IBM

System i

Networking
TCP/IP setup

Version 5 Release 4

IBM

System i

Networking
TCP/IP setup

Version 5 Release 4

> **Note**
>
> Before using this information and the product it supports, read the information in "Notices," on page 41.

Contents

TCP/IP setup

Your IBM® System i™ product has arrived, and you are ready to put it to use. This topic provides tools and procedures for configuring TCP/IP on the i5/OS® operating system.

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 system with TCP/IP applications, protocols, and services to meet your unique needs.

Related information

Networking: TCP/IP applications, protocols, and services

What's new for V5R4

This topic highlights the changes made to this topic collection for V5R4.

IPv6 support enhancements

New Internet Protocol version 6 (IPv6) functions are consistent at the product level with their respective IPv4 counterparts.

IPv6 is now supported for the following functions:
- Loopback
- All Ethernet adapters (10/100 Mbps, 1 Gbps, and 10 Gbps)
- Virtual Ethernet between partitions

Multiple Ethernet adapters can be used simultaneously with IPv6.

IPv6 now supports the following functions:
- Multicast
- Fragmentation and reassembly
- Basic socket extensions (RFC 3494)

IPv6 configuration
- The Start and Stop TCP/IP actions on the **TCP/IP Configuration** folder were removed.
- IPv6 can be started and stopped in the same way as IPv4 with Start TCP/IP (STRTCP) and End TCP/IP (ENDTCP) commands. IPv6 cannot be started or stopped independent of IPv4.
- The IPv6 loopback interface, ::1, is automatically created by default when TCP/IP is started.
- The IPv6 Configuration Wizard was removed.
- You can use the new interface to configure Stateless Address Autoconfiguration.
- You can also use the new wizard to create IPv6 interfaces.
- The Configure, Start, Stop, and Remove functions for a line were added to the context menu in the IPv6 Stateless Address Autoconfig display.

Alias names

In IPv4 and IPv6, you can now use alias names. You can specify a name that identifies an interface in either IPv4 or IPv6, instead of using the dotted decimal notation. Interface alias names can be configured using both control language (CL) commands and iSeries Navigator.

Preferred interface list

You can now create a preferred interface list to select which adapters and IP addresses will be the preferred interface for the virtual IP address proxy Address Resolution Protocol (ARP) agent selection. This is available for both virtual IP addresses and virtual Ethernet.

What's changed for v5r4

Tunnels are no longer supported in IPv6:
- IPv6, IPv4, and Point-to-Point Protocol over Ethernet (PPPoE) can be used on the same adapter.
- Network routers can be used to send IPv6 packets over an IPv4 network.

IPv6 configurations from previous releases will not be migrated to V5R4.

How to see what's new or changed

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

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

Printable PDF

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

To view or download the PDF version of this document, select TCP/IP setup (about 660 KB).

Saving PDF files

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

Downloading Adobe Reader

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

Internet Protocol version 6

The Internet Protocol version 6 (IPv6) plays a key role in the future of the Internet, and you can use IPv6 on the i5/OS operating system. This topic describes IPv6 and how it is being implemented.

IPv6 is the updated version of IPv4 and is gradually replacing IPv4 as the Internet standard.

IPv6 overview

You will find information about why Internet Protocol version 6 (IPv6) is replacing Internet Protocol version 4 (IPv4) as the Internet standard, and how you can use it to your advantage.

IPv6 is the next evolution in Internet Protocol. Most of the Internet uses IPv4, and this protocol has been reliable and resilient for over 20 years. However, IPv4 has limitations that might cause 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 provides 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 do not have to renumber your device addresses when you change to a different Internet service provider (ISP). Site renumbering is an important architectural element of IPv6, and is largely automatic. The lower half of your IPv6 address will remain unchanged, because this is traditionally the MAC address of your Ethernet adapter. A new IPv6 prefix will be assigned to you by the ISP, and this new prefix can be distributed to all of the end hosts by updating the IPv6 routers in the network and allowing IPv6 stateless autoconfiguration to "re-learn" the new prefix.

The IPv6 autoconfiguration feature automatically configures interface addresses and default routes for you. In stateless autoconfiguration, IPv6 takes the MAC address of the machine and a network prefix provided by a local router and combines these two addresses to create a new, unique IPv6 address. This feature eliminates the need for a Dynamic Host Configuration Protocol (DHCP) server.

Related concepts

"Available IPv6 functions"
IBM is implementing IPv6 on i5/OS over several software releases. IPv6 functions are transparent to existing TCP/IP applications and coexist with IPv4 functions.

Related reference

"Related information for IPv6" on page 16
Use these resources to help you understand IPv6.

Available IPv6 functions

IBM is implementing IPv6 on i5/OS over several software releases. IPv6 functions are transparent to existing TCP/IP applications and coexist with IPv4 functions.

These are the main i5/OS features that are affected by IPv6:

- **Configuration**

By specifying the Start IPv6 (STRIP6) parameter on the Start TCP/IP (STRTCP) command, you can start IPv6 optionally when TCP/IP starts. By default, the Start IPv6 (STRIP6) parameter on the Start TCP/IP (STRTCP) command is set to *YES.

If you configure IPv6, you are sending IPv6 packets over an IPv6 network. See "Scenario: Creating an IPv6 local area network" on page 15 for a scenario that describes a situation in which you configure IPv6 on your network.

The Start and Stop menu items on the **TCP/IP Configuration** folder are removed. IPv6 can be started and stopped in the same way as IPv4, with STRTCP and ENDTCP commands. IPv6 cannot be started or stopped independent of IPv4.

The Configure IPv6 wizard is removed from iSeries Navigator. The line configuration options in the wizard are replaced by actions on individual lines in the **Lines** folder. Similarly, you can use a new wizard to create IPv6 interfaces. For more information about the new features, see "Configuring IPv6" on page 21 to configure your network for IPv6.

- **Sockets**

  Develop and test sockets applications using IPv6 application programming interfaces (APIs) and tools. IPv6 enhances sockets so that applications can use IPv6 using a new address family, which is AF_INET6. These enhancements do not affect existing IPv4 applications. You can create applications that use concurrent IPv4 and IPv6 traffic or IPv6-only traffic.

- **DNS**

  Domain Name System (DNS) supports AAAA addresses and a new domain for reverse lookups, which is IP6.ARPA. The DNS retrieves IPv6 information; however, i5/OS 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. These tools now support the IPv6 address format. See TCP/IP troubleshooting to solve problems for both IPv4 and IPv6 networks.

  Related concepts

  "IPv6 overview" on page 3
  You will find information about why Internet Protocol version 6 (IPv6) is replacing Internet Protocol version 4 (IPv4) as the Internet standard, and how you can use it to your advantage.

  Related reference

  "Related information for IPv6" on page 16
  Use these resources to help you understand IPv6.

IPv6 concepts

Before implementing IPv6 on your system, you can read about the basic IPv6 concepts, such as IPv6 address formats, IPv6 address types, and neighbor discovery.

If you are not 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.

  Related concepts

  "Scenario: IPv6" on page 15
  These examples can help you understand situations in which you use IPv6 for your business and how to set up your network.

IPv6 address formats

The size and format of the IPv6 address expand addressing capability.

The IPv6 address size is 128 bits. The preferred IPv6 address representation is: x:x:x:x:x:x:x:x, where each x is the hexadecimal values of the eight 16-bit pieces of the address. 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 might 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` can 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` can be written as `ff06::c3`. Double colons can be used only once in an IP address.

An alternative format for IPv6 addresses combines the colon and dotted notation, so the IPv4 address can 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.

IPv4-mapped IPv6 address uses this alternative format. 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).

All of these formats are valid IPv6 address formats. You can specify these IPv6 address formats in iSeries Navigator except IPv4-mapped IPv6 address.

IPv6 address types
IPv6 addresses are categorized into these 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.

The two regular 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.

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

There are two special unicast addresses defined:

Unspecified address
The unspecified address is `0:0:0:0:0:0:0:0`. You can abbreviate the address with two colons (`::`). The unspecified address indicates the absence of an address, and it can never be assigned to a host. It can 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 if an address is used by 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`. You can abbreviate the address as `::1`. The loopback address is used by a node to send a packet to itself.

Anycast address
An 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. i5/OS does not 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 i5/OS currently provides basic support for multicast
| addressing.

Neighbor discovery

Neighbor discovery allows hosts and routers to communicate with one another.

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 is used by hosts to automatically create 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 (www.rfc-editor.org/rfcsearch.html) .

Stateless address autoconfiguration

Stateless address autoconfiguration automates some of the network administrator's tasks.

| 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 an identifier derived from 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).

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.

Comparison of IPv4 and IPv6

You might wonder how IPv6 differs from IPv4. This table allows you to quickly look up specific
functions and compare their use in each Internet Protocol.

IBM is implementing IPv6 on i5/OS over several software releases. However, IPv6 is now product-ready.

You can select an attribute from this list to link to the comparison in the table.
- Address
- Address allocation
- Address lifetime
- Address mask
- Address prefix
- Address Resolution Protocol (ARP)
- Address scope
- Address types
- Communications trace
- Configuration
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- File Transfer Protocol (FTP)
- Fragments
- Host table
- Interface
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)
- IP header
- IP header options
- IP header protocol byte
- IP header Type of Service (TOS) byte
- iSeries Navigator support
- LAN connection
- Layer 2 Tunnel Protocol (L2TP)
- Loopback address
- Maximum Transmission Unit (MTU)
- Netstat
- Network Address Translation (NAT)
- Network table
- Node info query
- Packet filtering
- Packet forwarding
- PING
- Point-to-Point Protocol (PPP)
- Port restrictions
- Ports
- Private and public addresses
- Protocol table
- Quality of service (QoS)
- Renumbering
- Route
- Routing Information Protocol (RIP)
- Services table
- Simple Network Management Protocol (SNMP)
- Sockets API
- Source address selection
- Starting and stopping
- Telnet
- Trace route
- Transport layers
- Unspecified address
- Virtual private network (VPN)

Description	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 can 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 derived from 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 larger 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 can be omitted. The double colon (::) can 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 IPv4-mapped IPv6 address. (See RFC 3513 for details. To view this RFC, see RFC Editor (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 for new connections if an equally good preferred address is available. After the valid lifetime expires, the address is not used (recognized) as a valid destination IP address for incoming packets or used as a source IP address. 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).

Description	IPv4	IPv6
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 no 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 two defined scopes, including link-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 must 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 the system.	Same for IPv6, and IPv6 is supported.
Configuration	You must configure a newly installed system before it can communicate with other systems; that is, IP addresses and routes must be assigned.	Configuration is optional, depending on functions required. IPv6 can be used with any Ethernet adapter and can be run over the loopback interface. IPv6 interfaces are self-configuring using IPv6 stateless autoconfiguration. You can also manually configure the IPv6 interface. 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.

Description	IPv4	IPv6
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()` only supports IPv4. For IPv6, a new `getaddrinfo()` API is used to obtain (at application choice) IPv6 only, or IPv4 and IPv6 addresses. For IPv6, the domain used for reverse 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. i5/OS supports a DHCP server for IPv4.	The i5/OS implementation of DHCP does not support IPv6.
File Transfer Protocol (FTP)	File Transfer Protocol allows you to send and receive files across networks.	The i5/OS implementation of 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. The fragmentation extension header is used.
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 an AAAA record in a DNS for IPv6 domain resolution. You can run the DNS locally on the same system as the resolver, or you can 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.

Description	IPv4	IPv6
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 might 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 supports some extension headers.
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 complete configuration solution for TCP/IP.	Same for IPv6. No CL commands are available for IPv6 configuration.
LAN connection	Used by an IP interface to get to the physical network. Many types exist; for example, token ring, and Ethernet. Sometimes referred to as the physical interface, link, or line.	IPv6 can be used with any Ethernet adapters and is also supported over virtual Ethernet between logical partitions.
Layer 2 Tunnel Protocol (L2TP)	L2TP can be thought of as virtual PPP, and works over any supported line type.	Currently, the i5/OS implementation of L2TP does not support IPv6.
Loopback address	An interface with an 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. The single loopback address is 0000:0000:0000:0000:0000:0000:0000:0001 or ::1 (shortened version). The virtual physical interface is named *LOOPBACK.

Description	IPv4	IPv6
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 the 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.	You cannot use packet filtering with IPv6.
Packet forwarding	The i5/OS TCP/IP stack 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.	IPv6 packets are not forwarded.
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 dialup interfaces over various modem and line types.	Currently, the i5/OS implementation of PPP does not support IPv6.
Port restrictions	These i5/OS panels allow a customer to configure a selected port number or port number ranges for TCP or UDP so that they are only available for a specific profile.	Same for IPv6. Port restrictions for IPv6 are identical to those available in 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.

Description	IPv4	IPv6
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).
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 can be used with IPv6 without change.
Quality of service (QoS)	Quality of service allows you to request packet priority and bandwidth for TCP/IP applications.	Currently, the i5/OS implementation of QoS does not support IPv6.
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 largely automatic, especially within the /48 prefix.
Route	Logically, a mapping of a set of IP addresses (might contain only one) 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, similar to IPv4. One important difference: IPv6 routes are associated (bound) to a physical interface (a link, such as ETH03) rather than an interface. One reason that a route is associated with a physical interface is because source address selection functions differently for IPv6 than for IPv4. See Source address selection.
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 i5/OS, a configurable table that associates a service name with a port and protocol; for example, service name FTP-control, port 21, TCP, and User Datagram Protocol (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.

Description	IPv4	IPv6
Simple Network Management Protocol (SNMP)	SNMP is a protocol for system management.	Currently, the i5/OS implementation of SNMP does not support 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 Using AF_INET6 address family for more information about 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 can 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 because 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. The IPv6 loopback interface, `::1`, will automatically be defined and activated when IPv6 is started.
Telnet	Telnet allows you to log on and use a remote computer as though you were connected to it directly.	Currently, the i5/OS implementation of 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.	The same transports exist in 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.

Description	IPv4	IPv6
Virtual private network (VPN)	Virtual private network (using IPsec) allows you to extend a secure, private network over an existing public network.	Currently, the i5/OS implementation of VPN does not support IPv6.

Scenario: IPv6

These examples can help you understand situations in which you use IPv6 for your business and how to set up your network.

Note: In the scenario, the IP addresses x:x:x:x:x:x:x:x represent link-local IP addresses. All addresses used in the scenario are for example purposes only.

Related concepts

"Configuring IPv6" on page 21
You can use these instructions to configure your system for IPv6 functions.

"IPv6 concepts" on page 4
Before implementing IPv6 on your system, you can read about the basic IPv6 concepts, such as IPv6 address formats, IPv6 address types, and neighbor discovery.

Scenario: Creating an IPv6 local area network

This scenario shows the prerequisites and the configuration steps for setting up an IPv6 local area network.

Situation

Because IPv6 will eventually replace IPv4 as the Internet standard, your company is implementing IPv6 for its financial operations. It has purchased 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 system connected to the site Ethernet local area network (LAN). Your job is to configure your system for IPv6 so that your firm can start using the accounting application. The following figure illustrates the network setup in this scenario.

Accounting Department IPv6 network
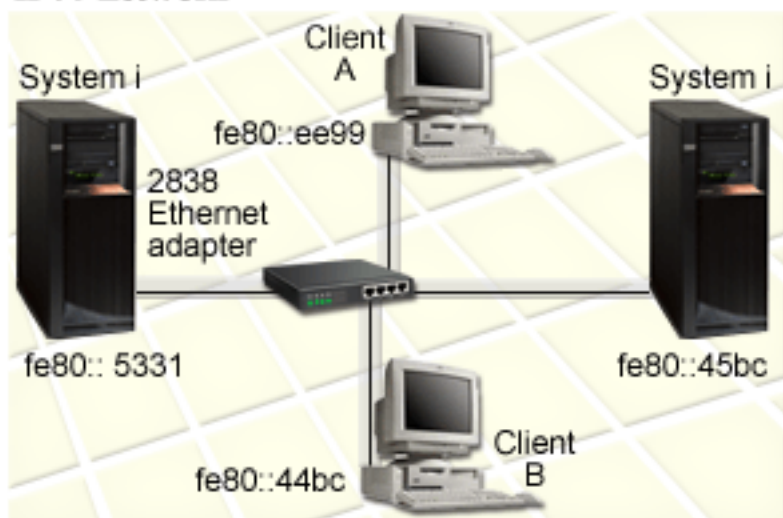
| **Solution**

| To create an IPv6 LAN, you must configure an Ethernet line description. IPv6 packets travel between
| various systems on the network while employees use the accounting application.

| Setup requirements include:
| • i5/OS Version 5 Release 4
| • iSeries Access for Windows® and iSeries Navigator (Network component of iSeries Navigator)
| • The system must first have TCP/IP configured and have an IPv4 address because IPv6 must be
| configured through iSeries Navigator. Currently iSeries Navigator can only connect to the network
| using IPv4. If you have not configured the system for IPv4, see Configuring TCP/IP for the first time
| before you configure IPv6 on your system.

| **Configuration**

| To configure IPv6, you must use iSeries Navigator. IPv6 can only be configured from iSeries Navigator,
| and cannot be configured from the character-based interface.

| Start the IPv6 stack using the STRIP6 (*YES) parameter on the Start TCP/IP (STRTCP) command. Use the
| actions on individual lines in the **Lines** folder to specify line configuration options. For information about
| having IPv6 addresses configured automatically by the iSeries Navigator, see "Configuring IPv6 stateless
| address autoconfiguration" on page 22.

IPv6 troubleshooting

If you have IPv6 configured on i5/OS, you can 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
can use them to test connections and routes for both types of networks. In addition, you can 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**

>   Communications trace

>   TCP/IP troubleshooting

Related information for IPv6

Use these resources to help you understand IPv6.

• The Internet Engineering Task Force (IETF) (http://www.ietf.org/)

   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 (www.ipv6forum.com/)

   Find news and events that communicate the latest IPv6 developments.

Planning TCP/IP setup

Before you begin to install and configure your system, take a few moments to plan the operation. This
topic helps you prepare for the installation and configuration of TCP/IP on i5/OS.

The planning guidelines in this topic pertain to basic TCP/IP setup using IPv4. If you intend to configure IPv6, see Configuring IPv6 for setup requirements and configuration instructions.

Gathering TCP/IP configuration information

You must gather and record basic configuration information that is required to set up TCP/IP.

Print this page and record the configuration information about your system and the TCP/IP network to which you are connecting. You must 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 the IBM Redbook TCP/IP for AS/400®: More Cool Things Than Ever for information about basic installation and configuration procedures.

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 system		199.5.83.158
Subnet mask for your system		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 command line, type go hardware, and press Enter.
2. To select Option 1 (Work with communication resources), 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 Installing TCP/IP

TCP/IP security considerations

When planning your TCP/IP configuration for a System i platform, 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 NO.
- **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 signon.** Applications such as FTP and Telnet are more vulnerable to outside attack. For details on how to control your exposure, read the topic on controlling interactive signon in Signon system values.

  Related information

  System i and Internet security

Installing TCP/IP

Base TCP/IP support is included with the i5/OS operating system and allows you to connect the system to a network.

If you want to use any TCP/IP applications, such as Telnet, FTP, and SMTP, you also need to install IBM TCP/IP Connectivity Utilities for i5/OS. TCP/IP Utilities is a separately installable licensed program. To install TCP/IP Utilities on your system, follow these steps:

1. Insert your installation media for TCP/IP into your system. 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 (IBM TCP/IP Connectivity Utilities for i5/OS). 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 reinstall TCP/IP Connectivity Utilities. If the problem is not resolved, you might need to contact support.

Note: Other licensed programs that you might want to install include:
- • IBM eServer™ iSeries Access for Windows (5722–XE1) provides iSeries Navigator support that is used to configure some of the TCP/IP components.
- • IBM HTTP Server for i5/OS (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.

Configuring TCP/IP

You might be configuring TCP/IP for the first time, or you might be changing an existing configuration to use the IPv6 function. This topic shows you how to configure TCP/IP. In addition, you can see instructions for configuring IPv6.

Before you use this information to configure TCP/IP, see Hardware installation and use to ensure you have installed all the necessary hardware components.

Configuring TCP/IP for the first time

If you are setting up a new system, you can use these instructions to establish a connection and configure TCP/IP for the first time.

Select one of the following methods for setting up TCP/IP on your new system.

Configuring TCP/IP using the EZ-Setup wizard

If your PC is equipped to use the EZ-Setup wizard, you can use this preferred method to configure TCP/IP. The EZ-Setup wizard is packaged with your System i product.

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 system because the interface is easy to use. The CD-ROM containing the EZ-Setup wizard is packaged with your System i product.

To configure your system, follow these steps:
1. Access the EZ-Setup wizard from the CD-ROM that is packaged with your system.
2. Follow the wizard's instructions to configure TCP/IP.
3. Start TCP/IP.
    a. In iSeries Navigator, expand *your system* → **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 system. Use iSeries Navigator to modify the configuration as your networking needs change.

See Customizing TCP/IP with iSeries Navigator to add routes and interfaces or Configuring IPv6 to use Internet Protocol version 6 on your network.

Configuring TCP/IP using the character-based interface

You can use the character-based interface to configure TCP/IP for your System i product 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 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 about this type of authority, see the chapter on user profiles in

Security Reference .

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

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

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

Configuring a line description (Ethernet):

Use these instructions to configure TCP/IP over an Ethernet communications adapter.

To configure a line description, follow these steps:
1. On the command line, type CRTLINETH to access the Create Line Desc (Ethernet) (CRTLINETH) prompt panel, and then press Enter.
2. Specify the line name. (Use any name.)
3. Specify the resource name.
4. Press Enter several times to run the command.

Turning on IP datagram forwarding:

You need to 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. On the command line, type CHGTCPA, and then press F4.
2. At the *IP datagram forwarding* prompt, type *YES.

Configuring an interface:

Now you need to configure a TCP/IP interface for your system.

To configure an interface, follow these steps:
1. On the command line, type CFGTCP to access the Configure TCP/IP menu, and then press Enter.
2. Select Option 1 (Work with TCP/IP interfaces) on the Configure TCP/IP menu, and then press Enter.
3. Specify Option 1 (Add) to show the Add TCP/IP Interface display, and then press Enter.
4. Specify the address value that you want to represent your system, the subnet mask address, and the line description name that you previously defined, and then press Enter.

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

Configuring a route:

To reach remote networks, at least one routing entry is required.

If no routing entries are manually added, you cannot reach systems that are not on the same network to which the system is attached. You must also add routing entries to allow TCP/IP clients that are attempting to reach your system 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 then press Enter.
2. Select Option 1 (Add) to show the Add TCP/IP Route (ADDTCPRTE) display, and then press Enter.
3. Specify *DFTROUTE for the route destination, specify *NONE for the subnet mask, specify the IP address for the next hop, and then press Enter.

Defining local domain and host names:

After specifying the routing entries, you need to define the local domain and host names to allow communication within the network.

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 then press Enter.
2. Specify the names you selected to be the local host name and local domain name, leaving the other parameters at the default values, and press Enter.

Defining a host table:

You must define the host table to allow communication with the hosts on the network.

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 then press Enter.
2. Specify Option 1 (Add) to show the Add TCP/IP Host Table Entry display, and then 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 steps 1 to 4 for each of the other hosts on the network to which you want to communicate with by name, and add an entry for each.

Starting 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. TCP/IP interfaces and servers that specify AUTOSTART *YES, PPP profiles, and IPv6 can all be started optionally.

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

Configuring IPv6

You can use these instructions to configure your system for IPv6 functions.

If you are unfamiliar with IPv6, see Internet Protocol version 6 for an overview. You must have TCP/IP configured on the system before you can configure IPv6.

You are ready to take advantage of the next-generation Internet by using IPv6 on your network. To use IPv6, you can configure it on an existing line by manually configuring interfaces, by utilizing the IPv6 Stateless Address Autoconfiguration feature, or both.

Related concepts

"Scenario: IPv6" on page 15
These examples can help you understand situations in which you use IPv6 for your business and how to set up your network.

Hardware and software requirements

Listed here are the hardware and software requirements for configuring i5/OS for IPv6.

Configuring an Ethernet line for IPv6

Your system should meet these requirements to configure IPv6 on an Ethernet line:

- i5/OS Version 5 Release 4.
- iSeries Access for Windows and iSeries Navigator:
  - Network component of iSeries Navigator.
- IPv6-capable router, if you want to send IPv6 traffic beyond the immediate LAN.
- TCP/IP (using IPv4), configured because TCP/IP must be running on the system. If you have not configured your system for IPv4, see Configuring TCP/IP for the first time before configuring the line for IPv4.

Configuring IPv6 stateless address autoconfiguration

To use IPv6 on your System i product, you can use the IPv6 stateless address autoconfiguration feature.

To configure IPv6 stateless address autoconfiguration, follow these steps:

1. In iSeries Navigator, expand **Network** → **TCP/IP Configuration** → **Lines**.
2. Right-click one of the lines in the right panel and select **IPv6 Stateless Address Autoconfig** → **Configure**.
3. Right-click the line you have configured, and select **IPv6 Stateless Address Autoconfig** → **Start**.

You can also configure IPv6 stateless address autoconfiguration by following these steps:

1. In iSeries Navigator, expand **Network** → **TCP/IP Configuration** → **Lines**.
2. Right-click **Lines**, and then select **Configure IPv6 Stateless Address Autoconfig**.

Note: To ensure that it is started automatically when you start TCP/IP, select **Start when TCP/IP is started** in the Configure Line for IPv6 display.

Creating a new IPv6 interface

You can also use IPv6 by using the new wizard to manually create a new IPv6 interface.

To create a new IPv6 interface, follow these steps:

1. In iSeries Navigator, expand **Network** → **TCP/IP Configuration** → **IPv6**.
2. Right-click **Interface**, and then select **New Interface**.
3. Follow the steps in the New IPv6 Interface wizard to create the new IPv6 interface. The new interface appears in the right panel when you finish the configuration.
4. Right-click the new IPv6 interface, and then select **Start**.
   You can also check the **Start when TCP/IP is started** check box in the New IPv6 Interface wizard to ensure that it starts automatically the next time that you start TCP/IP.
5. In iSeries Navigator, select **Network** → **TCP/IP Configuration** → **Utilities** → **Ping** to test the new IPv6 interface and verify that it connects to the network.

Note: The New Interface menu item is enabled only if you have *IOSYSCFG authority.

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

If you need to run TCP/IP while the operating system is in restricted state, you can use the method outlined in this topic.

Situation

As the network administrator, you need to obtain backup status reports for your system. When you are running backup procedures, the operating system must be in restricted state to prevent users from changing any configuration. Because you are remote, you access status reports using a personal digital assistant (PDA) device (or any TCP/IP networking device). The PDA uses a socket-enabled application that requires an active TCP/IP interface that is available to communicate with the system. 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 following information provides more detail.

Restrictions

The following restrictions apply when the operating system is running in restricted state:

- You cannot start TCP/IP servers (STRTCPSRV CL command), because they require active subsystems.
- You can only start interfaces that are not attached to a network server description (NWSD) or a network interface description (NWID).

Configuration steps

1. Start TCP/IP using special parameters.

   In order to start TCP/IP while in restricted state, enter the command: `STRTCP STRSVR(*NO) STRIFC(*NO) STRPTPPRF(*NO) STRIP6(*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 specifies a virtual IP address or uses a line description of *ELAN, *TRLAN, or *DDI.

      To view the line type for your interface, enter `CFGTCP` (the Configure TCP/IP command) at a command line interface 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 an NWID or NWSD, enter `DSPLIND abc` (where `abc` is the name of your line description) from a command line interface. Verify that the Resource name is not *NWID or *NWSD.

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

   c. Start the interface. At a command line interface, enter `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, review Tools to verify your network structure within TCP/IP troubleshooting.

Customizing TCP/IP with iSeries Navigator

iSeries Navigator also provides you with many options that you can use to customize your configuration.

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

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

Changing TCP/IP settings

You can view and change your TCP/IP settings using iSeries Navigator.

For instance, you can change properties for host or domain names, name server, host table entries, system attributes, port restrictions, servers, or client connections. You can 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 system* → **Network**.
2. Right-click **TCP/IP Configuration** and select **Properties** to open the **TCP/IP Properties** dialog box.
3. Select the tabs at the top of the dialog box to view and edit TCP/IP information.

To add and change host table entries, follow these steps:
1. In iSeries Navigator, select *your system* → **Network**.
2. Right-click **TCP/IP Configuration** and select **Host Table** to open the **Host Table** dialog box.
3. Use the **Host Table** dialog box 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 system* → **Network**.
2. Right-click **IPv4** and select **Properties** to open the **IPv4 Properties** dialog box.
3. Select the tabs at the top of the dialog box 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 system* → **Network**.
2. Right-click **IPv6** and select **Properties** to open the **IPv6 Properties** dialog box.
3. Select the tabs at the top of the dialog box to view and edit the IPv6 property settings.

Configuring IPv6

To configure IPv6, you must change the system's configuration by using the iSeries Navigator.

See "Configuring IPv6" on page 21 for instructions and special requirements. If you are unfamiliar with IPv6, see "Internet Protocol version 6" on page 2 for an overview.

Adding IPv4 interfaces

Using iSeries Navigator, you can create new IPv4 interfaces for your system.

To create a new IPv4 interface, follow these steps:
1. In iSeries Navigator, select *your system* → **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.

Adding IPv6 interfaces

Using the wizard in iSeries Navigator, you can add new IPv6 interfaces for your system.

To create a new IPv6 interface, follow these steps:
1. In iSeries Navigator, select *your system* → **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.

Adding IPv4 routes

By following the wizard in iSeries Navigator, you can configure new IPv4 routes for your system.

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 system* → **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.

Adding IPv6 routes

To configure new IPv6 routes, you can also use iSeries Navigator.

Any changes that you make to the routing information take effect immediately.
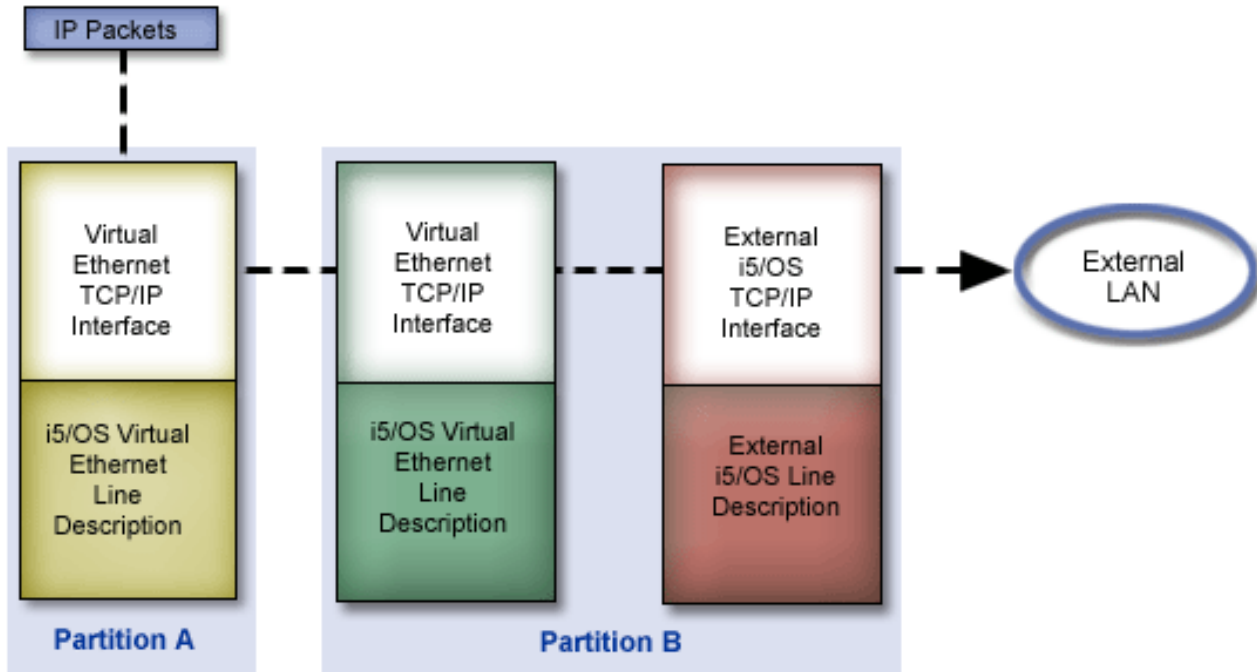
To configure a new IPv6 route, follow these steps:
1. In iSeries Navigator, select *your system* → **Network** → **TCP/IP Configuration** → **IPv6**.
2. Right-click **Routes**, and select **New Route**.
3. Follow the wizard's instructions to configure a new IPv6 route.

TCP/IP techniques connecting virtual Ethernet to external LANs

Different TCP/IP techniques can be used to connect the virtual Ethernet network to an external LAN. You can take advantage of virtual Ethernet on the i5/OS operating system.

If you are using a virtual Ethernet network for interpartition communication, you might need to enable these partitions to communicate with a physical, external LAN. 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.

Virtual Ethernet TCP/IP Interface — i5/OS Virtual Ethernet Line Description — **Partition A**

Virtual Ethernet TCP/IP Interface — i5/OS Virtual Ethernet Line Description / External i5/OS TCP/IP Interface — External i5/OS Line Description — **Partition B**

External LAN

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 method
- Network address translation method
- TCP/IP routing method

Proxy Address Resolution Protocol method

This proxy Address Resolution Protocol (ARP) method uses transparent subnetting to associate a partition's virtual interface with an external interface.

The proxy ARP function is built into the TCP/IP stack. It is suggested that you use this method if you have the necessary IP addresses.
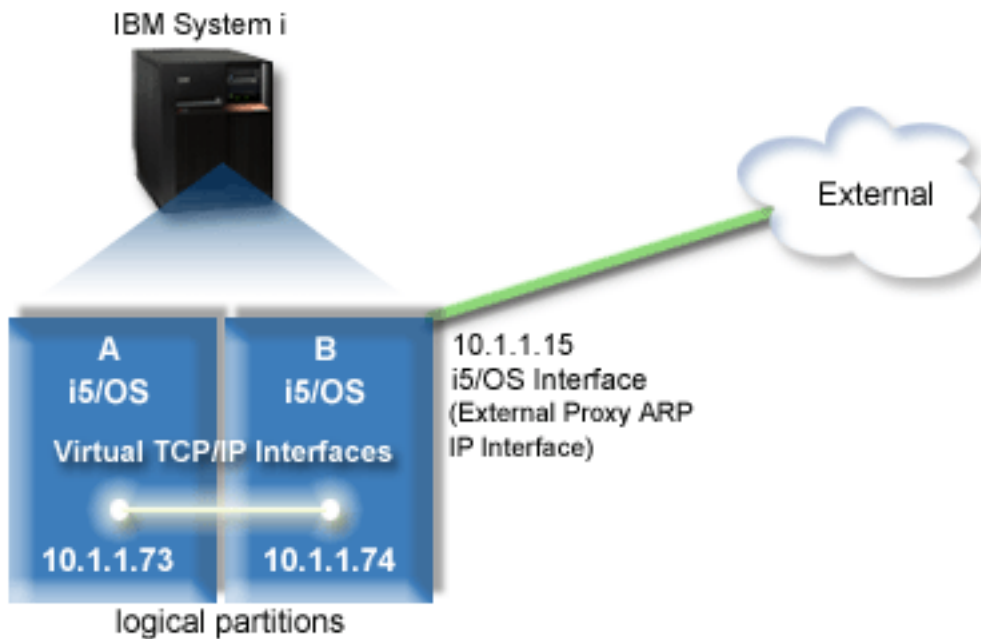
You might want to learn more information about transparent subnetting:

- V4 TCP/IP for AS/400: More Cool Things Than Ever

  This IBM Redbook provides scenarios that demonstrate common solutions with example configurations. It also helps you plan, install, tailor, configure, and troubleshoot TCP/IP on i5/OS.
- 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. Because 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.

IBM System i

External

A
i5/OS

B
i5/OS

Virtual TCP/IP Interfaces

10.1.1.73   10.1.1.74

10.1.1.15
i5/OS Interface
(External Proxy ARP
IP Interface)

logical partitions

In this example, TCP/IP traffic from partition A runs across the virtual Ethernet to the 10.1.1.74 interface on partition B. Because 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.

Step 1: Enabling logical partitions to participate in a virtual Ethernet

The first step for associating the virtual interface with an external interface is to enable virtual Ethernet.

Note: If you are setting up virtual Ethernet on model 5*xx*, see Virtual Ethernet for i5/OS logical partitions in the IBM Systems Hardware Information Center for the instructions.

To enable virtual Ethernet, follow these steps:
1. On the command line on the primary partition (partition A), type STRSST, and then press Enter.
2. Type your service tools user ID and password.
3. From the System Service Tools (SST) panel, select Option 5 (Work with System Partitions).
4. From the Work with System Partitions panel, 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.
   Related information
   Consolidating i5/OS, AIX®, and Linux® partitions on your IBM eServer™ i5 system

Step 2: Creating Ethernet line descriptions

You need to perform this step in one of two ways depending on the model you are using. Select the appropriate procedure for your particular model.

Creating Ethernet line descriptions on models 270 and 8*xx*:

Use these steps to create an Ethernet line description on models 270 and 8*xx* so that the system can use virtual Ethernet.

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

1. On the command line on partition A, type WRKHDWRSC *CMN, and then press Enter.
2. From the Work with Communication Resources panel, 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 is one port for each virtual Ethernet that is connected to the logical partition.
3. From the Display Resource Detail panel, 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 panel, select Option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet port, and then press Enter.
5. From the Work with Configuration Descriptions panel, select Option 1 (Create), and then press Enter to see the Create Line Description Ethernet (CRTLINETH) panel.
   a. At 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. At the *Line speed* prompt, type 1G.
   c. At the *Duplex* prompt, type *FULL, and then press Enter.
   d. At the *Maximum frame size* prompt, type 8996, and then 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 then 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 the 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: Turning on IP datagram forwarding

Creating the Ethernet line descriptions on systems other than models 270 and 8xx:

Use these steps to create an Ethernet line description on models other than 270 and 8*xx* so that the system can use virtual Ethernet.

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

1. On the command line on partition A, type WRKHDWRSC *CMN, and then press Enter.
2. From the Work with Communication Resources panel, 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 is 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 panel, 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 panel, select Option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet resource, and then press Enter.
5. From the Work with Configuration Descriptions panel, select Option 1 (Create), and then press Enter to see the Create Line Description Ethernet (CRTLINETH) panel.

a. At 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. At the *Line speed* prompt, type 1G.

c. At the *Duplex* prompt, type *FULL, and then press Enter.

d. At the *Maximum frame size* prompt, type 8996, and then 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 then 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 the 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: Turning on IP datagram forwarding

Step 3: Turning 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. On the command line on partition B, type CHGTCPA and press F4.

2. At the *IP datagram forwarding* prompt, type *YES.

Step 4: Creating the interface to enable proxy ARP

You need to create an external 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.

   Because 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 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 i5/OS 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. On the command line on partition B, type CFGTCP, and then press Enter to see the Configure TCP/IP panel.

   b. Select Option 1 (Work with TCP/IP Interfaces), and then press Enter.

   c. Select Option 1 (Add), and then press Enter to see the Add TCP/IP Interface (ADDTCPIFC) panel.

   d. At the *Internet address* prompt, type '10.1.1.15'.

   e. At the *Line description* prompt, type the name of your line description, such as ETHLINE.

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

3. Start the interface. On the Work with TCP/IP Interfaces panel, select Option 9 (Start) by the interface.

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

You need to specify the virtual TCP/IP interface on Partition A.

To create the virtual interface, follow these steps:

1. On the command line on partition A, type CFGTCP, and then press Enter to see the Configure TCP/IP panel.
2. Select Option 1 (Work with TCP/IP Interfaces), and then press Enter.
3. Select Option 1 (Add), and then press Enter to see the Add TCP/IP Interface (ADDTCPIFC) panel.
4. At the *Internet address* prompt, type '10.1.1.73'.
5. For the *Line description* prompt, type the name of your line description, such as VETH0.
6. At the *Subnet mask* prompt, type '255.255.255.252'.
7. Start the interface. On the Work with TCP/IP Interfaces panel, select Option 9 (Start) by the interface.

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

You need to create the virtual TCP/IP interface on Partition B.

To create the virtual interface, follow these steps:

1. On the command line on partition B, type CFGTCP, and then press Enter to see the Configure TCP/IP panel.
2. Select Option 1 (Work with TCP/IP Interfaces), and then press Enter.
3. Select Option 1 (Add), and then press Enter to see the Add TCP/IP Interface (ADDTCPIFC) panel.
4. At the *Internet address* prompt, type '10.1.1.74'.
5. For the *Line description* prompt, type the name of your line description, such as VETH0.
6. At the *Subnet mask* prompt, type '255.255.255.252'.
7. Start the interface. On the Work with TCP/IP Interfaces panel, select Option 9 (Start) by the interface.

Step 7: Creating a preferred interface list

You can now create a preferred interface list to control which adapters and IP addresses are the preferred interface for virtual Ethernet proxy Address Resolution Protocol (ARP) agent selection.

To create a preferred interface list, follow these steps:

1. In iSeries Navigator, expand **Network** ▸ **TCP/IP Configuration** ▸ **IPv4**.
2. Select **Interfaces**.
3. From the list of interfaces that are displayed, select the virtual Ethernet interface for which you want to create the preferred interface list.
4. Right-click the interface, and then click **Properties**.
5. Click the **Advanced** tab.
6. In the panel, select the interface addresses from the Available interfaces list, and click **Add**.

    You can also remove an interface from the Preferred interface list in the right pane by clicking **Remove** , or move an interface up and down the list to change the order by clicking **Move up** and **Move down**.
7. Select the **Enable proxy ARP** check box to enable the list.
8. Click **OK** to save the preferred interface list that you have just created.

    Notes:

    a. Only 10 interfaces are supported for the preferred interface list. If you configure more than 10, the list is truncated to the first 10.

    b. The interface for which you want to create the preferred interface list must be inactive for the list to be configured. Interfaces listed in the preferred interface list do not need to be inactive at the time the list is configured.

Step 8: Creating the route

Creating the default route enables the packet to exit the virtual Ethernet network.

To create the default route, follow these steps:

1. On the command line on partition A, type CFGTCP, and then press Enter.
2. Select Option 2 (Work with TCP/IP Routes), and then press Enter.
3. Select Option 1 (Add), and then press Enter.
4. At the *Route destination* prompt, type *DFTROUTE.
5. At the *Subnet mask* prompt, type *NONE.
6. At 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. Because 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.

Step 9: Verifying network communications

You can now verify your network communications.

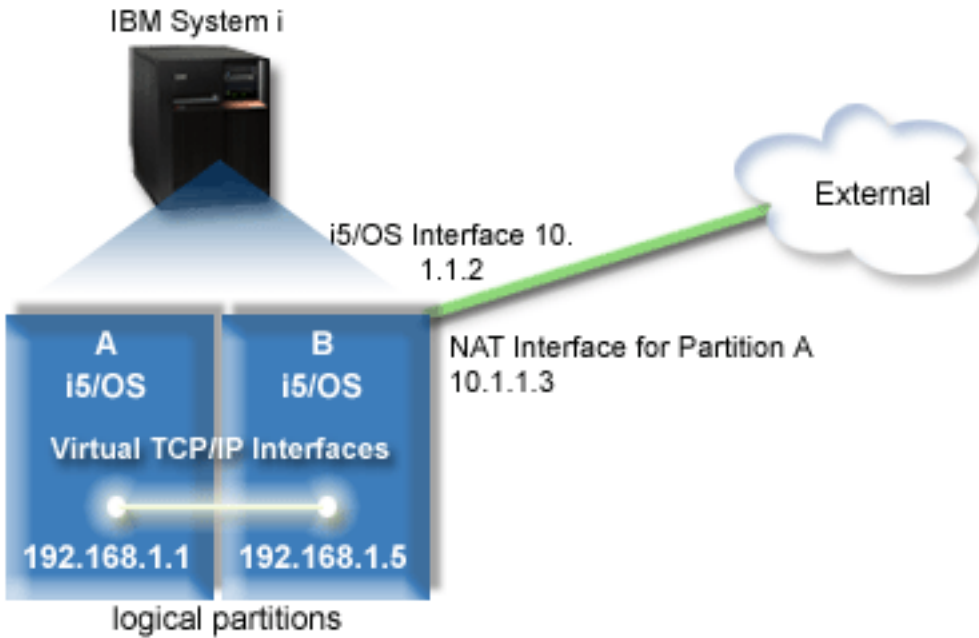To verify your network communications, use the ping command:
- From partition A, ping the virtual Ethernet interface 10.1.1.74 and an external host.
- From an external i5/OS host, ping the virtual Ethernet interfaces 10.1.1.73 and 10.1.1.74.

Network address translation method

You can use i5/OS packet filtering to route traffic between a partition and the outside network.

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 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 i5/OS network connection. Because 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 System i

i5/OS Interface 10.1.1.2

External

A
i5/OS

B
i5/OS

NAT Interface for Partition A
10.1.1.3

Virtual TCP/IP Interfaces

192.168.1.1   192.168.1.5

logical partitions

In this example, any existing TCP/IP traffic for the system runs over the 10.1.1.2 interface. A new interface, 10.1.1.3, is created for communicating between the 10.1.1.x network and the 192.168.1.x network. Because this is a static map scenario, the inbound traffic gets translated from the 10.1.1.3 interface to the 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 to communicate with one another.

To make static NAT work, you need to first set up your i5/OS 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:

Step 1: Enabling logical partitions to participate in a virtual Ethernet

The first step for associating the virtual interface with an external interface is to enable virtual Ethernet.

Note: If you are setting up virtual Ethernet on a model 5*xx*, see Virtual Ethernet for i5/OS logical partitions in the IBM Systems Hardware Information Center for the instructions.

To enable virtual Ethernet, follow these steps:

1. On the command line on the primary partition (partition A), type STRSST, and then press Enter.
2. Type your service tools user ID and password.
3. From the System Service Tools (SST) panel, select Option 5 (Work with System Partitions).
4. From the Work with System Partitions panel, 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.

   Related information

   Consolidating i5/OS, AIX®, and Linux® partitions on your IBM eServer™ i5 system

Step 2: Creating Ethernet line descriptions

You need to perform this step in one of two ways depending on the model you are using. Select the appropriate procedure for your particular model.

Creating Ethernet line descriptions on models 270 and 8*xx*:

Use these steps to create an Ethernet line description on models 270 and 8*xx* so that the system can use virtual Ethernet.

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

1. On the command line on partition A, type `WRKHDWRSC *CMN`, and then press Enter.
2. From the Work with Communication Resources panel, 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 is one for each virtual Ethernet that is connected to the logical partition.
3. From the Display Resource Detail panel, scroll down to find the port address. The port address corresponds to the virtual Ethernet that you selected during the configuration of the logical partition.
4. From the Work with Communication Resources panel, select Option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet port, and press Enter.
5. From the Work with Configuration Descriptions panel, select Option 1 (Create), and then press Enter to see the Create Line Description Ethernet (CRTLINETH) panel.

   a. At 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. At the *Line speed* prompt, type `1G`.

   c. At the *Duplex* prompt, type `*FULL`, and then press Enter.

   d. At the *Maximum frame size* prompt, type 8996, and then 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 then 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 the 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: Turning on IP datagram forwarding

Creating Ethernet line descriptions on systems other than models 270 and 8xx:

Use these steps to create an Ethernet line description on models other than 270 and 8*xx* so that the system can use virtual Ethernet.

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 then press Enter.
2. From the Work with Communication Resources panel, 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 is 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 panel, 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 panel, select Option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet resource, and then press Enter.

5. From the Work with Configuration Descriptions panel, select Option 1 (Create), and then press Enter to see the Create Line Description Ethernet (CRTLINETH) panel.

   a. At 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. At the *Line speed* prompt, type 1G.

   c. At the *Duplex* prompt, type *FULL, and then press Enter.

   d. At the *Maximum frame size* prompt, type 8996, and then 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 then 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 the 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: Turning on IP datagram forwarding

Step 3: Turning 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. On the command line on partition A, type CHGTCPA, and then press F4.

2. At the *IP datagram forwarding* prompt, type *YES.

Step 4: Creating the interfaces

To allow traffic between your virtual Ethernet network and the external network, you need to create several TCP/IP interfaces for your system.

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

1. Create and start an i5/OS TCP/IP interface on partition B for general communication to and from the system. To create the interface, follow these steps:

   a. On the command line on partition B, type CFGTCP, and then press Enter to see the Configure TCP/IP panel.

   b. Select Option 1 (Work with TCP/IP Interfaces), and then press Enter.

   c. Select Option 1 (Add), and then press Enter to see the Add TCP/IP Interface (ADDTCPIFC) panel.

   d. At the *Internet address* prompt, type '10.1.1.2'.

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

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

   g. Start the interface. On the Work with TCP/IP Interfaces panel, 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. On the command line on partition B, type CFGTCP, and then press Enter to see the Configure TCP/IP panel.

   b. Select Option 1 (Work with TCP/IP Interfaces), and then press Enter.

   c. Select Option 1 (Add), and then press Enter to see the Add TCP/IP Interface (ADDTCPIFC) panel.

   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 panel, select Option 9 (Start) by the interface.

3. Create and start the i5/OS TCP/IP interface on partition A for the virtual Ethernet. To create the interface, follow these steps:

   a. On the command line on partition A, type CFGTCP, and press Enter to see the Configure TCP/IP panel.

   b. Select Option 1 (Work with TCP/IP Interfaces), and then press Enter.

   c. Select Option 1 (Add), and press Enter to see the Add TCP/IP Interface (ADDTCPIFC) panel.

   d. At the *Internet address* prompt, type '192.168.1.1'.

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

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

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

4. Create and start the i5/OS TCP/IP interface on partition B for the virtual Ethernet. To create the interface, follow these steps:

   a. On the command line on partition B, type CFGTCP, and press Enter to see the Configure TCP/IP panel.

   b. Select Option 1 (Work with TCP/IP Interfaces), and then press Enter.

   c. Select Option 1 (Add), and press Enter to see the Add TCP/IP Interface (ADDTCPIFC) panel.

   d. At the *Internet address* prompt, type '192.168.1.5'.

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

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

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

Step 5: Verifying network communications

You can now verify your network communications.

To verify your network communications, use the ping command:

* From partition A, ping the virtual Ethernet interface 192.168.1.5 and an external host.

* From an external i5/OS host, ping each of the virtual Ethernet interfaces 192.168.1.1 and 192.168.1.5.

Step 6: Creating 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 system** → **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.

Step 7: Verifying network communications

After creating the packet rules, 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

Standard TCP/IP routing is used to route traffic to the virtual Ethernet network in the same way you define routing to any other LAN. This requires that you update routing information throughout your network.

You can also route traffic to your partitions through i5/OS with various routing techniques. This solution is not difficult to configure on the system but, depending on the topology of your network, it might not be practical to implement. Consider the following figure.
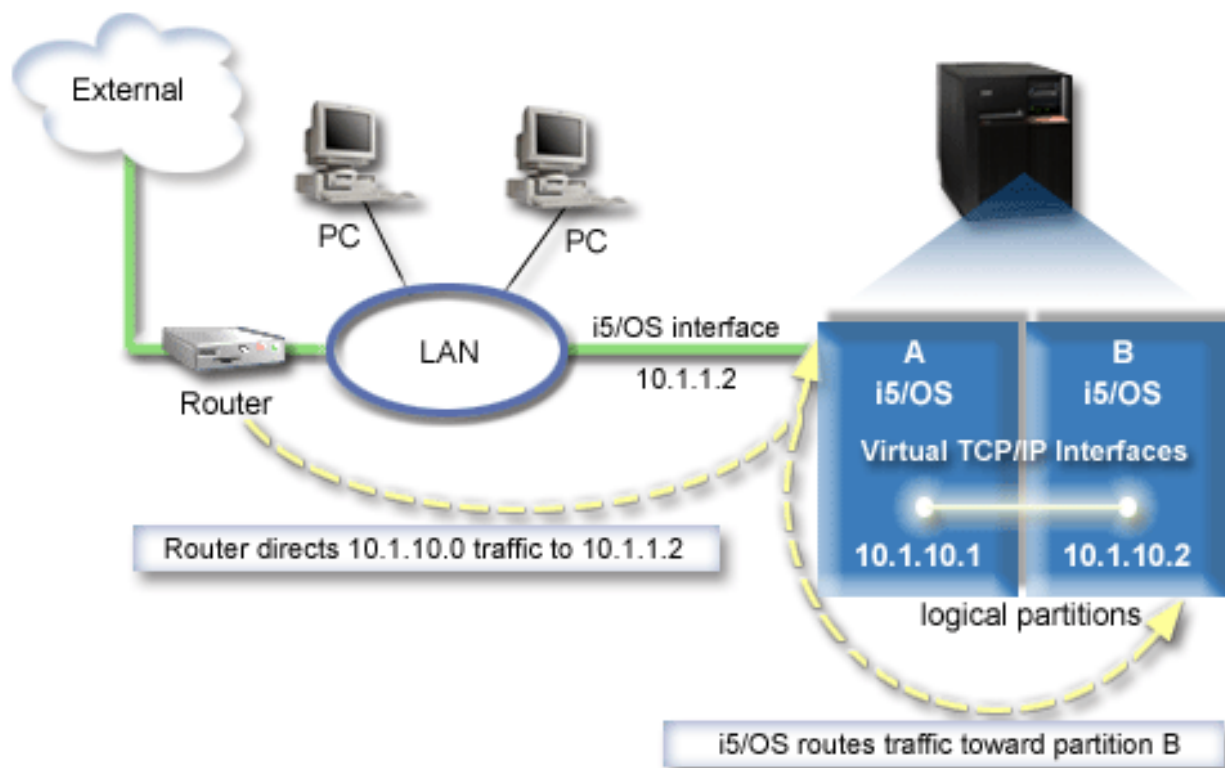
The existing TCP/IP interface (10.1.1.2) connects to the LAN. The LAN is connected to remote networks with a router. The virtual TCP/IP interface on partition B is addressed as 10.1.10.2 and the virtual TCP/IP interface on partition A as 10.1.10.1. In i5/OS, if you turn on IP datagram forwarding, i5/OS 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 system. In this scenario, you can 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 also works for the local LAN clients (clients connected to the same LAN as the System i platform) 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 i5/OS 10.1.1.2 interface; therein starts the impracticability of this method. If you have many LAN clients, then you must define many routes.

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

Step 1: Enabling logical partitions to participate in a virtual Ethernet

The first step for associating the virtual interface with an external interface is to enable virtual Ethernet.

Note: If you are setting up a virtual Ethernet on a model 5*xx*, see Virtual Ethernet for i5/OS logical partitions in the IBM Systems Hardware Information Center for the instructions.

To enable virtual Ethernet, follow these steps:

1. On the command line on the primary partition (partition A), type STRSST, and then press Enter.
2. Type your service tools user ID and password.
3. From the System Service Tools (SST) panel, select Option 5 (Work with System Partitions).
4. From the Work with System Partitions panel, 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.

   Related information

   Consolidating i5/OS, AIX®, and Linux® partitions on your IBM eServer™ i5 system

Step 2: Creating Ethernet line descriptions

You need to perform this step in one of two ways depending on the system model you are using. Select the appropriate procedure for your particular model.

Creating Ethernet line descriptions on models 270 and 8*xx*:

Use these steps to create an Ethernet line description on models 270 and 8*xx* so that the system can use virtual Ethernet.

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

1. On the command line on partition A, type WRKHDWRSC *CMN, and then press Enter.
2. From the Work with Communication Resources panel, 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 is one for each virtual Ethernet that is connected to the logical partition.
3. From the Display Resource Detail panel, 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 panel, select Option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet port, and then press Enter.
5. From the Work with Configuration Descriptions panel, select Option 1 (Create), and then press Enter to see the Create Line Description Ethernet (CRTLINETH) panel.
   a. At 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. At the *Line speed* prompt, type 1G.
   c. At the *Duplex* prompt, type *FULL, and then press Enter.
   d. At the *Maximum frame size* prompt, type 8996, and then 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 then 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 the 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: Turning on IP datagram forwarding

Creating Ethernet line descriptions on systems other than models 270 and 8xx:

Use these steps to create an Ethernet line description on models other than 270 and 8*xx* so that the system can use virtual Ethernet.

To configure new Ethernet line descriptions to support virtual Ethernet, follow these steps:
1. On the command line on partition A, type WRKHDWRSC *CMN, and then press Enter.
2. From the Work with Communication Resources panel, 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 is 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 panel, 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 panel, select Option 5 (Work with configuration descriptions) next to the appropriate virtual Ethernet resource, and then press Enter.
5. From the Work with Configuration Descriptions panel, select Option 1 (Create), and then press Enter to see the Create Line Description Ethernet (CRTLINETH) panel.
   a. At 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. At the *Line speed* prompt, type 1G.
   c. At the *Duplex* prompt, type *FULL, and then press Enter.
   d. At the *Maximum frame size* prompt, type 8996, and then 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 then 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 the 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: Turning on IP datagram forwarding

Step 3: Turning 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. On the command line on partition A, type CHGTCPA, and then press F4.
2. At the *IP datagram forwarding* prompt, type *YES.

Step 4: Creating the interfaces

To allow traffic between your virtual Ethernet network and the external network, you need to create several TCP/IP interfaces for your system.

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

1. Create an i5/OS TCP/IP interface on partition A. To create the interface, follow these steps:

    a. On the command line on partition A, type `CFGTCP`, and then press Enter to see the Configure TCP/IP panel.

    b. Select Option 1 (Work with TCP/IP Interfaces), and then press Enter.

    c. Select Option 1 (Add), and then press Enter to see the Add TCP/IP Interface (ADDTCPIFC) panel.

    d. At the *Internet address* prompt, type '`10.1.1.2`'.

    e. At the *Line description* prompt, type the name of your line description, such as ETHLINE.

    f. At the *Subnet mask* prompt, type '`255.255.255.0`'.

2. Start the interface. On the Work with TCP/IP Interfaces panel, 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.

Virtual Ethernet 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 system and communicate with an external LAN without installing extra physical LAN cards. If the current system 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 system.

*   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 i5/OS 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.

Related information for TCP/IP setup

Listed here are the product manuals and IBM Redbooks™ (in PDF format), Web sites, and information center topics that relate to the TCP/IP setup topic. You can view or print any of the PDFs.

IBM Redbooks

- TCP/IP Tutorial and Technical Overview (about 12 390 KB) This IBM Redbook provides information about the basics of TCP/IP.

- TCP/IP for AS/400: More Cool Things Than Ever (about 10 035 KB) This IBM Redbook includes an extensive list of common TCP/IP applications and services.

Web sites

- The Internet Engineering Task Force (IETF) (http://www.ietf.org/)
  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 (www.ipv6forum.com)
  Find news and events that communicate the latest IPv6 developments.

Other information

- TCP/IP applications, protocols, and services: This topic contains information about TCP/IP applications and services beyond the scope of configuration.
- TCP/IP troubleshooting: This topic contains information that helps you solve problems related to TCP/IP connections or traffic for both IPv4 and IPv6.
- Planning and setting up system security: This topic contains information about planning and setting up security for System i products.

Saving PDF files

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

Downloading Adobe Reader

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

Appendix. Notices

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

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

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

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

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

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

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

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

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

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

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

IBM Corporation

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

Programming Interface Information

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

Trademarks

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

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

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

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

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

Terms and conditions

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

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

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

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

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

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

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

IBM ®

Printed in USA