration** wizard. Before using the wizard, see Configure IPv6 for instructions and special requirements.

Add IPv4 interfaces

To create a new IPv4 interface, follow these steps:
1. In iSeries Navigator, select your **server —> Network —> TCP/IP Configuration —> IPv4**.
2. Right-click **Interfaces**, select **New Interface**, and select **Local Area Network**, **Wide Area Network**, or **Virtual IP** to create the appropriate type of IPv4 interface.
3. Follow the wizard's instructions to create a new IPv4 interface.

Add IPv6 interfaces

To create a new IPv6 interface, follow these steps:
1. In iSeries Navigator, select your **server —> Network —> TCP/IP Configuration —> IPv6**.
2. Right-click **Interfaces** and select **New Interface**.
3. Follow the wizard's instructions to create a new IPv6 interface.

Add IPv4 routes

Any changes that you make to the routing information take effect immediately.

To configure a new IPv4 route, follow these steps:
1. In iSeries Navigator, select your **server —> Network —> TCP/IP Configuration —> IPv4**.
2. Right-click **Routes**, and select **New Route**.
3. Follow the wizard's instructions to configure a new IPv4 route.

Add IPv6 routes

Any changes that you make to the routing information take effect immediately.

To configure a new IPv6 route, follow these steps:
1. In iSeries Navigator, select your **server —> Network —> TCP/IP Configuration —> IPv6**.
2. Right-click **Routes**, and select **New Route**.
3. Follow the wizard's instructions to configure a new IPv6 route.

Chapter 8. TCP/IP techniques connecting virtual Ethernet to external LANs

≫ If you are using a virtual Ethernet network for interpartition communication, you may need to enable these partitions to communicate with a physical, external LAN. There are several ways to connect the virtual Ethernet network to an external LAN using different TCP/IP techniques. You need to enable the TCP/IP traffic to flow between the virtual Ethernet network and the external LAN. This figure shows a logical flow of the IP packets.
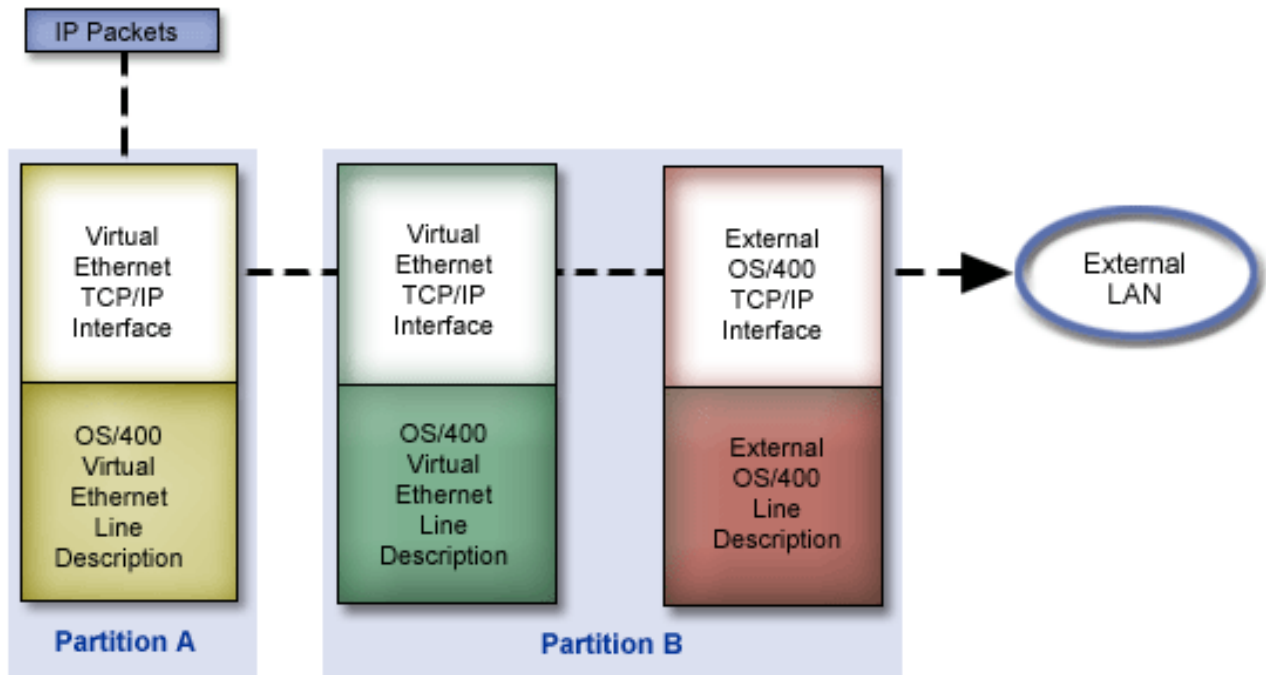
IP traffic initiated by Partition A goes from its virtual Ethernet interface to the virtual Ethernet interface on Partition B. By implementing any one of the three TCP/IP techniques described below, you can enable the IP packets to continue on to the external interface and toward their destination.

There are three methods for connecting the virtual Ethernet and external LAN. Each method has nuances that make it more feasible based on your knowledge of TCP/IP and your environment. Choose from one of the following methods:

- **Proxy ARP**
  This method uses transparent subnetting to associate a partition's virtual interface with an external interface. Proxy ARP function is built into the TCP/IP stack. If you have the necessary IP addresses, this approach is recommended.
- **Network address translation**
  OS/400 packet filtering can be used to route traffic between a partition and the outside network.
- **TCP/IP routing**
  Standard TCP/IP routing is used to route traffic to the virtual Ethernet network in the same way you would define routing to any other LAN. This requires that you update routing information throughout your network.

Proxy ARP method

The proxy ARP method uses a technique commonly known as *transparent subnetting*. You might want to learn more information about transparent subnetting:

- V4 TCP/IP for AS/400: More Cool Things Than Ever
  This redbook provides sample scenarios that demonstrate common solutions with example configurations. It also helps you plan, install, tailor, configure, and troubleshoot TCP/IP on your iSeries server.
- TCP/IP routing and workload balancing
  This topic provides techniques and instructions for routing and workload balancing.

If you choose to use the proxy ARP method, you must have a firm understanding of subnetting and TCP/IP. You need to obtain a contiguous block of IP addresses that are routable by your network. You subnet this block of IP addresses. In this example, a contiguous block of four IP addresses (10.1.1.72 through 10.1.1.75) is used. Since it is a block of four IP addresses, the subnet mask for these addresses is 255.255.255.252. You assign one to each of the virtual TCP/IP interfaces on your partitions as shown in this figure.
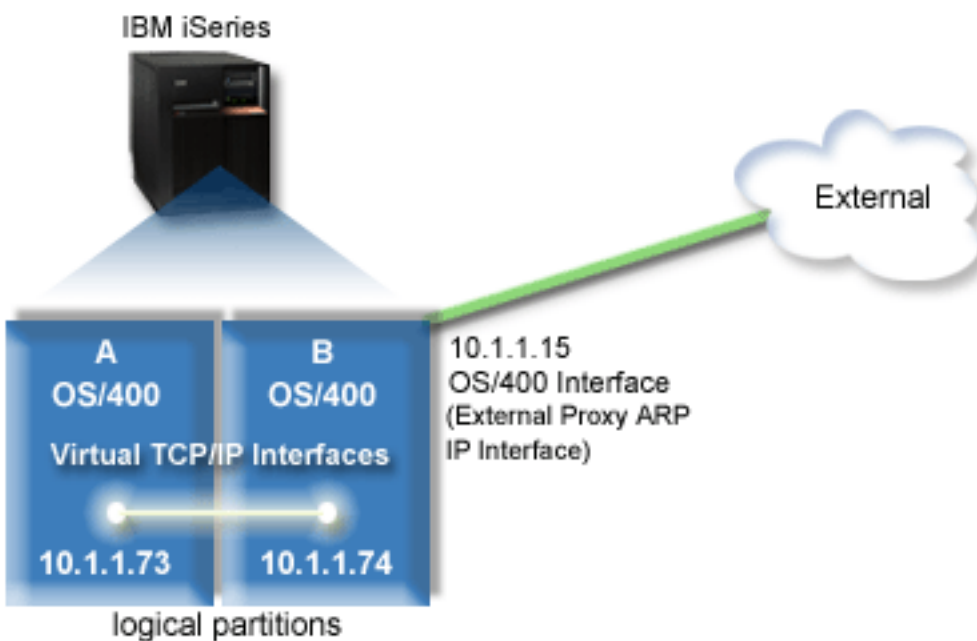
In this example, TCP/IP traffic from partition A runs across the virtual Ethernet to the 10.1.1.74 interface on partition B. Since 10.1.1.74 is associated with the external proxy ARP interface 10.1.1.15, the packets continue out of the virtual Ethernet using the proxy ARP interface.

To configure a virtual Ethernet to use the proxy ARP connection method, 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 TCP/IP interface on partition A
6. Create the virtual TCP/IP interface on partition B
7. Create the route
8. Verify network communications

Step 1: Enable the logical partitions to participate in a virtual Ethernet

Note: If you are using any servers other than the 270 and 8*xx* model servers, you need to perform this step using the Hardware Management Console for eServer™ (HMC) instead of the primary partition. See virtual Ethernet for details.

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 partition A and partition B to enable the partitions to communicate with one another over virtual Ethernet.
7. Exit System Service Tools (SST) to return to the command line.

What to do next

Create the Ethernet line descriptions

Step 2: Create the Ethernet line descriptions

You need to perform this step in one of two ways depending on the server model you are using. Choose one of these methods for creating the line descriptions based on your particular server model.
- Create the Ethernet line descriptions on the 270 and 8*xx* model servers
- Create the Ethernet line descriptions on any servers other than the 270 and 8xx model servers

Create the Ethernet line descriptions on the 270 and 8*xx* model servers

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

1. At the command line on 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 line on partition B to create an Ethernet line description for partition B.

   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.

What to do next

Turn on IP datagram forwarding

Create the Ethernet line descriptions on any servers other than the 270 and 8xx model servers

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

1. At the command line on 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 ports identified as 268C are the virtual Ethernet resources. There will be one for each virtual Ethernet adapter. Each port identified as 268C has an associated location code that is created when you create the virtual Ethernet adapter using the HMC (Step 1).

3. From the Display Resource Detail display, scroll down to find the 268C resource that is associated to the specific location code created for this virtual Ethernet.

4. From the Work with Communication Resources display, select option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet resource, 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. If you use the same names for the line descriptions and their associated virtual Ethernet, such as VETH0, 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 line on partition B to create an Ethernet line description for partition B.

   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.

What to do next

Turn on IP datagram forwarding

Step 3: Turn on IP datagram forwarding

Turn on IP datagram forwarding so that the packets can be forwarded among different subnets.

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

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 two partitions in this virtual Ethernet, you need a block of four addresses. The fourth segment of the first IP address in the block must be divisible by four. The first and last IP addresses of this block are the subnet and broadcast IP addresses and are unusable. The second and third IP address can be used for the TCP/IP interfaces for the virtual Ethernet on partition A and partition B. For this procedure, the IP address block is 10.1.1.72 through 10.1.1.75 with a subnet mask of 255.255.255.252.

   You also need a single IP address for your external TCP/IP address. This IP address does not have to belong to your block of contiguous addresses, but it must be within the same original subnet mask of 255.255.255.0. In this procedure, the external IP address is 10.1.1.15.

2. Create an OS/400 TCP/IP interface for partition B. 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 B, 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.

Step 5: Create the virtual TCP/IP interface on partition A

To create the virtual interface, follow these steps:

1. At the command line on partition A, type `CFGTCP`, and press Enter to see the Configure TCP/IP display.

2. Select option 1 (Work with TCP/IP Interfaces), and press Enter.

3. Select option 1 (Add), and press Enter to see the Add TCP/IP Interface (ADDTCPIFC) display.

4. For the *Internet address* prompt, type `'10.1.1.73'`.

5. For the *Line description* prompt, type the name of your line description, such as ETHLINE.

6. For the *Subnet mask* prompt, type `'255.255.255.252'`.

7. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface.

Step 6: Create the virtual TCP/IP interface on partition B

To create the virtual interface, follow these steps:

1. At the command line on partition B, type `CFGTCP`, and press Enter to see the Configure TCP/IP display.

2. Select option 1 (Work with TCP/IP Interfaces), and press Enter.
3. Select option 1 (Add), and press Enter to see the Add TCP/IP Interface (ADDTCPIFC) display.
4. For the *Internet address* prompt, type '10.1.1.74'.
5. For the *Line description* prompt, type the name of your line description, such as ETHLINE.
6. For the *Subnet mask* prompt, type '255.255.255.252'.
7. For the *Associated local interface* prompt, type '10.1.1.15'. This associates the virtual interface to the external interface and enables proxy ARP to forward packets between the virtual interface 10.1.1.74 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.

What to do next

Create the route

Step 7: Create the route

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

1. At the command line on partition A, 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 *DFTROUTE.
5. For the *Subnet mask* prompt, type *NONE.
6. For the *Next hop* prompt, type '10.1.1.74'.

   Packets from partition A travel over the virtual Ethernet to the 10.1.1.74 interface using this default route. Since 10.1.1.74 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.

What to do next

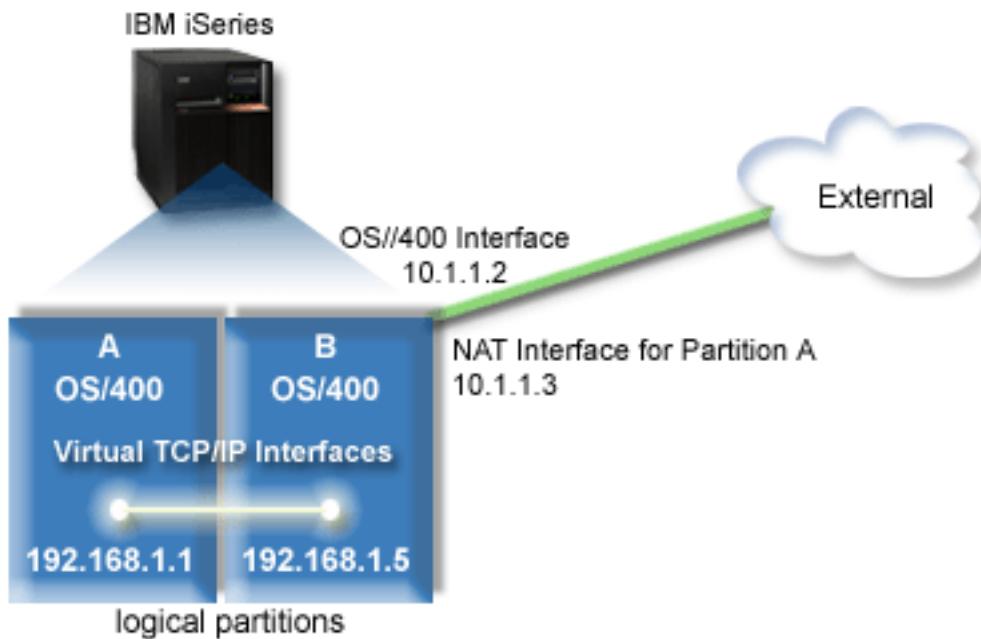Verify network communications

Step 8: Verify network communications

Verify your network communications by using the ping command:

- From partition A, ping the virtual Ethernet interface 10.1.1.74 and an external host.
- From an external OS/400 host, ping the virtual Ethernet interfaces 10.1.1.73 and 10.1.1.74.

Network address translation method

Network address translation (NAT) can route traffic between your virtual Ethernet network and the external network. This particular form of NAT is called static NAT, and it will allow both inbound and outbound IP traffic to and from the virtual Ethernet network. Other forms of NAT like masquerade NAT would also work if your virtual Ethernet network does not need to receive traffic initiated by external clients. Like the TCP/IP routing and proxy ARP methods, you can take advantage of your existing OS/400 network connection. Since you will be using IP packet rules, you must use iSeries Navigator to create and apply your rules.

The following figure is an example of using NAT to connect your virtual Ethernet network to an external network. The 10.1.1.*x* network represents an external network while the 192.168.1.*x* network represents the virtual Ethernet network.

IBM iSeries

OS//400 Interface
10.1.1.2

NAT Interface for Partition A
10.1.1.3

External

A
OS/400

B
OS/400

Virtual TCP/IP Interfaces

192.168.1.1   192.168.1.5

logical partitions

In this example, any existing TCP/IP traffic for the server runs over the 10.1.1.2 interface. Since this is a static map scenario, the inbound traffic gets translated from the 10.1.1.3 interface to 192.168.1.5 interface. The outbound traffic gets translated from the 192.168.1.5 interface to the external 10.1.1.3 interface. Partition A and partition B use their virtual interfaces 192.168.1.1 and 192.168.1.5 respectively, to communicate with one another.

To make static NAT work, you need to first set up your OS/400 and TCP/IP communications. Then you will create and apply some IP Packet rules. To configure virtual Ethernet to use the NAT method, 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 interfaces
5. Verify network communications
6. Create packet rules
7. Verify network communications

Step 1: Enable the logical partitions to participate in a virtual Ethernet

Note: If you are using any servers other than the 270 and 8*xx* model servers, you need to perform this step using the Hardware Management Console for eServer (HMC) instead of the primary partition. See virtual Ethernet for details.

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 partition A and partition B to enable the partitions to communicate with one another over virtual Ethernet.

7. Exit System Service Tools (SST) to return to the command line.

What to do next

Create the Ethernet line descriptions

Step 2: Create the Ethernet line descriptions

You need to perform this step in one of two ways depending on the server model you are using. Choose one of these methods for creating the line descriptions based on your particular server model.

- Create the Ethernet line descriptions on the 270 and 8*xx* model servers
- Create the Ethernet line descriptions on any servers other than the 270 and 8xx model servers

Create the Ethernet line descriptions on the 270 and 8*xx* model servers

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

1. At the command line on 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 line on partition B to create an Ethernet line description for partition B.

   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.

What to do next

Turn on IP datagram forwarding

Create the Ethernet line descriptions on any servers other than the 270 and 8xx model servers

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

1. At the command line on 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 ports identified as 268C are the virtual Ethernet resources. There will be one for each virtual Ethernet adapter. Each port identified as 268C has an associated location code that is created when you create the virtual Ethernet adapter using the HMC (Step 1).

3. From the Display Resource Detail display, scroll down to find the 268C resource that is associated to the specific location code created for this virtual Ethernet.

4. From the Work with Communication Resources display, select option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet resource, 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. If you use the same names for the line descriptions and their associated virtual Ethernet, such as VETH0, 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 line on partition B to create an Ethernet line description for partition B.

   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.

What to do next

Turn on IP datagram forwarding

Step 3: Turn on IP datagram forwarding

Turn on IP datagram forwarding so that the packets can be forwarded among different subnets.

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.

What to do next

Create the interfaces

Step 4: Create the interfaces

To create the TCP/IP interfaces, complete these steps:

1. Create and start an OS/400 TCP/IP interface on partition B for general communication to and from the server. To create the interface, follow these steps:

   a. At the command line on partition B, 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 '10.1.1.2'.

   e. For the *Line description* prompt, type ETHLINE.

   f. For the *Subnet mask* prompt, type '255.255.255.0'.

g. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface.

2. Create and start another TCP/IP interface that connects to the external network. It should use the same line description as your existing external TCP/IP interface. This interface will eventually perform the address translation for your partition. To create the interface, follow these steps:

   a. At the command line on partition B, 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 '10.1.1.3'.

   e. For the *Line description* prompt, type ETHLINE.

   f. For the *Subnet mask* prompt, type '255.255.255.0'.

   g. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface.

3. Create and start the OS/400 TCP/IP interface on partition A for the virtual Ethernet. 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 '192.168.1.1'.

   e. For the *Line description* prompt, type VETH0.

   f. For the *Subnet mask* prompt, type '255.255.255.0'.

   g. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface.

4. Create and start the OS/400 TCP/IP interface on partition B for the virtual Ethernet. To create the interface, follow these steps:

   a. At the command line on partition B, 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 '192.168.1.5'.

   e. For the *Line description* prompt, type VETH0.

   f. For the *Subnet mask* prompt, type '255.255.255.0'.

   g. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface.

What to do next

Verify network communications

Step 5: Verify network communications

Verify your network communications by using the ping command:

- From partition A, ping the virtual Ethernet interface 192.168.1.5 and an external host.
- From an external OS/400 host, ping each of the virtual Ethernet interfaces 192.168.1.1 and 192.168.1.5.

What to do next

Create packet rules

Step 6: Create packet rules

Use the Address Translation wizard in iSeries Navigator to create the packet rules that map the private address on partition A to the public address on partition B.

To create the packet rules, follow these steps:

1. In iSeries Navigator, expand your **iSeries server –> Network–> IP Policies**.
2. Right-click **Packet Rules** and select **Rules Editor**.
3. Select **Address Translation** from the **Wizard** menu.
4. Follow the wizard's instructions to create the packet rules. This procedure uses these selections:
   - Select **Map address translation**
   - Enter the private IP address 192.168.1.1
   - Enter the public IP address 10.1.1.3
   - Select the line on which the interfaces are configured, such as ETHLINE
5. Select **Activate Rules** from the **File** menu.

What to do next

Verify network communications

Step 7: Verify network communications

After creating the packet rules, you should verify network communications. To test outbound communications, ping an external host from partition A. Then from that external host, ping partition A to test inbound communications.

TCP/IP routing method

You can also route traffic to your partitions through your iSeries server with various routing techniques. This solution is not difficult to configure on the server but, depending on the topology of your network, it may not be practical to implement. Consider the following figure.
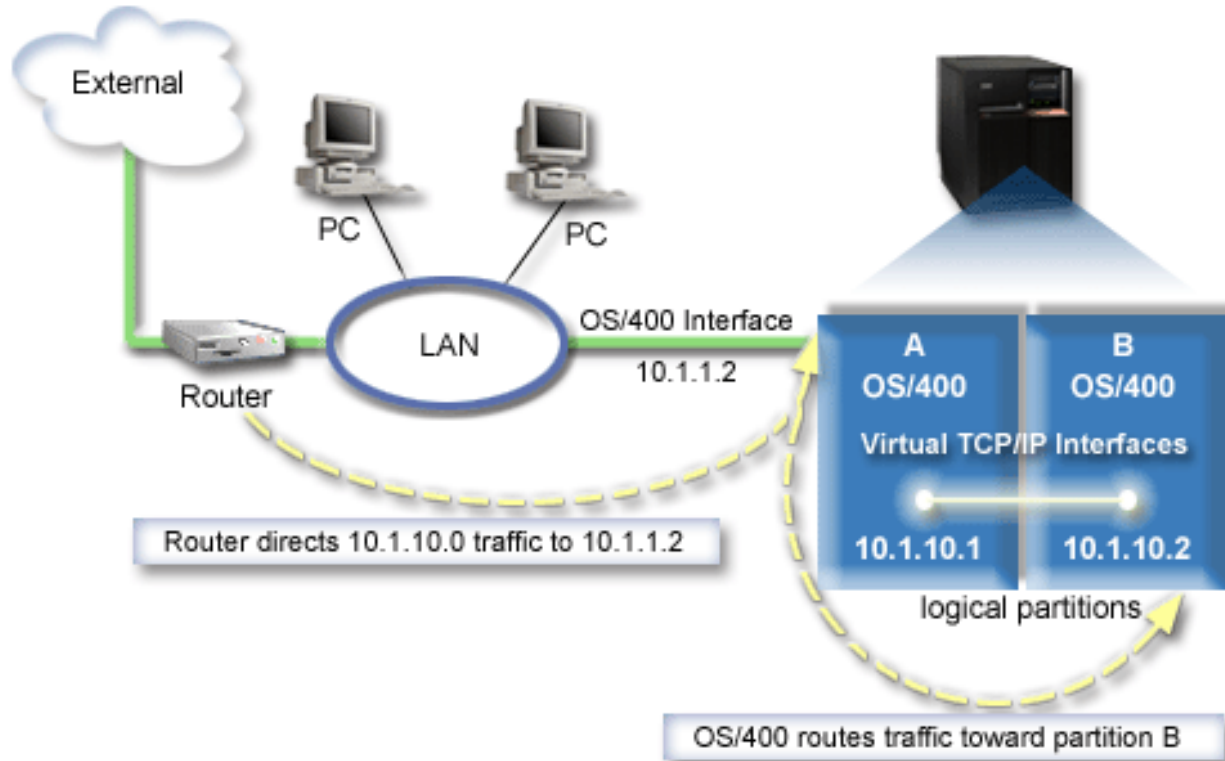
The existing TCP/IP interface (10.1.1.2) connects to the LAN. The LAN is connected to remote networks with a router. The virtual TCP/IP interface on partition B is addressed as 10.1.10.2 and the virtual TCP/IP interface on partition A as 10.1.10.1. In OS/400, if you turn on IP datagram forwarding, OS/400 will route the IP packets to and from partition B. When you define your TCP/IP connection for partition B, the router address must be 10.1.10.1.

The difficulty of this type of routing is getting the IP packets to the iSeries. In this scenario, you could define a route on the router so that it passes packets destined to the 10.1.10.0 network to the 10.1.1.2 interface. That works for remote network clients. It would also work for the local LAN clients (clients connected to the same LAN as the iSeries) if they recognize that same router as their next hop. If they do not, then each client must have a route that directs 10.1.10.0 traffic to the OS/400 10.1.1.2 interface; therein starts the impracticability of this method. If you have many LAN clients, then you have to define many routes.

To configure virtual Ethernet to use the TCP/IP routing method, use the following instructions:
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 interfaces

Step 1: Enable the logical partitions to participate in a virtual Ethernet

Note: If you are using any servers other than the 270 and 8*xx* model servers, you need to perform this step using the Hardware Management Console for eServer (HMC) instead of the primary partition. See virtual Ethernet for details.

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 partition A and partition B to enable the partitions to communicate with one another over virtual Ethernet.
7. Exit System Service Tools (SST) to return to the command line.

What to do next

Create Ethernet line descriptions

Step 2: Create the Ethernet line descriptions

You need to perform this step in one of two ways depending on the server model you are using. Choose one of these methods for creating the line descriptions based on your particular server model.

- Create the Ethernet line descriptions on the 270 and 8*xx* model servers
- Create the Ethernet line descriptions on any servers other than the 270 and 8xx model servers

Create the Ethernet line descriptions on the 270 and 8*xx* model servers

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

1. At the command line on 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 line on partition B to create an Ethernet line description for partition B.

   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.

What to do next

Turn on IP datagram forwarding

Create the Ethernet line descriptions on any servers other than the 270 and 8xx model servers

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

1. At the command line on 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 ports identified as 268C are the virtual Ethernet resources. There will be one for each virtual Ethernet adapter. Each port identified as 268C has an associated location code that is created when you create the virtual Ethernet adapter using the HMC (Step 1).

3. From the Display Resource Detail display, scroll down to find the 268C resource that is associated to the specific location code created for this virtual Ethernet.
4. From the Work with Communication Resources display, select option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet resource, 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. If you use the same names for the line descriptions and their associated virtual Ethernet, such as VETH0, 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 line on partition B to create an Ethernet line description for partition B.

   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.

What to do next

Turn on IP datagram forwarding

Step 3: Turn on IP datagram forwarding

Turn on IP datagram forwarding so that the packets can be forwarded among different subnets.

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.

| **What to do next**

| Create the interfaces

| # Step 4: Create the interfaces
| To create the TCP/IP interfaces, complete these steps:
| 1. Create an OS/400 TCP/IP interface on partition A. 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 `'10.1.1.2'`.
| 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'`.
| 2. Start the interface. On the Work with TCP/IP Interfaces display, select option 9 (Start) by the interface.
| 3. Repeat steps 2 and 3 to create and start the TCP/IP interfaces on partition A and partition B.
| These interfaces are used for the virtual Ethernet. Use IP addresses 10.1.10.1 and 10.1.10.2 for these
| interfaces and the subnet mask 255.255.255.0.

| # Virtual Ethernet considerations

| You can use virtual Ethernet as an alternative to using a network card for interpartition communication.
| It enables you to establish high-speed communication between logical partitions without purchasing
| additional hardware. For each of the 16 ports enabled, the system creates a virtual Ethernet
| communications port, such as CMN*xx* with a resource type of 268C. Logical partitions assigned to the
| same local area network (LAN) then become available to communicate through that link. A physical
| system allows you to configure up to 16 different virtual local area networks. Virtual Ethernet provides
| the same function as using a 1 Gb Ethernet adapter. Token Ring or Ethernet 10 Mbps and 100 Mbps local
| area networks are not supported with virtual Ethernet.

| Virtual Ethernet is an economical networking solution that provides substantial benefits:
| • Economical: Potentially no extra networking hardware is required. You can add partitions to the server
| and communicate with an external LAN without installing extra physical LAN cards. If the current
| server has limited available card slots in which to install additional LAN cards, then using the virtual
| Ethernet offers the capability to operate LAN-attached partitions without the requirement to upgrade
| the server.
| • Flexible: It is possible to configure a maximum of 16 distinctive connections enabling the configuration
| of selective communication paths between partitions. For added flexibility, the configuration model
| allows logical partitions to implement both a virtual Ethernet and physical LAN connection. This is a
| desirable feature when using the Linux partition to host a firewall application.
| • Fast: The virtual Ethernet emulates a 1 GB Ethernet connection and provides a fast and convenient
| communication method between partitions. This enhances the opportunity to integrate separate
| applications that run on different logical partitions.
| • Versatile: Regardless of whether your partitions are running on OS/400 or Linux, they can all be
| connected to the same virtual Ethernet.
| • Reduced congestion: By using the virtual Ethernet for interpartition communication, communication
| traffic is reduced on the external LAN. In the case of Ethernet, which is a collision-based standard, this
| will certainly help prevent a degradation of service for other LAN users.
| ≪

Chapter 9. Related information for TCP/IP setup

Now that your server is up and running, you may ask yourself, "What more can I accomplish with my server?" Listed below are the manuals and IBM Redbooks (in PDF format) and Information Center topic that relate to the TCP/IP setup topic. You can view or print the PDFs. Use the following references to make the most of TCP/IP on your iSeries server:

Manuals

- **TCP/IP Configuration and Reference** (592 KB)
  This book provides information on configuring Transmission Control Protocol/Internet Protocol (TCP/IP) and operating and managing your network.

- **Tips and Tools for Securing your iSeries** (1 MB)
  This book provides basic recommendations for using the security features of the iSeries to protect your server and its associated operations.

Redbooks

- **TCP/IP Tutorial and Technical Overview** (7 MB)
  This redbook provides information on the basics of TCP/IP.

- **TCP/IP for AS/400: More Cool Things Than Ever** (9 MB)
  This redbook includes an extensive list of common TCP/IP applications and services.

IPv6

- **The Internet Engineering Task Force (IETF)** (http://www.ietf.cnri.reston.va.us/)
  Learn about the group of individuals that develops Internet protocol, including IPv6.

- **IP Version 6 (IPv6)** (http://playground.sun.com/pub/ipng/html/ipng-main.html)
  Find current IPv6 specifications and references to several sources on IPv6.

- **IPv6 Forum** (http://www.ipv6forum.com/)
  Find news articles and events that communicate the latest IPv6 developments.

Other information
- **TCP/IP**
  This topic contains information about TCP/IP applications and services beyond the scope of configuration.

To save a PDF on your workstation for viewing or printing:
1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As...**.
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

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

Part 2. Appendixes

Appendix. Notices

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not 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.

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:

AS/400
e(logo)server
eServer
IBM
iSeries
OS/400
Redbooks

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

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

Terms and conditions 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.

IBM ®

Printed in USA