



iSeries

# TCP/IP Configuration and Reference

*Version 5*

SC41-5420-04







iSeries

## TCP/IP Configuration and Reference

*Version 5*

SC41-5420-04

**Note**

Before using this information and the product it supports, be sure to read the information in "Notices" on page 93.

**Fifth Edition (May 2001)**

This edition replaces SC41-5420-03. This edition applies only to reduced instruction set computer (RISC) systems.

© Copyright International Business Machines Corporation 1997, 2001. All rights reserved.

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

---

# Contents

## About TCP/IP Configuration and Reference (SC41-5420) . . . . . v

## Prerequisite and related information . . . . . vii

Operations Navigator . . . . . vii

## How to send your comments . . . . . ix

## Summary of changes . . . . . xi

## Chapter 1. Configuring TCP/IP . . . . . 1

|  |    |
|--|----|
| What you need to know before you can configure TCP/IP . . . . .      | 1  |
| Planning for TCP/IP Installation and Configuration . . . . .         | 2  |
| Gathering Information About your Network . . . . .                   | 2  |
| TCP/IP Planning Checklists . . . . .                                 | 3  |
| Line Description Parameters Checklist . . . . .                      | 3  |
| Local TCP/IP Host Information Checklist . . . . .                    | 4  |
| Installing the TCP/IP Application Programs . . . . .                 | 5  |
| Using the TCP/IP Administration Menu . . . . .                       | 6  |
| Using the Configure TCP/IP Menu . . . . .                            | 7  |
| Configuring TCP/IP using the EZ-Setup Wizard . . . . .               | 9  |
| Configuring TCP/IP using the Command Line Interface . . . . .        | 9  |
| Step 1—Configuring a Line Description . . . . .                      | 10 |
| Step 2—Configuring a TCP/IP Interface . . . . .                      | 10 |
| Step 3—Configuring TCP/IP Routes . . . . .                           | 12 |
| Step 4—Configuring TCP/IP attributes . . . . .                       | 16 |
| Step 5—Configuring TCP/IP Remote System Information (X.25) . . . . . | 16 |
| Step 6—Configuring TCP/IP Host Table Entries . . . . .               | 18 |
| Adding an Entry to the Host Table . . . . .                          | 18 |
| Work with TCP/IP Host Table Display . . . . .                        | 19 |
| AnyNet/400: APPC over TCP/IP . . . . .                               | 22 |
| Step 7—Configuring the Local Domain and Host Name . . . . .          | 22 |
| Domain Name System (DNS) Server . . . . .                            | 23 |
| Step 8—Starting TCP/IP and TCP/IP Servers . . . . .                  | 24 |
| TCP/IP Jobs . . . . .  | 25 |
| End TCP/IP (ENDTCP) . . . . .  | 26 |
| Step 9—Verifying the TCP/IP Connection . . . . .                     | 26 |
| Verifying Additional TCP/IP Connections . . . . .                    | 27 |
| Verifying TCP/IP Connections with Host Name—Example . . . . .        | 29 |
| Verifying TCP/IP Connections with Internet Address—Example . . . . . | 30 |
| Step 10—Saving Your TCP/IP Configuration . . . . .                   | 30 |

## Chapter 2. TCP/IP: Operation, Management, and Advanced Topics . . . . . 33

|  |    |
|--|----|
| Network Status . . . . .                       | 33 |
| Work with TCP/IP Network Status Menu . . . . . | 33 |
| Work with TCP/IP Interface Status . . . . .    | 34 |
| Starting TCP/IP Interfaces . . . . .           | 35 |

|  |    |
|--|----|
| Ending TCP/IP Interfaces . . . . .   | 36 |
| Route-to-Interface Binding . . . . .   | 36 |
| Display TCP/IP Route Information . . . . .   | 37 |
| Work with TCP/IP Connection Status . . . . .   | 38 |
| Ending TCP/IP Connections . . . . .  | 40 |
| Working with Configuration Status . . . . .  | 41 |
| Displaying TCP/IP Network Status Information . . . . .                                     | 42 |
| Display Multicast Groups . . . . .   | 42 |
| Displaying TCP/IP Interfaces . . . . .   | 43 |
| Displaying Associated Routes . . . . .   | 44 |
| Displaying Route Details Option . . . . .  | 45 |
| Displaying TCP/IP Route Information . . . . .  | 46 |
| Displaying TCP/IP Connections . . . . .  | 48 |
| Displaying Connection Totals . . . . .   | 49 |
| TCP/IP Host Tables . . . . .   | 50 |
| Managing TCP/IP Host Tables . . . . .  | 51 |
| Host File Formats . . . . .  | 51 |
| Host Table Information with *AIX Files . . . . .   | 51 |
| Host Table Information with *NIC Files . . . . .   | 51 |
| Host Table Information with *AS400 Files . . . . .   | 52 |
| Tips for Merging Host Tables . . . . .   | 52 |
| Merging TCP/IP Host Tables . . . . .   | 52 |
| Example: Successful Host Table Merge . . . . .   | 53 |
| Example: Partly Successful Host Table Merge . . . . .                                      | 53 |
| Managing the Host Table from a Central Site . . . . .                                      | 53 |
| Step 1—Create the Host Table on Your Central System . . . . .                              | 53 |
| Step 2—Start FTP to a Remote System . . . . .  | 53 |
| Step 3—Tell FTP to Send the Host File to the Remote System . . . . .                       | 53 |
| Step 4—Merge the File . . . . .  | 54 |
| IP Routing and Internet Control Message Protocol (ICMP) Redirecting . . . . .              | 54 |
| Dead Gateway Processing . . . . .  | 55 |
| Negative Advice from TCP or the Data Link Layer . . . . .                                  | 55 |
| How IP Responds to Negative Advice . . . . .   | 56 |
| Multihoming Function . . . . .   | 56 |
| Example: A Single Host on a Network over a Communications Line . . . . .                   | 57 |
| Example: Multiple Hosts on the Same Network over the Same Communications Line . . . . .    | 57 |
| Example: Multiple Hosts on the Same Network over Multiple Communications Lines . . . . .   | 57 |
| Example: Multiple Hosts on Different Networks over the Same Communications Line . . . . .  | 58 |
| Example: Multiple Hosts on Different Networks over Multiple Communications Lines . . . . . | 58 |
| Example: The Multihoming function . . . . .  | 59 |
| Type of Service (TOS) . . . . .  | 60 |
| TOS Example . . . . .  | 61 |
| Multiple Routes . . . . .  | 61 |
| TCP/IP Port Restriction . . . . .  | 62 |
| Configuring TCP/IP Port Restrictions . . . . .   | 63 |
| Related Tables and the Host Table . . . . .  | 65 |
| Using X.25 PVC instead of SVC . . . . .  | 67 |

|   |           |  |           |
|---|-----------|--|-----------|
| IP Multicasting . . . . .   | 68        | TCP/IP Application Exit Points. . . . .                                  | 80        |
| Multicast Application Programming Information                                     | 68        | Creating Exit Programs . . . . .   | 81        |
| Multicast Restrictions . . . . .  | 68        | Adding Your Exit Program to the Registration Facility . . . . .          | 81        |
| <b>Chapter 3. TCP/IP Performance . . . . .</b>                                    | <b>71</b> | Step 1. Select your exit point . . . . .                                 | 82        |
| *BASE Pool Size . . . . .   | 71        | Step 2: Select the Add Exit Program option. . . . .                      | 83        |
| TCP/IP Jobs . . . . .   | 71        | Step 3: Add your exit program . . . . .                                  | 83        |
| TCP/IP Protocol Support Provided by IOP. . . . .                                  | 71        | Removing Exit Programs . . . . .   | 84        |
| Merge Host Table Performance . . . . .  | 73        | Exit Point Interfaces for TCP/IP Application Exit Points . . . . .       | 85        |
| Running TCP/IP Only: Performance Considerations                                   | 73        | TCP/IP Application Request Validation Exit Point Interface . . . . .     | 85        |
| <b>Appendix A. Configuring a Physical Line for TCP/IP Communication . . . . .</b> | <b>75</b> | Required Parameter Group . . . . .                                       | 85        |
| Configuration Steps . . . . .   | 76        | Usage Notes . . . . .  | 87        |
| Creating the Line Description . . . . .   | 76        | Remote Execution Server Command Processing Selection Exit Point. . . . . | 89        |
| Line Description Name . . . . .   | 76        | Required Parameter Group . . . . .                                       | 89        |
| Source Service Access Point . . . . .   | 76        | Usage Notes . . . . .  | 90        |
| Setting the Maximum Transmission Unit . . . . .                                   | 77        | <b>Notices . . . . .</b>   | <b>93</b> |
| Determining the Maximum Size of Datagrams. . . . .                                | 77        | Programming Interface Information . . . . .                              | 94        |
| <b>Appendix B. TCP/IP Application Exit Points and Programs . . . . .</b>          | <b>79</b> | Trademarks . . . . .   | 94        |
| TCP/IP Exit Points and Exit Programs . . . . .                                    | 79        | <b>Index . . . . .</b>   | <b>97</b> |
| OS/400 Registration Facility. . . . .   | 80        |  |           |

---

## About TCP/IP Configuration and Reference (SC41-5420)

This book contains information about configuring Transmission Control Protocol/Internet Protocol (TCP/IP) and operating and managing your network. Most topics have been moved to the Information Center.

**Note:** This book contains links to various topics within the Information Center and to references outside the Information Center. The URL addresses for these links are current for V5R1.





---

## Prerequisite and related information

Use the iSeries Information Center as your starting point for looking up iSeries and AS/400e technical information. You can access the Information Center two ways:

- From the following Web site:  
<http://www.ibm.com/eserver/iseries/infocenter>
- From CD-ROMs that ship with your Operating System/400 order:  
*iSeries Information Center*, SK3T-4091-00. This package also includes the PDF versions of iSeries manuals, *iSeries Information Center: Supplemental Manuals*, SK3T-4092-00, which replaces the Softcopy Library CD-ROM.

The iSeries Information Center contains advisors and important topics such as CL commands, system application programming interfaces (APIs), logical partitions, clustering, Java™, TCP/IP, Web serving, and secured networks. It also includes links to related IBM® Redbooks and Internet links to other IBM Web sites such as the Technical Studio and the IBM home page.

With every new hardware order, you receive the following CD-ROM information:

- *iSeries 400 Installation and Service Library*, SK3T-4096-00. This CD-ROM contains PDF manuals needed for installation and system maintenance of an IBM @server iSeries 400 server.
- *iSeries 400 Setup and Operations CD-ROM*, SK3T-4098-00. This CD-ROM contains IBM iSeries Client Access Express for Windows and the EZ-Setup wizard. Client Access™ Express offers a powerful set of client and server capabilities for connecting PCs to iSeries servers. The EZ-Setup wizard automates many of the iSeries setup tasks.

---

## Operations Navigator

IBM iSeries Operations Navigator is a powerful graphical interface for managing your iSeries and AS/400e servers. Operations Navigator functionality includes system navigation, configuration, planning capabilities, and online help to guide you through your tasks. Operations Navigator makes operation and administration of the server easier and more productive and is the only user interface to the new, advanced features of the OS/400 operating system. It also includes Management Central for managing multiple servers from a central server.

For more information on Operations Navigator, see the iSeries Information Center.



---

## How to send your comments

Your feedback is important in helping to provide the most accurate and high-quality information. If you have any comments about this book or any other iSeries documentation, fill out the readers' comment form at the back of this book.

- If you prefer to send comments by mail, use the readers' comment form with the address that is printed on the back. If you are mailing a readers' comment form from a country other than the United States, you can give the form to the local IBM branch office or IBM representative for postage-paid mailing.
- If you prefer to send comments by FAX, use either of the following numbers:
  - United States, Canada, and Puerto Rico: 1-800-937-3430
  - Other countries: 1-507-253-5192
- If you prefer to send comments electronically, use one of these e-mail addresses:
  - Comments on books:  
RCHCLERK@us.ibm.com
  - Comments on the iSeries Information Center:  
RCHINFOC@us.ibm.com

Be sure to include the following:

- The name of the book or iSeries Information Center topic.
- The publication number of a book.
- The page number or topic of a book to which your comment applies.



---

## Summary of changes

This is the fifth edition of *TCP/IP Configuration and Reference*.

Most topics from the fourth edition of *TCP/IP Configuration and Reference* have been moved to the iSeries Information Center. See the iSeries Information Center for information on the following relocated topics:

- Bootstrap Protocol (BOOTP)
- Domain Name Server (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- File Transfer Protocol (FTP)
- Line Printer Daemon (LPD)
- Line Printer Requester (LPR)
- Point-to-Point Protocol (PPP)
- Post Office Protocol (POP)
- Remote Execution (REXEC)
- Route Daemon (RouteD)
- Telnet
- Trivial File Transfer Protocol (TFTP)
- Troubleshooting
- Workstation Gateway Server (WSG)

This edition of *TCP/IP Configuration and Reference* retains basic information on configuring Transmission Control Protocol/Internet Protocol (TCP/IP) and operating and managing the network.

New features in this edition include the EZ Setup Wizard as the preferred method for configuring TCP/IP on the iSeries and the addition of links to supplementary information in the iSeries Information Center and on the World Wide Web.



---

## Chapter 1. Configuring TCP/IP

This chapter explains how to configure an iSeries 400<sup>®</sup> server for Transmission Control Protocol/Internet Protocol (TCP/IP). If this is the first time that you have configured TCP/IP on an iSeries, you should read the entire chapter before performing any of the configuration tasks.

If you are unfamiliar with TCP/IP, see TCP/IP (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzahgictcp2.htm>) in the Information Center, refer to the Manuals and Redbooks topic, and select IBM redbook *TCP/IP Tutorial and Technical Overview* as a resource. For a complete formal description of TCP/IP, you can read the Request for Comments (RFC). Or, refer to any of the TCP/IP references that are listed on the RFC Editor Site (<http://www.rfc-editor.org/rfc.html>).

---

### What you need to know before you can configure TCP/IP

Before you start configuring TCP/IP, you must ensure that the *TCP/IP Connectivity Utilities for AS/400<sup>®</sup>* licensed program (LP) is installed on your system. See “Installing the TCP/IP Application Programs” on page 5 for more information.

The iSeries has many commands and menus available to help you configure TCP/IP on the server. Before you begin this task, take time to review the TCP/IP Administration (TCPADM) menu, Figure 1 on page 6, and the Configure TCP/IP (CGFTCP) menu, Figure 2 on page 8.

The initial displays and menus that are shown when you configure TCP/IP on your system may not contain any entries. The sample command line interface displays in this chapter may already contain data, which was entered for the purpose of example in previous configuration steps.

Performing configuration tasks on a single network or even a simple multiple network requires that you do some planning before configuring TCP/IP on any system in that network, including an iSeries. To help you get started with setting up TCP/IP, this chapter includes complete planning details and checklists.

Once you have designed a plan, follow the step-by-step process that is outlined for you in this chapter. Each step guides you through TCP/IP installation and configuration on your system, defines various terms, and describes how these terms relate to TCP/IP.

**Using the Operations Navigator interface:** After initial setup and configuration, you can customize your TCP/IP through Operations Navigator. Information related to Operations Navigator is located in the online help and on the Operations Navigator ([http://www.as400.ibm.com/oper\\_nav/index.htm](http://www.as400.ibm.com/oper_nav/index.htm)) Web page. See the online help in Operations Navigator for information about the following TCP/IP functions:

- Configuring TCP/IP, including basic functions such as starting and stopping TCP/IP
- Creating a new Ethernet line
- Creating a new token-ring line
- Working with TCP/IP interfaces, including configuring a TCP/IP route

- Working with TCP/IP host tables, including configuring a TCP/IP host name and domain name
- Verifying a TCP/IP connection (PING)

---

## Planning for TCP/IP Installation and Configuration

If you are in charge of configuring an iSeries server for TCP/IP communications you will, in most cases, include your server in an existing TCP/IP network. Before you are able to start configuring, you will need to collect all of the required information. Use Table 1 on page 3 and Table 2 on page 4 as checklists to record this information.

### Gathering Information About your Network

After collecting the preliminary information about your network, plan the installation and configuration of TCP/IP by using the steps that are listed below:

1. **Draw a diagram of your network:** A diagram will help you decide how you want to attach your iSeries server to the other systems in the network. Include data that relates to your network, such as:
  - Line description information
  - Internet Protocol addresses and domain names
  - The number of route entries that are required

Refer to Table 1 on page 3.

2. **Identify the names of the systems in your network:** For example, do either of the following:
  - Build a local host table.
  - Identify a Domain Name System (DNS) server for maintaining host table entries.
3. **Install the appropriate hardware and software:** You must install the appropriate hardware adapters in your server if you are going to connect to the following networks:
  - X.25 packet-switching
  - Frame relay
  - Token-ring
  - Ethernet
  - Fiber distributed data interface (FDDI)
  - Shielded twisted pair distributed data interface (SDDI)
  - Wireless local area network (LAN)
  - Synchronous or asynchronous communications line
  - Twinaxial data link support (TDLC)

You also need to make sure that the appropriate software is installed on all the systems. On the iSeries server, the OS/400 licensed program and the TCP/IP Connectivity Utilities for iSeries licensed program must be installed.

4. **Assign names and Internet addresses:** If you are attaching to an existing network, you need to know the Internet addresses and names used by the other systems.

Depending on the size of your network and its complexities, determine whether a host table or a DNS server is the preferred method for maintaining and updating host name and IP address associations. In this chapter, refer to



“Step 6—Configuring TCP/IP Host Table Entries” on page 18. For information about configuring and using a DNS server, see DNS(<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzakk/rzakkkickoff.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

5. **Obtain X.25 network addresses:** If you plan to use TCP/IP on an X.25 private or public data network, you need to know whether you will be using a switched virtual circuit (SVC) or permanent virtual circuit (PVC).

- To use an SVC, you need to know the network address of each remote system in the network with which you want to communicate.
- To use a PVC, you need to know the related logical channel identifier. You can have a network address or a permanent virtual circuit, but not both, for a remote system information entry.

If a remote system is an iSeries, you can determine its network address by using the Display Line Description (DSPLIND) command on that remote system.

6. **Familiarize yourself with the TCP/IP Administration Menu:** The TCP/IP Administration menu (Figure 1 on page 6) provides easy access to common functions associated with administering TCP/IP.

To get to this menu, enter the GO TCPADM command from the iSeries Main Menu.

7. **Familiarize yourself with the Configure TCP/IP Menu:** The Configure TCP/IP menu (Figure 2 on page 8) guides you through all the tasks for configuring your server to communicate with other systems in a TCP/IP network.

You can reach this menu in two ways:

- Select option 1 on the TCPADM menu.
- Enter the Configure TCP/IP (CFGTCP) command.

## TCP/IP Planning Checklists

The following checklists (Table 1 and Table 2 on page 4) can help you prepare for the installation and configuration of TCP/IP on your network

- Line description parameters
- Local TCP/IP host information

### Line Description Parameters Checklist

Table 1. Line Description Parameters

| Line Type                            | *ELAN | *TRLAN | *WLS | *DDI | *FR | *X25 | *ASYN | *PPP | *TDLC |
|--------------------------------------|-------|--------|------|------|-----|------|-------|------|-------|
| Resource name                        | R     | R      | R    | R    |     | R    | R     | R    |       |
| Local adapter address                | O     | O      | O    | O    |     |      |       |      |       |
| Speed                                |       | O      | O    | O    | O   | O    | O     | O    |       |
| SSAP (session services access point) | O     | O      | O    | O    | O   |      |       |      |       |
| Maximum frame size                   | O     | O      | O    | O    | O   | O    | O     | O    |       |
| Local manager mode                   |       |        |      | O    |     |      |       |      |       |
| Attached non-switched NWI name       |       |        |      |      | R   |      |       |      |       |
| Data link connection ID              |       |        |      |      | R   |      |       |      |       |

Table 1. Line Description Parameters (continued)

| Line Type                                  | *ELAN | *TRLAN | *WLS | *DDI | *FR | *X25 | *ASYNC | *PPP | *TDLC |
|--|-------|--------|------|------|-----|------|--------|------|-------|
| Network controller                         |       |        |      |      | R   |      |        |      |       |
| Connection type                            |       |        |      |      |     | R    |        |      |       |
| Logical channel identifier                 |       |        |      |      |     | R    |        |      |       |
| Logical channel type                       |       |        |      |      |     | R    |        |      |       |
| PVC (permanent virtual circuit) controller |       |        |      |      |     | R    |        |      |       |
| Local network address                      |       |        |      |      |     | R    |        |      |       |
| Physical interface type                    |       |        |      |      |     | O    |        |      |       |
| Packet size                                |       |        |      |      |     | O    |        |      |       |
| Window size                                |       |        |      |      |     | O    |        |      |       |
| Attached workstation controller            |       |        |      |      |     |      |        |      | R     |

**Note:**

R means the parameter is required

O means OS/400 suggests a default value

## Local TCP/IP Host Information Checklist

Table 2. Local TCP/IP Host Information

| Interfaces to Local TCP/IP Networks           |              |              |              |
|---|--------------|--------------|--------------|
|   | Interface #1 | Interface #2 | Interface #3 |
| Internet address                              |              |              |              |
| Line description name                         |              |              |              |
| Subnet mask                                   |              |              |              |
| Interface MTU                                 |              |              |              |
| Local host name                               |              |              |              |
| Local domain name                             |              |              |              |
| Domain name server (Internet address)         |              |              |              |
| Default route/next hop (Internet address)     |              |              |              |
| IP datagram forwarding (yes or no)            |              |              |              |
| Explicit Routes to Remote TCP/IP Networks     |              |              |              |
|   | Route #1     | Route #2     | Route #3     |
| Internet address                              |              |              |              |
| Subnet mask                                   |              |              |              |
| Next hop (Internet address)                   |              |              |              |
| MTU size                                      |              |              |              |
| Local Host Table Entries: Remote TCP/IP Hosts |              |              |              |
|   | Host Name #1 | Host Name #2 | Host Name #3 |
| Internet address                              |              |              |              |
|   |              |              |              |
|   |              |              |              |

Table 2. Local TCP/IP Host Information (continued)

| X.25 / Remote System Information |         |         |         |
|----------------------------------|---------|---------|---------|
|                                  | Host #1 | Host #2 | Host #3 |
| Internet address                 |         |         |         |
| X.25 network address             |         |         |         |
| PVC channel ID                   |         |         |         |
| Packet or window size            |         |         |         |

Once you have documented configuration information, you are ready to install the TCP/IP program on your server. The information in the section that follows will help you do that. See "Installing the TCP/IP Application Programs".

## Installing the TCP/IP Application Programs

### Important

To determine whether the TCP/IP LP is already installed, enter GO LICPGM (Go Licensed Program) on the command line and then select Option 10 to display the installed licensed programs. If the TCP/IP Connectivity Utilities LP is not installed on your system, continue by following the instructions in this section to perform the installation.

Installing TCP/IP on your iSeries server allows you to connect an iSeries to a network.

Perform the following steps to install TCP/IP on your server:

1. Insert your installation media for TCP/IP into your server. If your installation media is a CD-ROM, insert it into your optical device. If your installation media is a tape, insert it into your tape drive.
2. Type **GO LICPGM** at the command prompt 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** in the option column next to 5769TC1 *TCP/IP Connectivity Utilities for AS/400* licensed program. 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 **OPT01**, if installing from a CD drive.  
Type **TAP01**, if installing from a tape drive.
  - Objects to Install  
The Objects to Install option allows you to install both programs and language objects, only programs, or only language objects.

- Automatic IPL

The Automatic IPL option determines whether the system automatically starts when the installation process has completed successfully.

When TCP/IP 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.

To use TCP/IP, you must configure it after you have completed the installation. See "Configuring TCP/IP using the EZ-Setup Wizard" on page 9.

## Using the TCP/IP Administration Menu

The TCP/IP Administration menu (Figure 1) is a starting point for the configuration tasks. To display the menu, enter GO TCPADM from the iSeries Main Menu.

```

TCPADM                TCP/IP Administration                System:  RC
Select one of the following:

    1. Configure TCP/IP
    2. Configure TCP/IP applications
    3. Start TCP/IP
    4. End TCP/IP
    5. Start TCP/IP servers
    6. End TCP/IP servers
    7. Work with TCP/IP network status
    8. Verify TCP/IP connection
    9. Start TCP/IP FTP session
   10. Start TCP/IP TELNET session
   11. Send TCP/IP spooled file

    20. Work with TCP/IP jobs in QSYSWRK subsystem

Selection or command
===>

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel

```

Figure 1. TCP/IP Administration Menu

Following are descriptions of the menu options.

- **Option 1. Configure TCP/IP:** Displays the Configure TCP/IP menu. Use the options on this menu to configure your local server to communicate with other systems in a TCP/IP network.
- **Option 2. Configure TCP/IP applications:** Displays the Configure TCP/IP Applications menu. Use the options on this menu to configure the TCP/IP licensed program (5769-TC1) applications installed on your system.
- **Option 3. Start TCP/IP:** Select this option to issue the Start TCP/IP (STRTCP) command. This command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the TCP/IP server jobs.
- **Option 4. End TCP/IP:** Select this option to issue the End TCP/IP (ENDTCP) command. This command is used to end all TCP/IP processing on this system.

- **Option 5. Start TCP/IP servers:** Select this option to issue the Start TCP/IP Server (STRTCPSVR) command. This command is used to start the TCP/IP application servers that are shipped with OS/400® or the TCP/IP licensed program (5769-TC1). This command starts the TCP/IP application server jobs in the QSYSWRK subsystem.
- **Option 6. End TCP/IP servers:** Select this option to issue the End TCP/IP Server (ENDTCPSVR) command. This command is used to end the TCP/IP application servers that are shipped with OS/400 or the TCP/IP licensed program (5769-TC1). This command ends the TCP/IP application server jobs in the QSYSWRK subsystem.
- **Option 7. Work with TCP/IP network status:** Select this option to issue the Work with TCP/IP Network Status (WRKTCPSTS) command. This command is used to view and manage the status information of your TCP/IP and IP over Systems Network Architecture (SNA) interfaces, routes, and connections. This command is the iSeries version of the TCP/IP NETSTAT (Network Status) command. NETSTAT is also shipped as an iSeries command.
- **Option 8. Verify TCP/IP connection:** Select this option to issue the Verify TCP/IP Connection (VFYTCPCNN) command. This command tests the TCP/IP connection between your system and a remote system. The VFYTCPCNN command is the iSeries version of the TCP/IP PING (Packet InterNet Groper) command. PING is also shipped as an iSeries command.
- **Option 9. Start TCP/IP FTP session:** Select this option to issue the Start TCP/IP FTP (STRTCPFTP) command. This command is used to start a file transfer using TCP/IP. This command is the iSeries version of the TCP/IP FTP (File Transfer Protocol) command. FTP is also shipped as an iSeries command.
- **Option 10. Start TCP/IP TELNET session:** Select this option to issue the Start TCP/IP TELNET (STRTCPTELN) command. This command is used to start a TELNET client session with a remote system. This command is the iSeries version of the TCP/IP TELNET command. TELNET is also shipped as an iSeries command.
- **Option 11. Send TCP/IP spooled file:** Select this option to issue the Send TCP/IP Spooled File (SNDTCPSPLF) command. This command sends a spooled file to be printed on a remote system. The remote system must be running TCP/IP. The SNDTCPSPLF command is the iSeries version of the TCP/IP LPR (line printer requester) command. LPR is also shipped as an iSeries command.
- **Option 20. Work with TCP/IP jobs in QSYSWRK subsystem:** Select this option to work with the status and performance information for the active TCP/IP jobs in the QSYSWRK subsystem. This option issues the Work with Active Jobs (WRKACTJOB) command with these parameters:  
WRKACTJOB SBS(QSYSWRK) JOB(QT\*)

---

## Using the Configure TCP/IP Menu

The Configure TCP/IP menu is shown here (Figure 2 on page 8) so that you are familiar with all of the options available during configuration of the TCP/IP network. To get to this menu, select option 1 on the TCPADM menu or enter the Configure TCP/IP (CFGTCP) command.

```
CFGTCP                      Configure TCP/IP                      System:  SYSNAM890

Select one of the following:

    1. Work with TCP/IP interfaces
    2. Work with TCP/IP routes
    3. Change TCP/IP attributes
    4. Work with TCP/IP port restrictions
    5. Work with TCP/IP remote system information

    10. Work with TCP/IP host table entries
    11. Merge TCP/IP host table
    12. Change TCP/IP domain information

    20. Configure TCP/IP applications
    21. Configure related tables
    22. Configure point-to-point TCP/IP

Selection or command
===>

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
```

Figure 2. Configure TCP/IP Menu

Following are descriptions of the Configure TCP/IP menu options.

- **Option 1. Work with TCP/IP interfaces:** Select this option to add TCP/IP interface information to the list of current interfaces or to display, change, print, or remove TCP/IP interface information that you have already added. Select this option to start or end a TCP/IP interface.
- **Option 2. Work with TCP/IP routes:** Select this option to add route information or to display, change, print, or remove route information that you have already added.
- **Option 3. Change TCP/IP attributes:** Select this option to run the Change TCP/IP Attributes (CHGTCPA) command.  
With this option you can change User Datagram Protocol (UDP) checksum processing, IP datagram forwarding, IP time-to-live values, and other attributes that relate to the TCP/IP protocol stack.
- **Option 4. Work with TCP/IP port restrictions:** Select this option to add port restrictions or to display, remove, or print port restrictions that you have already added.
- **Option 5. Work with TCP/IP remote system information:** Select this option to add or remove X.25 data network addresses or to print the list.
- **Option 10. Work with TCP/IP host table entries:** Select this option to add host IP addresses and their associated host names to the host table or to display, change, print, rename, or remove items that you have already added.
- **Option 11. Merge TCP/IP host table:** Select this option to merge or replace a local host table by using the Merge TCP/IP Host Table (MRGTCPHT) command.
- **Option 12. Change TCP/IP domain information:** Select this option to change TCP/IP domain information.

**Note:** Prior to Version 4 Release 2, the Configure TCP/IP menu contained both an option 12 and an option 13. In Version 4 Release 2, the functions of options 12 and 13 were combined, and option 13 (Change Remote name

server) was removed from the menu. Option 12, formerly Change local domain and host names, was renamed to Change TCP/IP domain information.

- **Option 20. Configure TCP/IP applications:** Select this option to configure the TCP/IP applications that are installed on your system. The list of applications varies depending on whether the TCP/IP licensed program is installed on your system. If the TCP/IP licensed program is not installed on your system, you can configure *only* the following server applications:
  - Simple Network Management Protocol (SNMP)
  - Bootstrap Protocol (BOOTP) server
  - Trivial File Transfer Protocol (TFTP) server
  - Route Daemon (RouteD)

If the TCP/IP licensed program is installed on your system, you can configure the following server applications:

- Simple Mail Transfer Protocol (SMTP)
  - File Transfer Protocol (FTP), TELNET
  - Post Office Protocol (POP) Version 3 mail server
  - Line Printer Daemon (LPD)
  - Remote Execution (REXEC) server
  - Workstation gateway applications
  - Simple Network Management Protocol (SNMP)
- **Option 21. Configure related tables:** Select this option to configure the tables related to TCP/IP. These tables are:
    - **Protocol table**  
Contains a list of protocols used in the Internet.
    - **Services table**  
Contains a list of services and the specific port and protocol a service uses.
    - **Network table**  
Contains a list of networks and the corresponding IP addresses for that network.
  - **Option 22. Configure point-to-point TCP/IP:** Select this option to define, change, or display your TCP/IP point-to-point (SLIP) configuration.

---

## Configuring TCP/IP using the EZ-Setup Wizard

If you are setting up a new iSeries, use the EZ-Setup Wizard to establish a connection and to configure TCP/IP for the first time. The CD-ROM containing the EZ-Setup Wizard is packaged with your new iSeries. The wizard steps you through a process that will get your iSeries up and running.

**Note:** If you are unable to use the EZ-Setup Wizard, you may use the command line interface to configure TCP/IP. See the next section for these instructions.

---

## Configuring TCP/IP using the Command Line Interface

The following steps using the command line interface will guide you through configuring TCP/IP on your iSeries server:

1. Configuring line descriptions
2. Configuring TCP/IP interfaces



3. Configuring TCP/IP routes
4. Configuring TCP/IP attributes
5. Configuring remote system information (X.25)
6. Configuring host table entries
7. Configuring local domain and host name
8. Starting TCP/IP
9. Verifying TCP/IP connection
10. Saving the TCP/IP configuration

**Important Note:**

To perform the configuration steps discussed throughout this chapter, you need the special authority of \*IOSYSCFG defined in your user profile.

## Step 1—Configuring a Line Description

iSeries TCP/IP supports various local area network (LAN) and wide area network (WAN) connection types: Ethernet, token-ring, SDDI and FDDI, wireless LAN, X.25 SVC, and permanent virtual circuit (PVC), Async (for SLIP), Point-to-Point (PPP) and frame relay. Refer to Appendix A. Configuring a Physical Line for TCP/IP Communication for information about how to configure an Ethernet line for TCP/IP communications.

These are the important parameters for configuring a line description:

- Line description name
- Resource name
- Local adapter address
- Ethernet standard
- Source service access point (SSAP) list.

The SSAP X'AA' required for an IEEE 802.3 Ethernet is automatically allocated if you use the \*SYSGEN special value.

When TCP/IP starts an interface, the line, controller, and device descriptions are varied on automatically. If the controller and device descriptions for a line do not exist, TCP/IP creates them automatically when it attempts to start an interface using that line. This happens at TCP/IP startup time if the TCP/IP interface that is associated with the newly configured line is set to AUTOSTART \*YES.

## Step 2—Configuring a TCP/IP Interface

In an iSeries server, each line that connects to a TCP/IP network must be assigned to at least one Internet address. You do this by configuring, or *adding* a TCP/IP interface. The additional interfaces are logical interfaces, not physical ones. These logical interfaces are associated with a line description.

An **interface** identifies a direct connection to a network using TCP/IP and a physical medium (communications line). You must consider the following when defining an interface:

**Internet address**

A 32-bit address assigned to hosts using TCP/IP. It is associated with the line description.



**Subnet mask**

Defines which part of an Internet address forms the subnet (subnetwork) field of an Internet address. An example of a single-network subnet mask is: 255.255.255.128.

**Line description**

Contains information describing a communications line that is attached to the iSeries server, as defined previously in “Step 1—Configuring a Line Description” on page 10.

To find the names of the currently defined line descriptions, use the Work with Line Descriptions (WRKLIND) command.

**Associated local interface**

Allows the network to which this interface is attached appear to be part of the same network that the associated local interface is attached to. This is referred to as *transparent subnetting*.

Transparent subnetting allows TCP/IP traffic to flow between the two physical networks without defining additional routing. This is only valid for broadcast-capable networks. This also requires the Internet address for Add TCP/IP Interface (ADDTCPIFC) to be configured in the same network as the associated local interface. An additional requirement is for the subnet mask that is defined for the associated local interface.

**Automatic start**

Refers to whether the TCP/IP interface is started automatically whenever TCP/IP is started. The default setting is \*YES. If you choose \*NO, you must start the interface yourself by using the STRTCPIFC command or by selecting option 9 (Start) on the Work with TCP/IP Interfaces display, as shown in Figure 4 on page 12.

To add a TCP/IP interface, do the following:

1. Enter GO TCPADM to get the TCP/IP Administration menu.
2. Select option 1 to get to the Configure TCP/IP menu.
3. Select option 1 on the Configure TCP/IP menu.

The Work with TCP/IP Interfaces display is shown in Figure 4 on page 12.

4. Type option 1 (Add) at the input-capable top list entry on this display to go to the Add TCP/IP Interfaces (ADDTCPIFC) display, as shown in Figure 3 on page 12.

(You can go directly to this display by typing ADDTCPIFC command on any command line and pressing F4.)

iSeries TCP/IP supports multihoming, which allows you to specify multiple interfaces for each line description. See “Multihoming Function” on page 56 for further information.

```

Add TCP/IP Interface (ADDTCPIFC)

Type choices, press Enter.

Internet address . . . . .
Line description . . . . . Name, *LOOPBACK, *VIRTUALIP
Subnet mask . . . . .
Associated local interface . . . *NONE
Type of service . . . . . *NORMAL *MINDELAY, *MAXTHRPUT...
Maximum transmission unit . . . *LIND 576-16388, *LIND
Autostart . . . . . *YES *YES, *NO
PVC logical channel identifier 001-FFF
+ for more values
X.25 idle circuit timeout . . . 60 1-600
X.25 maximum virtual circuits . 64 0-64
X.25 DDN interface . . . . . *NO *YES, *NO
TRLAN bit sequencing . . . . . *MSB *MSB, *LSB

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More key

```

Figure 3. Add TCP/IP Interfaces Display

When you are finished adding entries, the Work with TCP/IP Interfaces display looks like Figure 4.

```

Work with TCP/IP Interfaces System: SYSNAM890

Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display 9=Start 10=End

Opt Internet Subnet Line Line
Address Mask Description Type
- 9.4.73.129 255.255.255.128 ETHLINE *ELAN

```

Figure 4. Work with TCP/IP Interfaces Display

**Note:** Any change to the TCP/IP interfaces configuration, except for the automatic start parameter, takes effect immediately.

### Step 3—Configuring TCP/IP Routes

**Do you need to add routes at all?**

If you have several individual networks to which the server is not directly attached, you must add routing entries to allow the server to reach these remote networks.

If your server is attached to a single network and if there are no IP routers in your network, you do not need to add routes.

To reach remote networks, at least one routing entry is required. If no routing entries are manually added, your server cannot reach systems that are not on the

same network that the server is attached to. You must also add routing entries to allow TCP/IP clients that are attempting to reach your server from a remote network to function correctly.

For example, suppose that someone using a PC is using the TELNET application to start a remote terminal session on your server. The application on the PC must know the route or path to reach the server. Your server must also be able to determine the route back to the PC. If the PC and your server are not on the same network, a routing entry must exist on the PC and on your server.

**Note:** You should plan to have the routing table defined so that there is always an entry for at least one default route (\*DFTRROUTE). 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. The only exception to this is if you intend to dial out over a SLIP link to an Internet Service Provider or another remote host.

Before adding routing entries, familiarize yourself with the following terms:

#### **Route destination**

The network ID portion of an Internet address. The network ID portion is composed of the first byte, the first two bytes, or the first three bytes of the Internet address (depending on the network class). The remaining bytes define the host ID portion of the Internet address.

If subnetting is used, route destination includes the subnet part as well. In other words, **the route destination equals the address of a TCP/IP network to be reached.**

#### **Subnet mask**

A bit mask that defines which part of an Internet address forms the network and the subnetwork.

The technique known as **subnet addressing, subnet routing, or subnetting** allows a single network ID to be used on multiple physical networks. This technique lets you define separate routes to different sets of Internet addresses within a specific network.

#### **Next hop**

The Internet address of the first system in the route between your system and the destination network. The next hop value is always an Internet address. Next hops need to be hosts on a directly connected TCP/IP network defined by the TCP/IP interfaces.

#### **Maximum Transmission Unit (MTU) size**

The maximum size (in bytes) of IP datagrams sent on a route. If you specify \*IFC, the size is calculated for you based on values found in the server line description. The maximum size specified for a particular route must not be larger than the smallest MTU supported by any router or bridge in that route. If you specify a larger size, some datagrams may be lost.

In addition, the MTU specified for a particular route should not be larger than the smallest MTU supported by any system used as an IP router for that route. If you specify a larger size, performance may degrade as systems attempt to divide the IP datagrams into smaller fragments.

For additional information about setting the MTU, see Appendix A. Configuring a Physical Line for TCP/IP Communication.

### Preferred binding interface

The preferred binding interface allows administrators to choose which of the TCP/IP interfaces that they prefer the route to be bound to or on. This provides the administrator with more flexibility to route traffic over a specific interface. The interface is preferred because the route is bound to the indicated interface if the interface is active. If the indicated interface is not active, then a best-match-first algorithm is used in determining which interface the route is bound.

In Figure 5, a preferred binding interface of \*NONE has been defined. By using this definition, the user allows the TCP/IP protocol stack to choose an interface to bind this route to, using a best-match-first algorithm.

### Adding TCP/IP routes

You must define routes for any TCP/IP network, including subnetworks, with which you want to communicate. You do not need to define routes for the TCP/IP network that your server is directly attached to when you are using an iSeries adapter.

Manual configuration of the routes that tell TCP/IP how to reach the local networks is not required. iSeries TCP/IP generates these routes automatically from the configuration information for the interfaces every time TCP/IP is started. In other words, the direct route to the network, which has an interface attached, is automatically created when you add the interface.

To display all routing entries, including direct routes, use the Network Status (NETSTAT) command after starting TCP/IP.

To add a route, type option 2 on the Configure TCP/IP menu. The Work with TCP/IP Routes display (Figure 5) is shown.

| Work with TCP/IP Routes           |                   |             |            | System: SYSNAM890   |
|-----------------------------------|-------------------|-------------|------------|---------------------|
| Type options, press Enter.        |                   |             |            |                     |
| 1=Add 2=Change 4=Remove 5=Display |                   |             |            |                     |
| Opt                               | Route Destination | Subnet Mask | Next Hop   | Preferred Interface |
| -                                 | *DFTRROUTE        | *NONE       | 9.4.73.193 | *NONE               |

Figure 5. Work with TCP/IP Routes Display

Type option 1 (Add) at the input-capable top list entry on that display to go to the Add TCP/IP Route (ADDTCP RTE) display, as shown in Figure 6 on page 15.

(To go directly to this display, type the ADDTCP RTE command on any command line and press F4.)

```

Add TCP/IP Route (ADDTCPRTE)

Type choices, press Enter.

Route destination . . . . . > '9.4.6.128'
Subnet mask . . . . . > '255.255.255.128'
Type of service . . . . . *NORMAL *MINDELAY, *MAXTHRPUT...
Next hop . . . . . > '9.4.73.193'
Preferred binding interface . . *NONE
Maximum transmission unit . . . 576 576-16388, *IFC
Route metric . . . . . 1 1-16
Route redistribution . . . . . *NO *NO, *YES
Duplicate route priority . . . . 5 1-10

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

```

Figure 6. Add TCP/IP Routes Display

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

```

Work with TCP/IP Routes

Type options, press Enter.
1=Add 2=Change 4=Remove 5=Display

Opt  Route      Subnet      Next      Preferred
Destination  Mask        Hop        Interface
-
-  *DFTRoute  *NONE      9.4.73.193 *NONE
-  9.4.6.128  255.255.255.128  9.4.73.193
-

```

Figure 7. Work with TCP/IP Routes Display

### Multiple Default Routes

Default routes are used to route data that is being addressed to a remote destination and that does not have a specific route defined. Default routes are based on the availability of the next hop router and the type of service (TOS). If no specific TOS is requested, the first available default route with TOS of \*NORMAL is used.

If a default route is not defined, only the networks explicitly defined by any non-default routes appear as though TCP/IP can reach them, and datagrams bound for any undefined networks are not sent.

**Note:** A default route cannot have a subnetwork; therefore, you must leave the subnet mask at the default value of \*NONE.

Consult "Multiple Routes" on page 61 for further information about multiple default routes and the type of service (TOS) parameter.

## Step 4—Configuring TCP/IP attributes

To configure the TCP/IP attributes, type option 3 on the Configure TCP/IP menu. The Change TCP/IP Attributes (CHGTCPA) display is shown (Figure 8).

```
Change TCP/IP Attributes (CHGTCPA)

Type choices, press Enter.

TCP keep alive . . . . . 120          1-40320, *SAME, *DFT
TCP urgent pointer . . . . . *BSD      *SAME, *BSD, *RFC
TCP receive buffer size . . . . . 8192  512-8388608, *SAME, *DFT
TCP send buffer size . . . . . 8192    512-8388608, *SAME, *DFT
UDP checksum . . . . . *YES           *SAME, *YES, *NO
IP datagram forwarding . . . . . *YES   *SAME, *YES, *NO
IP source routing . . . . . *YES       *SAME, *YES, *NO
IP reassembly time-out . . . . . 10     5-120, *SAME, *DFT
IP time to live . . . . . 64           1-255, *SAME, *DFT
ARP cache timeout . . . . . 5          1-1440, *SAME, *DFT
Log protocol errors . . . . . *YES     *SAME, *YES, *NO
```

Figure 8. Change TCP/IP Attributes Display

For information about the various parameters for this command, see the online help. In this step only the IP Datagram Forwarding (IPDTGFWD) parameter is discussed.

### IP Datagram Forwarding

Specifies whether your system should forward datagrams destined for other networks. The default value is \*NO.

## Step 5—Configuring TCP/IP Remote System Information (X.25)

**Note:** If you are not using X.25, then proceed to “Step 6—Configuring TCP/IP Host Table Entries” on page 18.

If you use an X.25 connection to reach TCP/IP hosts with a public or private packet switched data network (PSDN), you need to add remote system information for each remote TCP/IP host. You must define the X.25 network address of each system if you use a switched virtual circuit (SVC). If a permanent virtual circuit (PVC) is set up by the network connecting your system with your remote TCP/IP partner, you need to know the local logical channel identifier of this PVC.

### Adding Remote System Information (X.25)

To add an X.25 remote system address, type option 5 on the Configure TCP/IP menu. The Work with the TCP/IP Remote System Information display appears, as shown in Figure 9 on page 17.

```

Work with TCP/IP Remote System Information
System: SYSNAM890
Type options, press Enter.
  1=Add  4=Remove  5=Display

Opt      Internet      Network      PVC      Reverse
  -      Address      Address      Address      Charges
-----
(No remote system information)

```

Figure 9. Work with Remote System (X.25) Information

Type option 1 (Add) at the input-capable top list entry to go to the Add TCP/IP Remote System (ADDTCPRSI) display, as shown in Figure 10.

```

Add TCP/IP Remote System (ADDTCPRSI)
Type choices, press Enter.
Internet address . . . . . > '9.4.73.66'
Network address . . . . . > 40030002
PVC logical channel identifier . . . . . 001-FFF
X.25 reverse charge . . . . . *NONE *NONE, *REQUEST, *ACCEPT

Additional Parameters

Default packet size:
Transmit packet size . . . . . *LIND *LIND, 64, 128, 256, 512...
Receive packet size . . . . . *LIND *LIND, *TRANSMIT, 64, 128...

Default window size:
Transmit window size . . . . . *LIND 1-15, *LIND
Receive window size . . . . . *LIND 1-15, *LIND, *TRANSMIT

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

```

Figure 10. Add Remote System (X.25) Information

The network controller used by iSeries TCP/IP does not allow you to specify X.25 user facilities. However, some of the values usually configured on a controller, using the ADDTCPRSI command, allow you to configure each X.25 remote system. These values include reverse charging, packet sizes, and window sizes.

Use the following CL command to enter the information as shown in the display above:

```

ADDTCPRSI INTNETADR('9.4.73.66')
NETADR(40030002)

```

**Notes:**

1. Specifying remote system information for an X.25 DDN interface causes that information to be used instead of the DDN conversion algorithm. The DDN conversion algorithm is used only for a connection with DDN specified as \*YES when you try to connect to a host that is not defined in the remote system

information. If DDN is specified as \*YES on the X.25 connection, you should not specify remote system information for that interface or its associated DDN network systems.

2. A routing error occurs when both of the following are true:
  - The remote system information associated with the Internet address is an extended data terminal equipment (DTE) address.
  - The configured X.25 interface's line does not support X.25 extended addressing.

**Note:** Any changes that you make to the remote system information take effect immediately.

## Step 6—Configuring TCP/IP Host Table Entries

Each computer system in your network is called a **host**. The host table allows you to associate a host name to an Internet address. This step gives instruction for configuring a host table and host table entries. However, you should determine early in the configuration planning if a host table or a Domain Name System (DNS) server is the best option for you in managing host name and IP address translations.

Whenever possible, a DNS server should be used as a replacement for, or in addition to, the local host table. The DNS server is a single source for host names, which is one reason that it is often preferred over host tables, especially for larger networks.

The local host table on your server contains a list of the Internet addresses and related host names for your network. Host tables map Internet addresses to TCP/IP host names. Host tables allow users to use an easily remembered name for a system in a network without having to remember the Internet address.

To configure the mapping of host names to Internet addresses, you can use three different options on the Configure TCP/IP menu. You can use only one or a combination of all three to obtain the host name processing you need for your network. The three options on the Configure TCP/IP menu related to Internet address mappings are:

1. Option 10 (Work with TCP/IP host table entries) to create your own host table. The Work with Host Table Entries display is shown in Figure 11 on page 19.
2. Option 11 (Merge TCP/IP host table) to merge or convert a host table sent from another system.

For more information about merging and converting host tables, see "Merging TCP/IP Host Tables" on page 52.

3. Option 12 (Change TCP/IP domain information) to call the following new command, CHGTCPDMN.

**Note:** You can start TCP/IP client functions, such as FTP, by specifying the Internet address directly without using the host table.

For more information about managing host tables, including host file formats, and merging host tables, see "Managing TCP/IP Host Tables" on page 51.

### Adding an Entry to the Host Table

The Add TCP/IP Host Table Entry display provides fields for an Internet address, associated host name, and an optional text description.



To add an entry to your local host table, type option 10 on the Configure TCP/IP menu. The Work with TCP/IP Host Table Entries display is shown in Figure 11.

```

Work with TCP/IP Host Table Entries
System: SYSNAM890
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  7=Rename

Opt  Internet      Host
     Address      Name
-----
  -   127.0.0.1    LOOPBACK
  -                       LOCALHOST

```

Figure 11. Work with TCP/IP Host Table Entries Display

**Note:** Just as iSeries TCP/IP automatically creates a LOOPBACK interface, it also automatically adds an entry to your local host table to associate the IP address 127.0.0.1 with the host names LOOPBACK and LOCALHOST. Type option 1 (Add) at the input-capable top list entry to show the Add TCP/IP Host Table Entry display.

### Work with TCP/IP Host Table Display

Figure 12 and Figure 13 on page 20 show how the host table looks after you enter all hosts explicitly known.

```

Work with TCP/IP Host Table Entries
System: SYSNAM890
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  7=Rename

Opt  Internet      Host
     Address      Name
-----
  -   9.4.6.129    ROUTER2
  -   9.4.6.134    HPUX
  -   9.4.6.138    SPARKY
  -   9.4.6.252    MVAX
  -   9.4.73.65    XSYSNAM890
  -   9.4.73.66    XSYSNAM456
  -   9.4.73.129   ESYSNAM890
  -   9.4.73.130   ESYSNAMRS
  -   9.4.73.193   ROUTER1
  -   9.4.73.198   SYSNAMRS
  -   9.4.73.206   ITALY
  -   9.4.73.207   HOLLAND
  -   9.4.73.208   ENGLAND

More...

```

Figure 12. Work with Host Table Entries, Display 1 of 2

```

Work with TCP/IP Host Table Entries
System:  SYSNAM890
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  7=Rename

  Internet      Host
  Opt  Address   Name
  ---  -
  -    9.4.73.211  BERN
  -    9.4.73.212  SYSNAM890
  -    9.4.73.214  MACIAN
  -    9.4.191.76  DNS
  -    127.0.0.1   LOOPBACK
  -                   LOCALHOST

```

Figure 13. Work with Host Table Entries, Display 2 of 2

The iSeries TCP/IP host table is shipped with the LOOPBACK entry. The LOOPBACK entry has an Internet address of 127.0.0.1 and two host names: LOOPBACK and LOCALHOST.

The 127.0.0.1 Internet address can be changed (CHGTCPHTE) and a different one can be added (ADDTCPHTE). The local table command processing programs ensure that any LOOPBACK host name added or changed in the host table is in the range of 127.0.0.1 to 127.255.255.254. Multiple loopback host table entries are allowed in the server host table.

You may alter the LOOPBACK host name or add additional host names using the (CHGTCPHTE) command.

If the LOOPBACK or LOCALHOST name is changed or removed from the host table, the name is not valid, unless the domain name server has a LOOPBACK entry that specifies this value as a host name.

You can define up to four names for each Internet address. If the TCP/IP host is in your local domain, then it is not necessary to qualify the host with the domain name. As long as a TCP/IP host is in your local domain, you need only to enter the host name with the host table entry.

However, if you would like to add TCP/IP hosts that are outside of your local domain, you need to add these TCP/IP hosts as fully qualified. The fully qualified host name of SYSNAMEND.ENDICOTT.IBM.COM shows this as an example in Figure 14 on page 21.

```

Work with TCP/IP Host Table Entries
System:  SYSNAM890
Type options, press Enter.
1=Add  2=Change  4=Remove  5=Display  7=Rename

  Internet      Host
Opt  Address    Name
-
-  9.4.73.211   BERN
-  9.4.73.212   SYSNAM890
-  9.4.73.214   MACIAN
-  9.4.191.76   DNS
-  9.125.87.127 SYSNAMEND.ENDICOTT.IBM.COM
-  127.0.0.1    LOOPBACK
-                LOCALHOST

```

Figure 14. Example of a Fully Qualified Host Table Entry

Additional host names are useful as alternative nicknames. See the examples in Figure 15.

Host names need not be unique. When searching the host table with a duplicate host name, the result is random. However, IP addresses have to be unique. The uniqueness of the IP address is enforced at the time you try to add a new entry to the host table.

**Note:** An IP address cannot be used as a host name.

```

Work with TCP/IP Host Table Entries
System:  SYSNAM890
Type options, press Enter.
1=Add  2=Change  4=Remove  5=Display  7=Rename

  Internet      Host
Opt  Address    Name
-
-  9.4.73.211   BERN
-  9.4.73.212   SYSNAM890
-                M03
-                F25
-                MYSYSTEM
-  9.4.73.214   MACIAN
-  9.4.191.76   DNS
-  9.4.73.198   SYSNAMRS

```

Figure 15. Multiple Host Names

To remove one of the additional host names, select option 2 to change the selected host table entry. Type \*BLANK over the host name to remove it.

**Note:** The fully qualified host name is used when sending mail between two TCP/IP hosts.

Notice in the example that the name of server SYSNAM890 is in the host table too. There are several reasons to put your host name in the host table:

- You may want to use your host name when using FTP, TELNET, or PING to test your own system's configuration.

- Simple Mail Transfer Protocol (SMTP) requires your host name to be in the host table or on a domain name server.
- You may want to use your host table on other systems in the network. Your host name must be in the host table on those systems so they can refer to your system by name.
- Applications written to use host table lookup routines may require this information.

When you are finished working with the host table, press F3 (Exit) or F12 (Cancel).

### **AnyNet/400: APPC over TCP/IP**

Advanced program-to-program communication (APPC) over TCP/IP support allows Common Programming Interface (CPI) Communications or Intersystem Communications Function (ICF) applications to run over TCP/IP with no changes. To use the APPC over TCP/IP support, the logical unit (LU) name or the remote location that your application uses must be mapped to an Internet address. For APPC over TCP/IP support, the host table is configured to map Internet addresses to LU names. To do this, you can update the TCP/IP host table using the configuration menus. The format for the host name is:

```
LUNAME.NETID.SNA.IBM.COM
```

## **Step 7—Configuring the Local Domain and Host Name**

Within TCP/IP, the primary name associated with your system (your system can have more than one name) is called your **local domain and host name**. The combination of the local domain and host name forms a fully-qualified host name. The fully qualified host name is the name by which your system is known and identified in the TCP/IP domain. The local domain name is also used by sockets to help in host name resolution at the Domain Name System (DNS) server. The Post Office Protocol (POP) and Simple Mail Transfer Protocol (SMTP) mail servers require that the local domain and host name be configured. It is used, but not required, by line printer requester (LPR), File Transfer Protocol (FTP), and Simple Network Management Protocol (SNMP).

A domain name consists of labels that are separated by periods, for example, SYSNAM890.ROCHESTER.IBM.COM. For hosts, the first label in a domain name is the name of a host that belongs in the domain identified by the other labels. In this example, host SYSNAM890 belongs to the domain ROCHESTER.IBM.COM. SYSNAM890.ROCHESTER.IBM.COM is known as the host's fully qualified domain name.

To define a local domain name and a host name, use option 12 (Change TCP/IP domain information) from the Configure TCP/IP menu (Figure 2 on page 8).

You may need to configure the local domain name if you use a DNS server that requires a fully qualified host name to resolve an Internet address. For more information on how to do that, see DNS

(<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzakk/rzakkkickoff.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

The iSeries TCP/IP applications concatenate the local domain name to the host name if a period is not used at the end of the domain name. For an example, see Concatenating the Domain Name to the Host Name

(<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzaku/rzakuconcat.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

To change the local domain name, type option 12 on the Configure TCP/IP menu. The Change TCP/IP domain information display is shown in Figure 16.

```
Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name . . . . . SYSNAM890

Domain name . . . . . SYSNAM123.IBM.COM

Host name search priority . . . *LOCAL      *REMOTE, *LOCAL, *SAME
Domain name server:
  Internet address . . . . . '9.4.73.129'
```

Figure 16. Change TCP/IP Domain Information (CHGTCPDMN)

**Notes:**

1. Changes that you make using the Change TCP/IP domain information (CHGTCPDMN) command take effect immediately.
2. The local domain name is used by many applications including PING. PING appends the local domain to a host name if a domain is not specified or if a period (.) does not appear at the end of the specified host name.

**Domain Name System (DNS) Server**

The conversion from host name to Internet address can be performed by using the host table on the local system or by defining a Domain Name System server, or DNS server.

In large networks with large host tables, it is more convenient to have DNS servers than to have a complete copy of the host table on every host in the network.

A DNS server maintains the host table for an entire TCP/IP domain. This prevents each single host from having to maintain its own local host table.

You can configure your server to use both a DNS server and your local host table, but they are not mutually exclusive. You can also specify whether the domain name server or your local host table is searched first.

For more information about how the Domain Name System works and how to configure a DNS server, see DNS

(<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzakk/rzakkkickoff.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

## Step 8—Starting TCP/IP and TCP/IP Servers

Before any TCP/IP services are available on the iSeries system, TCP/IP processing must be initialized and activated. To start TCP/IP, you have two options:

1. Select option 3 from the TCP/IP Administration menu (GO TCPADM),
2. Enter the Start TCP/IP (STRTCP) command.

The STRTCP command initializes and activates TCP/IP processing, starts the TCP/IP interfaces, and starts the TCP/IP server jobs. Only TCP/IP interfaces with AUTOSTART \*YES are started at STRTCP time. Allow a few moments for TCP/IP to start, and then check to see if the QTCPIP job has started.

Option 20 of the TCP/IP Administration menu allows you to display the jobs related with TCP/IP. You can also use the following command:

```
WRKACTJOB SBS(QSYSWRK) JOB(QT*)
```

The job QTCPIP should be displayed.

Messages indicating that TCP/IP has been started are sent to the QTCP and QSYSOPR message queues. To check for the successful start of TCP/IP, enter either of these commands:

```
DSPMSG QSYSOPR  
DSPMSG QTCP
```

Figure 17 contains a sample of the messages that are issued.

```
STRTCP issued by job 007138/DJONES/DSP02.  
QTCPIP job started.  
127.0.0.1 interface started.  
QTCPIP job starting 9.5.5.162 interface.  
127.0.0.2 interface started.  
SNMP Server starting.  
TELNET Server starting  
FTP Server starting  
SMTP Server starting  
POP Server starting  
LPD Server starting  
9.5.5.162 interface started.  
STRTCP completed successfully.
```

*Figure 17. Sample Messages from STRTCP with All Applications Autostarted*

If the QTCPIP job does not start, look for spooled job logs. Generally, the user for these job logs is QTCP. Use the Work with Spooled Files (WRKSPLF) command and specify QTCP for the user (WRKSPLF QTCP) to find the logs.

**Application Servers:** The TCP/IP application server jobs run under subsystem QSYSWRK. Several types of TCP/IP server jobs run in the QSYSWRK subsystem. They are the server jobs for TELNET, POP, FTP, SMTP, LPD, BOOTP, TFTP, RouteD, REXEC, and SNMP.

The STRTCP command starts the server jobs for an application if the automatic start attribute for that server is equal to \*YES. To change the autostart attribute for an application, do either of the following:

- Select option 2 from the TCP/IP Administration menu
- Option 20 from the TCP/IP Configuration menu

Using the Start TCP/IP Server (STRTCPSVR) command starts the servers individually or together. You can monitor the jobs with option 20 (Work with TCP/IP jobs in QSYSWRK subsystem) from the TCP/IP Administration menu.

If you want TCP/IP processing and any related TCP/IP servers to start automatically at the initial program load (IPL), add STRTCP to the QSTRUP CL program.

**Note:** If they are installed, the Client Access host servers are automatically started when TCP/IP is started.

**Changing the IPL Start-Up Program** The autostart job in the controlling subsystem transfers control to the program specified in the system value QSTRUPPGM. You can tailor this program. For instructions on how to create your own IPL start-up program, see Work Management (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzaks/rzaks1.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

**REMINDER: Host Table Conversion:** If you had a pre-V3R1M0 version of TCP/IP installed on your iSeries and you had a local host table with more than 75 entries, use one of the host table configuration commands, such as CHGTCPHTE or MRGTCPHT before you run the STRTCP command. Using the host table configuration commands converts pre-V3R1M0 host tables to the new format without affecting the performance of the STRTCP command processing.

## TCP/IP Jobs

Jobs started by the Start TCP/IP (STRTCP) command are listed in Table 3.

Table 3. Jobs Used by TCP/IP

| Job Name    | Description                          |
|-------------|--------------------------------------|
| QAPPCTCP    | APPC over TCP/IP applications        |
| QTBOOTP     | BOOTP server                         |
| QTCPIP      | Main TCP/IP job                      |
| QTFTPxxxxx  | FTP server (there may be several)    |
| QTGTELNETS  | TELNET server (there may be several) |
| QTRTDxxxxx  | RouteD server                        |
| QTRXCxxxx   | REXEC server (there may be several)  |
| QTSMTPLNT   | SMTP client                          |
| QTSMTPSRVR  | SMTP server                          |
| QTSMTPBRCCL | SMTP bridge client                   |
| QTSMTPBRSR  | SMTP bridge server                   |
| QTIFTxxxxx  | TFTP server (there may be several)   |
| QTMSNMP     | SNMP server                          |
| QTMSNMPRCV  | SNMP server                          |
| QSNMPSA     | SNMP server                          |
| QTLPDxxxxx  | LPD server (there may be several)    |
| QTPOxxxxxx  | POP server (there may be several)    |
| QTTPANSxxx  | Dial-in (*ANS) support (PPP)         |
| QTTPDIALxx  | Dial-out (*DIAL) support (PPP)       |

Table 3. Jobs Used by TCP/IP (continued)

| Job Name  | Description                                |
|---|--|
| ADMIN and DEFAULT   | ICS (HTTP) server                          |
| QTWSGxxxx   | Workstation gateway (there may be several) |
| <p><b>Note:</b></p> <ol style="list-style-type: none"> <li>1. There may be other jobs running in the QSYSWRK subsystem that have nothing to do with TCP/IP.</li> <li>2. The TCP/IP jobs in QSYSWRK run under the QTCP user profile, with two exceptions: the TFTP server runs under the QTFTP profile, and the workstation gateway server runs under the QTMTWSG profile.</li> <li>3. To use APPC over TCP/IP applications, you must set the network attribute Allow AnyNet<sup>®</sup> (ALWANYNET) to *YES.</li> </ol> |  |

### End TCP/IP (ENDTCP):

#### **ATTENTION!**

No confirmation display appears when you enter ENDTCP is entered. Therefore, you must use the ENDTCP command carefully. The default for the ENDTCP command is to immediately end all TCP/IP processing on the server that you are working on.

Use the End TCP/IP (ENDTCP) command to end all TCP/IP processing.

The command can be issued from the command line or by using option 4 on the TCP/IP Administration menu. To display this menu, enter GO TCPADM on the command line.

## Step 9—Verifying the TCP/IP Connection

To verify the TCP/IP connection from your server to the network, use the PING (VFYTCPCNN) function.

1. To test the TCP/IP code without sending anything out of the token-ring adapter, specify the special host name LOOPBACK as follows:

```
PING LOOPBACK
```

2. To test the TCP/IP code, token-ring adapter, and token-ring connection, specify the Internet address of the local adapter, as defined in the host table, as follows:

```
PING RMTSYS(*INTNETADR)
INTNETADR('9.4.73.212')
```

Or you may enter:

```
PING RMTSYS(SYSNAM890)
```

This command sends data out onto the token-ring line, which the local adapter receives again as if the data is from the TCP/IP network.

Figure 18 on page 27 shows the results from a successful connection verification.



```

> ping '9.4.73.212'
Verifying connection to host system 9.4.73.212.
PING request 1 from 9.4.73.212 took 24 ms. 256 bytes. TTL 64.
PING request 2 from 9.4.73.212 took 11 ms. 256 bytes. TTL 64.
PING request 3 from 9.4.73.212 took 31 ms. 256 bytes. TTL 64.
PING request 4 from 9.4.73.212 took 11 ms. 256 bytes. TTL 64.
PING request 5 from 9.4.73.212 took 12 ms. 256 bytes. TTL 64.
Round-trip (in milliseconds) min/avg/max = 11/17/31
Connection verification statistics: 5 of 5 successful (100 %).

```

Figure 18. Successful PING Messages

3. If the PING operation is successful, you should see messages similar to those in Figure 18.

If the PING operation is unsuccessful, you should see messages similar to those in Figure 19.

If you receive an unsuccessful PING message, check your configuration steps. Also check that the configuration at the remote system is correct and that the remote system is not powered down. For additional information about identifying the cause for an unsuccessful connection verification, see TCP/IP Troubleshooting

(<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzaku/rzakuoverview.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

```

> ping '9.4.73.198'
Verifying connection to host system 9.4.73.198.
No response from host within 1 seconds for connection verification 1.
No response from host within 1 seconds for connection verification 2.
No response from host within 1 seconds for connection verification 3.
No response from host within 1 seconds for connection verification 4.
No response from host within 1 seconds for connection verification 5.
Connection verification statistics: 0 of 5 successful (0 %).

```

Bottom

Figure 19. Unsuccessful PING Messages

**Note:** A datagram sent by TCP or UDP to a system with the name LOOPBACK does not actually leave the system. The IP layer, instead, returns the datagram to the TCP or UDP layer from which it came. The other layers then treat the datagram as a normal incoming datagram. The LOOPBACK host name can be used with any TCP/IP command requiring a system name, such as PING or FTP (or any TCP or UDP application including user-written applications). Using the LOOPBACK default host name provides an ability to test TCP/IP applications without actually connecting to a physical network.

The server defines LOOPBACK as the default host name by automatically creating an entry in the local host table.

## Verifying Additional TCP/IP Connections

Once TCP/IP is configured on the iSeries, and the initial connection is verified, you will probably want to add more systems to your network. When you connect

additional systems to your network, you also need to verify their TCP/IP connection. The examples in the following paragraphs show you how to verify a remote TCP/IP connection.

Use the system menus or the Verify TCP/IP Connection (VFYTCPCNN or PING) command to verify your system's ability to communicate with a remote system using TCP/IP.

**Note:** PING uses the Internet Control Message Protocol (ICMP) to send data to a host's Internet address and waits for a response. The user command to perform this verification is called PING (Packet InterNet Groper) on non-iSeries servers. On an iSeries server, use either the PING command or the VFYTCPCNN command.

To verify TCP/IP connections, perform the three steps below in the order in which they are listed:

1. Type VFYTCPCNN and then press F4.  
The display for the VFYTCPCNN command appears (Figure 20).
2. Type the name of a remote system as defined in your host table or as defined by your domain name server.  
If you prefer to use an Internet address, type the address enclosed in apostrophes. You can also type \*INTERNETADR to be prompted for the Internet address.
3. Press F10 to view or change the additional parameters.  
As you can see in Figure 21 on page 29, the system defaults are to send five packets of 256 bytes each and to wait 1 second for a response on each packet.

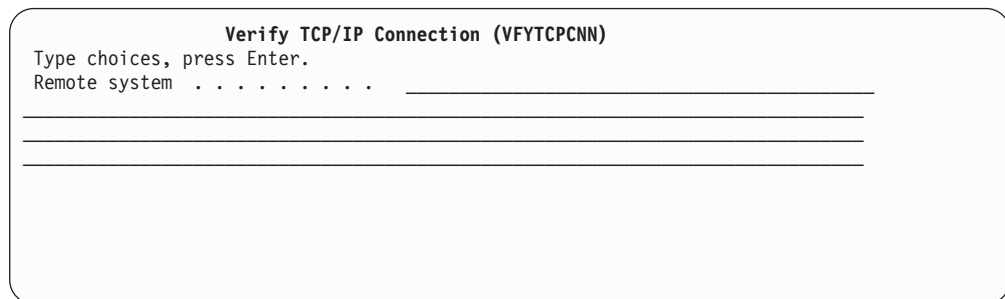


Figure 20. Verify TCP/IP Connection

**Verify TCP/IP Connection (PING)**

Type choices, press Enter.

Remote system . . . . . sysnam36.sysnam123.ibm.com

---

Remote internet address . . . . . \_\_\_\_\_

Additional Parameters

Message mode:

|                                  |                   |                                 |
|----------------------------------|-------------------|---------------------------------|
| Response message detail . . .    | <i>*VERBOSE</i>   | <i>*VERBOSE, *QUIET</i>         |
| Summary, if response errors .    | <i>*COMP</i>      | <i>*COMP, *ESCAPE</i>           |
| Packet length (in bytes) . . . . | <i>256</i>        | <i>8-512</i>                    |
| Number of packets . . . . .      | <i>5</i>          | <i>1-999</i>                    |
| Wait time (in seconds) . . . . . | <i>1</i>          | <i>1-120</i>                    |
| Local internet address . . . . . | <i>*ANY</i> _____ |                                 |
| Type of service . . . . .        | <i>*NORMAL</i>    | <i>*MINDELAY, *MAXTHRPUT...</i> |
| IP time to live . . . . .        | <i>*DFT</i>       | <i>1-255, *DFT</i>              |

**More...**

F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display  
F24=More keys

Figure 21. Verify TCP/IP Connection, Additional Parameters

### Verifying TCP/IP Connections with Host Name—Example

In this example, sending five packets of 256 bytes each verifies the connection to the remote system SYSNAM36. The local system waits 1 second for a response to each packet that is sent.

```

Verify TCP/IP Connection (PING)

Type choices, press Enter.

Remote system . . . . . > SYSNAM36.SYSNAM123.IBM.COM_____

_____  

_____  

_____  

Additional Parameters

Message mode:
Response message detail . . . *VERBOSE *VERBOSE, *QUIET
Summary, if response errors . *COMP *COMP, *ESCAPE
Packet length (in bytes) . . . 256 8-512
Number of packets . . . . . 5 1-999
Wait time (in seconds) . . . . 1 1-120
Local internet address . . . . *ANY_____
Type of service . . . . . *NORMAL *MINDELAY, *MAXTHRPUT...
IP time to live . . . . . *DFT 1-255, *DFT

More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

```

Figure 22. Verifying Connection to Remote System SYS1

### Verifying TCP/IP Connections with Internet Address—Example

In this example, (Figure 22) the connection to the remote system at Internet address 9.4.191.76 is verified using the system defaults for packet length, number of packets, and wait time.

```

Verify TCP/IP Connection (PING)

Type choices, press Enter.

Remote system . . . . . *intnetadr_____

_____  

_____  

Remote internet address . . . . > '9.4.191.76'

```

Figure 23. Verifying Connection to Remote System at Internet Address 9.4.191.76

## Step 10—Saving Your TCP/IP Configuration

To save your TCP/IP configuration files, use the following command:

```
SAVOBJ OBJ(QATOC* QATM*) LIB(QUSRSYS)
DEV(TAP01) OBJTYPE(*FILE)
```

The associated line descriptions are not saved with this command. Configuration objects are saved with the system.

To maintain consistency, save all TCP/IP configuration files together.

**Note:** You do not have to end TCP/IP in order to save the configuration files. However, you should end TCP/IP before any TCP/IP configuration files are restored.



---

## Chapter 2. TCP/IP: Operation, Management, and Advanced Topics

This chapter discusses managing your network by using the NETSTAT command, and the maintenance of host tables. In addition, this chapter covers other topics beyond those that are required to configure and use TCP/IP on iSeries 400. This information may help you to understand and maximize your usage of the iSeries TCP/IP support.

TCP/IP on an iSeries server can also be managed by Simple Network Management Protocol (SNMP). For information about SNMP, see resources in the Information Center: Supplemental Manuals.

---

### Network Status

The network status function on the server allows you to get information about the status of TCP/IP network interfaces, routes, and connections on your local system. This function also allows you to end TCP/IP connections and to start or end TCP/IP interfaces.

**Note:** Network status functions may also be administered by Operations Navigator. Use the Operations Navigator interface for these functions if it is installed on your system. See the Operations Navigator ([http://www.as400.ibm.com/oper\\_nav/index.htm](http://www.as400.ibm.com/oper_nav/index.htm)) Web page for more information.

NETSTAT displays the current TCP/IP protocol stack information. This information does not necessarily match the configuration data you see when using the Configure TCP/IP (CFGTCP) menu. In most cases, the NETSTAT command displays more information than the configuration data. In some cases, the configuration data might even change.

The reason for such a change is that the iSeries TCP/IP dynamically creates some information, such as \*DIRECT routes, when TCP/IP starts. A change may also occur if the configuration data that was sent to TCP/IP when it starts is changed dynamically by TCP/IP applications that run after you start TCP/IP. Several types of processing alter the initial TCP/IP configuration:

- Internet Control Message Protocol (ICMP) requests
- Sockets ioctl system calls
- Simple Network Management Protocol (SNMP) requests
- iSeries TCP/IP internal processing

### Work with TCP/IP Network Status Menu

The Work with TCP/IP Network Status menu allows you to work with the various network status functions.

To display the Work with TCP/IP Network Status menu, take these steps:

1. Type the WRKTCPSTS (Work with TCP/IP Network Status) command or the NETSTAT (Network Status) command.
2. Press the Enter key. (See Figure 24 on page 34.)

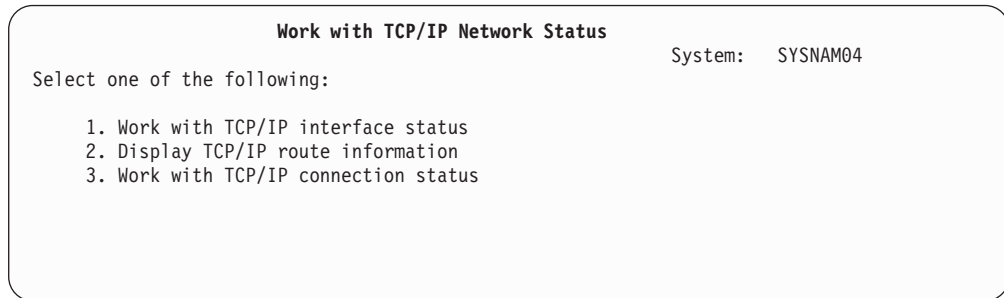


Figure 24. Work with TCP/IP Network Status

## Work with TCP/IP Interface Status

The Work with TCP/IP Interface Status display, as shown in Figure 25, provides the most current summary of interface activity. This display allows you to view TCP/IP interface information for selected interfaces and to start or end TCP/IP interfaces. To view the Work with TCP/IP Interface Status display, take these steps:

1. Type 1 on the command line of the Work with TCP/IP Network Status menu or enter the WRKTCPSTS \*IFC command.
2. Press the Enter key.

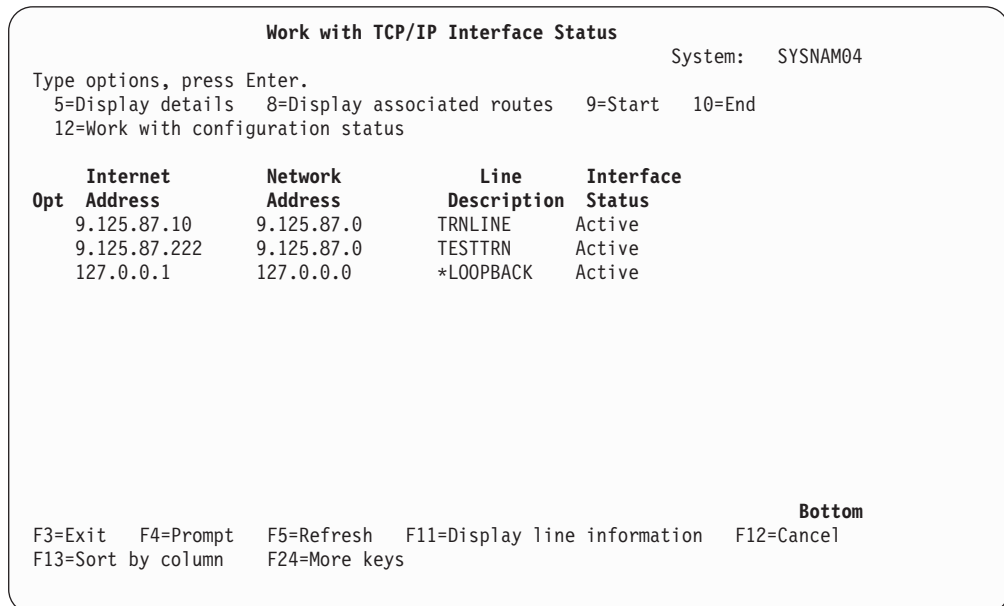


Figure 25. Work with TCP/IP Interface Status, Display 1 of 2

Press F11 to change the contents of the display to include the subnet mask, type of service, maximum transmission unit (MTU), and line type, as shown in Figure 26 on page 35.



```

Work with TCP/IP Interface Status
System:  SYSNAM04
Type options, press Enter.
5=Display details  8=Display associated routes  9=Start  10=End
12=Work with configuration status

  Internet      Subnet      Type of      Line
Opt  Address      Mask        Service      MTU  Type
  9.125.87.10   255.255.255.0 *MAXTHRPUT   1989 *TRLAN
  9.125.87.222 255.255.255.0 *NORMAL      1989 *TRLAN
  127.0.0.1     255.0.0.0    *NORMAL      576  *NONE

```

Figure 26. Work with TCP/IP Interface Status, Display 2 of 2

### Starting TCP/IP Interfaces

TCP/IP interfaces are started in one of the following ways:

- The Work with TCP/IP Interface Status displays are reached by:
  - Option 1 on the Configure TCP/IP (CFGTCP) menu
  - Option 1 on the Network Status (NETSTAT or WRKTC PSTS) menu
- The Start TCP/IP Interface (STRTCPIFC) command
- Using the Operations Navigator interface

**Note:** You can start TCP/IP interfaces through the Operations Navigator interface wizard. However, this chapter does not document any of the Operations Navigator functions. See the online help in Operations Navigator for this information.

To start a TCP/IP interface from the Work with TCP/IP Interface Status menu, type 9 in the option field for each interface that you want to start and press the Enter key.

To start a TCP/IP interface using the STRTCPIFC command, take these steps:

1. Type STRTCPIFC on the command line and press F4 (Prompt).
2. Type the Internet address of the interface that you want to start and press the Enter key.

Option 9 on the Work with TCP/IP Interface Status display is used to start both TCP/IP interfaces and Internet Protocol (IP) over Systems Network Architecture (SNA) interfaces. For information about starting IP over SNA interfaces, see the STRIPSIFC (Start IP over SNA Interface) command in Control Languages (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rbam6/rbam6clmain.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

**Note:** When starting the first TCP/IP interface associated with an Integrated xSeries Server for iSeries (also known as File Server Input/Output Processor and FSIOP) network server description, a considerable amount of time may pass before the interface becomes active. This is because TCP/IP activation includes starting the network server. The amount of time that is required

depends mainly on machine use and the size of the processor. To determine whether the interface has started, view the messages in the QTCPIP job log and the QSYSOPR message queue.

## Ending TCP/IP Interfaces

The ENDTCPIFC (End TCP/IP Interface) command ends an existing TCP/IP interface immediately. As a result, all TCP/IP connections using this interface also end immediately. However, the operation of any other TCP or IP over SNA interface, using the same line description as the interface that is ending, is not affected.

TCP/IP interfaces can be ended in one of two ways:

- Using the Work with TCP/IP Interface Status display, which is reached by:
  - Option 1 on the Configure TCP/IP (CFGTCP) menu
  - Option 1 on the Network Status (NETSTAT or WRKTCPSTS) menu
- Using the ENDTCPIFC (End TCP/IP Interface) command

To end a TCP/IP interface from the Work with TCP/IP Interface Status menu:

1. Type 10 in the option field for each interface that you want to end.
2. Press the Enter key.

To end a TCP/IP interface using the ENDTCPIFC command:

1. Type ENDTCPIFC on the command line.
2. Press F4 (Prompt).
3. Type the Internet address of the interface that you want to end.
4. Press the Enter key.

Option 10 on the Work with TCP/IP Interface Status display is used to end both TCP/IP interfaces and IP over SNA interfaces. For information about ending IP over SNA interfaces, see the ENDIPSIFC (End IP over SNA Interface) command in Control Languages

(<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rbam6/rbam6clmain.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

**Route-to-Interface Binding:** Interfaces define direct paths to networks or subnetworks to which an iSeries server is directly attached. Routes define indirect paths. A route identifies the first hop on the path to a network or subnetwork to which an iSeries is not directly attached.

Routes are bound to interfaces through the use of a best-match-first algorithm. This algorithm is based on the state of the interface, and on the type of service (TOS) specified for the route and interface. When you end an interface, the routes associated with the interface can move to another existing active interface if the following conditions are satisfied:

- If the TOS for the route is something other than \*NORMAL, the algorithm looks for an interface with the same TOS. If an interface with the specified TOS is not found, an interface with TOS \*NORMAL is sought. Again, if one is not found, that route will not be moved.
- The MTU value for the route that is being moved must be less than or equal to the MTU value for the active interface.

- The network ID of the interface must be equal to the logical AND of the next hop for the route and the subnet mask for the interface.

**Notes:**

1. If the next hop of a route is identical to an interface's IP address, that route will never be bound to another interface.
2. When starting interfaces (if all interfaces are currently inactive) routes are bound to the interfaces with the same best-match-first algorithm. An exception is if the route is defined with a preferred binding interface. In this case, an attempt is made to bind the route to the interface that is indicated. If the binding attempt fails, then the best-match-first algorithm is used.

## Display TCP/IP Route Information

The display TCP/IP route information function allows you to view information about TCP/IP routes.

To display TCP/IP route information:

1. On the Work with TCP/IP Network Status menu, type 2 on the command line or enter the WRKTCPSTS \*RTE command.
2. Press the Enter key.

The first of the two Display TCP/IP Route Information displays appears, as shown in Figure 27.

| Display TCP/IP Route Information |                   |               |                        | System: SYSNAM04 |
|----------------------------------|-------------------|---------------|------------------------|------------------|
| Type options, press Enter.       |                   |               |                        |                  |
| 5=Display details                |                   |               |                        |                  |
| Opt                              | Route Destination | Subnet Mask   | Next Hop               | Route Available  |
|                                  | 9.125.87.0        | 255.255.255.0 | *DIRECT                | *YES             |
|                                  | 9.125.87.0        | 255.255.255.0 | *DIRECT                | *YES             |
|                                  | 9.125.109.3       | *HOST         | 9.125.87.17            | *YES             |
|                                  | 127.0.0.0         | 255.0.0.0     | *DIRECT                | *YES             |
|                                  | *DFTRROUTE        | *NONE         | 9.125.87.169           | *YES             |
|                                  | *DFTRROUTE        | *NONE         | 9.125.87.250           | *YES             |
|                                  |                   |               |                        | <b>Bottom</b>    |
| F3=Exit                          | F5=Refresh        | F6=Print list | F11=Display route type | F12=Cancel       |
| F13=Sort by column               |                   | F17=Top       | F18=Bottom             |                  |

Figure 27. Display TCP/IP Route Information, Display 1 of 2

To view the second display, press F11 (Display route type). The route information is presented as shown in Figure 28 on page 38. To return to the first display, press F11 (Display next hop).

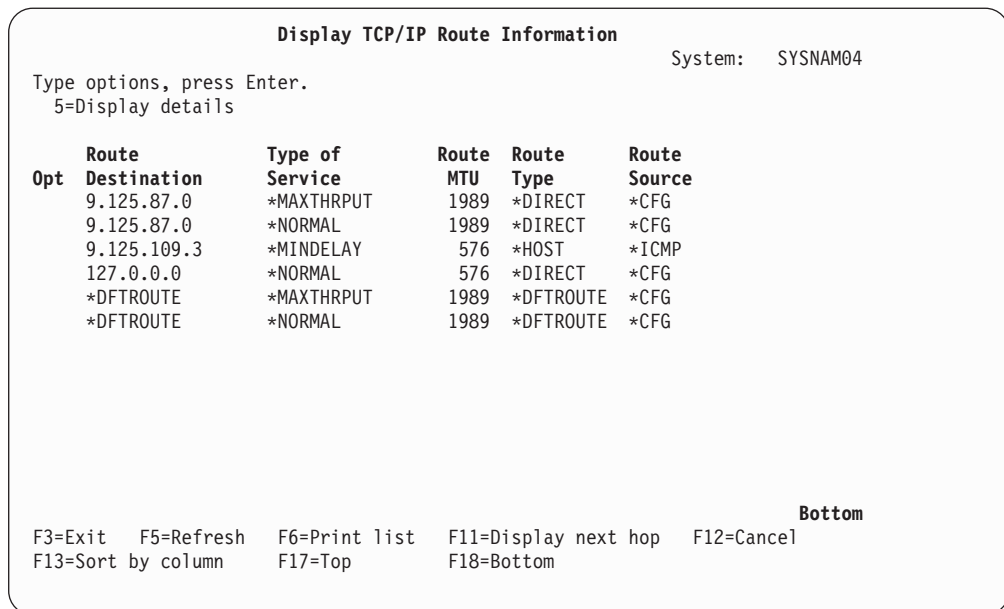


Figure 28. Display TCP/IP Route Information, Display 2 of 2

To view detailed information about a specific route, type 5 in the option field next to the route and press the Enter key.

Routes listed on the Display TCP/IP Route Information display differ from the routes that are displayed on the Work with TCP/IP Routes display. Only routes with a route source of \*CFG and a route type that is not \*DIRECT can be changed with the Work with TCP/IP Routes display. Similarly, only routes that meet these conditions can be changed or removed with the CHGTCPRTE or RMVTCPRTE commands. \*CFG means the route was added using iSeries configuration commands or is a \*DIRECT route. \*DIRECT means that the route is to a network or subnetwork to which this system has a direct physical connection. This route is not defined with an add route command.

## Work with TCP/IP Connection Status

The Work with TCP/IP Connection Status display allows you to display or end a TCP/IP connection between a local system and a remote system.

To display the Work with TCP/IP Connection Status display:

1. Type 3 on the command line of the Work with TCP/IP Network Status menu or enter the WRKTCPSTS \*CNN command.
2. Press the Enter key.

The first of the three Work with TCP/IP Connection Status displays, as shown in Figure 29 on page 39.

To display the second and third Work with TCP/IP Connection Status displays, press F11 (see Figure 30 on page 39 and Figure 31 on page 40). To display port numbers instead of port service names, press F14.

In Figure 29 on page 39, the connections indicate that the FTP server, SMTP server, and TELNET server are active and ready to receive connection attempts. Because no connection has been established yet, the *Remote Address* and *Remote Port* fields



```

Work with TCP/IP Connection Status
System:  SYSNAM04
Local internet address . . . . . : *ALL
Type options, press Enter.
  4=End  5=Display details

  Remote      Remote      Local      Local
  Opt  Address  Port      Address  Port      Type
  *    *      *         *        ftp-con > *TCP
  *    *      *         *        telnet    *TCP
  *    *      *         *        telnet    *TCP
  *    *      *         *        lpd       *TCP
  *    *      *         *        1070     *TCP
  9.5.1.131  1954      9.125.87.10  telnet    *TCP
  9.5.1.180  1211      9.125.87.10  telnet    *TCP
  9.5.15.134 1024      9.125.87.10  telnet    *TCP
  9.130.38.18 2099      9.125.87.222 telnet    *TCP
  9.130.38.74 1125      9.125.87.10  telnet    *TCP
  9.130.38.74 1126      9.125.87.222 telnet    *TCP

F5=Refresh  F11=Display connection state  F13=Sort by column
F14=Display port numbers  F22=Display entire field  F24=More keys
More...

```

Figure 31. Work with TCP/IP Connection Status, Display 3 of 3

### Ending TCP/IP Connections

TCP/IP connections and User Datagram Protocol (UDP) sockets can be ended from the Work with TCP/IP Connection Status display. To do so:

1. Type 4 in the option field for the lines containing the connections that you want to end.
2. Press the Enter key.

The Confirm End of TCP/IP Connections displays is then presented as shown in Figure 32 on page 41.

```

                                Confirm End of TCP/IP Connections
                                System:  SYSNAM04
Local internet address . . . . . : *ALL

Press Enter to confirm your choices for 4=End.
Press F12 to return to change your choices.

  Opt  Remote      Remote   Local      Local
      Address     Port     Address    Port      Type
  4    9.5.15.134  1024    9.125.87.10 telnet   *TCP

                                                                 Bottom
F11=Display connection state  F12=Cancel  F14=Display port numbers
F22=Display entire field

```

Figure 32. Confirm End of TCP/IP Connections

To end the TCP/IP connections, press the Enter key from the Confirm End of TCP/IP Connections display.

If you decide not to end a TCP/IP connection or if you want to change your choices, press F12 (Cancel).

## Working with Configuration Status

To work with the line description used by an interface:

1. On the Work with TCP/IP Interface Status menu, type 12 in the option field for each interface that you want to work with.
2. Press the Enter key.

This option issues the WRKCFGSTS (Work with Configuration Status) command for the line description associated with the interface. Using the options shown in Figure 33 on page 42 you can vary a line description on or off, display the Work with Job menu, and display the line description or mode status.

This option cannot be used for IP over SNA interfaces because IP over SNA does not use specific line descriptions.

```

Work with Configuration Status                                SYSNAM04
                                                           04/26/94 15:55:58
Position to . . . . . Starting characters

Type options, press Enter.
 1=Vary on  2=Vary off  5=Work with job  8=Work with description
 9=Display mode status ...

Opt  Description      Status      -----Job-----
TRNLINE              ACTIVE
TRNLINET             ACTIVE
TRNLITCP             ACTIVE
QTCTPIP             QTCTP             007936

```

Figure 33. Work with Configuration Status

## Displaying TCP/IP Network Status Information

In addition to working with network status functions, the Work with TCP/IP Network Status menu allows you to display current information about your TCP/IP network, including multicast groups, TCP/IP interfaces, and associated routes, to name a few.

### Display Multicast Groups

To display the multicast groups associated with an interface:

1. On the Work with TCP/IP Interface Status display, type 14 in the option field for each interface for which you want to see the associated multicast groups.
2. Press the Enter key.

Figure 34 on page 43 illustrates the display of the multicast groups for an Ethernet interface.

If you have requested multicast group information for more than one interface, press the Enter key to review the remaining displays.



```

Display Multicast Host Groups
System:  SYSNAM04
Interface internet address . . . . . : 10.5.5.55

Host Group      Hardware Address      Host Group      Hardware Address
224.0.0.1        01:00:5E:00:00:01
225.4.5.6        01:00:5E:04:05:06
233.32.40.51     01:00:5E:20:28:33
224.0.0.9        01:00:5E:00:00:09
229:200:100:1    01:00:5E:48:64:01

Bottom
F3=Exit  F5=Refresh  F6=Print  F9=Command line  F11=Hide hardware address
F12=Cancel

```

Figure 34. Display Multicast Host Groups

### Displaying TCP/IP Interfaces

To display more detailed information about the TCP/IP interface status for specific interfaces:

1. On the Work with TCP/IP Interface Status display, type 5 in the option field for each interface about which you want more information.
2. Press the Enter key.

If you requested status for a token-ring interface, the information displays, as shown in Figure 35 on page 44.

If you have requested interface status information for more than one interface, press the Enter key to view the remaining displays.

```

Display TCP/IP Interface Status
System:  SYSNAM04
Interface host name . . . . . :  sysnam04.endicott.ibm. >
Internet address . . . . . :  9.125.87.10
  Subnet mask . . . . . :  255.255.255.0
  Network address . . . . . :  9.125.87.0
  Host address . . . . . :  0.0.0.10
  Directed broadcast address . . . . . :  9.125.87.255

Interface status . . . . . :  Active
Change date/time . . . . . :  04/26/94  14:32:32
Line description . . . . . :  TRNLIN
Line type . . . . . :  *TRLAN
Type of service . . . . . :  *MAXTHRPUT
Maximum transmission unit . . . . . :  1989
Automatic start . . . . . :  *YES

TRLAN bit sequencing . . . . . :  *MSB

```

Figure 35. Display TCP/IP Interface Status for a Token-Ring Interface

### Displaying Associated Routes

To display information about the routes associated with a specific interface:

1. On the Work with TCP/IP Interface Status display, type 8 in the option field for each interface for which you want to see the associated routes information.
2. Press the Enter key.

The first of two displays with associated route information is shown in Figure 36 on page 45.

If you have requested associated route information for more than one interface, press the Enter key to view the remaining displays.

```

                                Display Associated Routes
                                System:  SYSNAM04
Interface internet address . . . . . : 9.125.87.10

Type options, press Enter.
5=Display details

  Route      Subnet      Next      Route
Opt  Destina  Mask       Hop       Availabl
   9.125.87.0 255.255.255.0 *DIRECT
   *DFTRoute *NONE         9.125.87.169 *YES
                                     *YES

                                Bottom
F3=Exit  F5=Refresh  F6=Print list  F11=Display route type  F12=Cancel
F13=Sort by column  F17=Top      F18=Bottom

```

Figure 36. Associated Route Information, Display 1 of 2

Press F11 to show the display that includes the type of service (TOS), maximum transmission unit (MTU), type, and source.

### Displaying Route Details Option

To display detailed information about the route:

1. On the Display Associated Routes display, type 5 in the option field for each route about which you want more information.
2. Press the Enter key.

Figure 37 on page 46 and Figure 38 on page 46 are examples.

```

                                Display TCP/IP Route Details
                                System:  SYSNAM04

Route information:
Route destination . . . . . : 9.125.87.0
Subnet mask . . . . . : 255.255.255.0
Next hop host name . . . . . : sysnam04.endicott.ibm. >
Next hop . . . . . : *DIRECT
Type of service . . . . . : *MAXTHRPUT
Route available . . . . . : *YES
Route type . . . . . : *DIRECT
Route source . . . . . : *CFG
Change date/time . . . . . : 04/26/94 14:32:32
Route maximum transmission unit . . . . . : 1989
Reference count . . . . . : 0

Local interface information:
Internet address . . . . . : 9.125.87.10
Subnet mask . . . . . : 255.255.255.0
Network address . . . . . : 9.125.87.0

More...

Press Enter to continue.

F3=Exit  F6=Print  F12=Cancel  F22=Display entire field

```

Figure 37. Display TCP/IP Route Details, Display 1 of 2

```

                                Display TCP/IP Route Details
                                System:  SYSNAM04

Interface status . . . . . : Active
Line description . . . . . : TRNLINE
Line type . . . . . : *TRLAN

```

Figure 38. Display TCP/IP Route Details, Display 2 of 2

### Displaying TCP/IP Route Information

To display TCP/IP route information:

1. On the Work with TCP/IP Network Status menu, type 2 on the command line or enter the WRKTCPSTS \*RTE command.
2. Press the Enter key.

The first of the two Display TCP/IP Route Information displays is presented as shown in Figure 39 on page 47.

```

Display TCP/IP Route Information                                System:  SYSNAM04
Type options, press Enter.
5=Display details

  Route      Subnet      Next      Route
Opt  Destination  Mask      Hop      Available
  9.125.87.0  255.255.255.0 *DIRECT   *YES
  9.125.87.0  255.255.255.0 *DIRECT   *YES
  9.125.109.3 *HOST        9.125.87.17 *YES
  127.0.0.0   255.0.0.0    *DIRECT   *YES
  *DFTRROUTE  *NONE        9.125.87.169 *YES
  *DFTRROUTE  *NONE        9.125.87.250 *YES

Bottom
F3=Exit  F5=Refresh  F6=Print list  F11=Display route type  F12=Cancel
F13=Sort by column  F17=Top      F18=Bottom

```

Figure 39. Display TCP/IP Route Information, Display 1 of 2

To view the second Display TCP/IP Route Information display, press F11 (Display route type). The route information is presented in Figure 40. To return to the first display, press F11 (Display next hop).

```

Display TCP/IP Route Information                                System:  SYSNAM04
Type options, press Enter.
5=Display details

  Route      Type of      Route  Route  Route
Opt  Destination  Service    MTU   Type   Source
  9.125.87.0  *MAXTHRPUT  1989  *DIRECT *CFG
  9.125.87.0  *NORMAL     1989  *DIRECT *CFG
  9.125.109.3 *MINDELAY   576   *HOST  *ICMP
  127.0.0.0   *NORMAL     576   *DIRECT *CFG
  *DFTRROUTE  *MAXTHRPUT  1989  *DFTRROUTE *CFG
  *DFTRROUTE  *NORMAL     1989  *DFTRROUTE *CFG

Bottom
F3=Exit  F5=Refresh  F6=Print list  F11=Display next hop  F12=Cancel
F13=Sort by column  F17=Top      F18=Bottom

```

Figure 40. Display TCP/IP Route Information, Display 2 of 2

To view detailed information about a specific route, type 5 in the option field next to the route and press the Enter key. See Figure 37 on page 46 and Figure 38 on page 46.

## Displaying TCP/IP Connections

You can request more detailed information about TCP/IP connections shown on the Work with TCP/IP Connection Status display. This information includes timing information and transmission statistics for the connection displayed.

To display more information about the listed TCP/IP connections:

1. Type 5 in the option field for each connection about which you want more information.
2. Press the Enter key.

A series of up to three displays for each connection appears. Press the Page Down key to view the remaining displays.

The contents of the displays vary depending on the type of connection, whether \*TCP, \*UDP, or \*IPS. (Figure 41, Figure 42 on page 49, and Figure 43 on page 49 show displays for a TCP connection.)

```

                                Display TCP Connection Status
                                System:  SYSNAM04
Connection identification:
Remote host name . . . . . : drfun.rchland.ibm.com
Remote internet address . . . . . : 9.5.15.134
Remote port . . . . . : 1025
Local host name . . . . . : sysnam04.endicott.ibm. >
Local internet address . . . . . : 9.125.87.143
Local port . . . . . : telnet
Associated user profile . . . . . : QTCP
TCP programming interface information:
State . . . . . : Established
Connection open type . . . . . : Passive
Timing information:
Idle time . . . . . : 000:00:00.381
Last activity date/time . . . . . : 05/25/94 14:38:11
Round-trip time . . . . . : .133
Round-trip variance . . . . . : .016

                                More...

Press Enter to continue.
F3=Exit  F5=Refresh  F6=Print  F10=Display IP options  F12=Cancel
F14=Display port numbers  F22=Display entire field
```

Figure 41. Display TCP/IP Connection Status, Display 1 of 3

```

Display TCP Connection Status
System:  SYSNAM04
Bytes out . . . . . : 57692
  Outgoing bytes buffered . . . . . : 0
  User send next . . . . . : 3270868150
  Send next . . . . . : 3270868150
  Send unacknowledged . . . . . : 3270868150
  Outgoing push number . . . . . : 3270868149
  Outgoing urgency number . . . . . : 3270868149
  Outgoing window number . . . . . : 3270896558
Bytes in . . . . . : 1021
  Incoming bytes buffered . . . . . : 0
  Receive next . . . . . : 1545153023
  User receive next . . . . . : 1545153023
  Incoming push number . . . . . : 1545153023
  Incoming urgency number . . . . . : 1545153022
  Incoming window number . . . . . : 1545160742

More...

Press Enter to continue.
F3=Exit  F5=Refresh  F6=Print  F10=Display IP options  F12=Cancel
F14=Display port numbers  F22=Display entire field

```

Figure 42. Display TCP/IP Connection Status, Display 2 of 3

```

Display TCP Connection Status
System:  SYSNAM04
Retransmission information:
  Total retransmissions . . . . . : 8
  Current retransmissions . . . . . : 0
Send window information:
  Maximum size . . . . . : 28672
  Current size . . . . . : 28408
  Last update . . . . . : 1545153004
  Last update acknowledged . . . . . : 3270868150
  Congestion window . . . . . : 2704
  Slow start threshold . . . . . : 1281
Precedence and security:
  Precedence . . . . . : 0
Initialization information:
  Maximum segment size . . . . . : 536
  Initial send sequence number . . . . . : 3270810457
  Initial receive sequence number . . . . . : 1545152001

Bottom

Press Enter to continue.
F3=Exit  F5=Refresh  F6=Print  F10=Display IP options  F12=Cancel
F14=Display port numbers  F22=Display entire field

```

Figure 43. Display TCP/IP Connection Status, Display 3 of 3

## Displaying Connection Totals

To display a summary of TCP and UDP counts, press F10 on the Work with TCP/IP Connection Status display. The counts provided are a cumulative summary of all TCP and UDP activity since the last time the STRTCP (Start TCP) command was issued.

The information in Figure 44 on page 50 and Figure 45 on page 50 shows TCP and UDP counts that are maintained for Simple Network Management Protocol

(SNMP). For additional information about SNMP, see resources in the Information Center: Supplemental Manuals.

```

Display TCP/IP Connection Totals                                System:  SYSNAM04
TCP connection information:
Currently established . . . . . : 1
Active opens . . . . . : 0
Passive opens . . . . . : 0
Attempted opens that failed . . . . . : 0
Established and then reset . . . . . : 0

TCP send information:
Segments sent . . . . . : 108
Retransmitted segments . . . . . : 10
Reset segments . . . . . : 0

TCP receive information:
Segments received . . . . . : 117
Segments received in error . . . . . : 0

Press Enter to continue.

F3=Exit  F5=Refresh  F6=Print  F12=Cancel

More...
```

Figure 44. Display TCP/IP Connection Totals, Display 1 of 2

```

Display TCP/IP Connection Totals                                System:  SYSNAM04
UDP send information:
Datagrams sent . . . . . : 0

UDP receive information:
Datagrams received . . . . . : 0
Datagrams not delivered . . . . . : 0
Application port not found . . . . . : 0
Other datagrams in error . . . . . : 0
```

Figure 45. Display TCP/IP Connection Totals, Display 2 of 2

---

## TCP/IP Host Tables

Host tables are a method for mapping host names to IP addresses. This is done by using a hosts file for name-to-address resolution. Because the host table lacks the structure to list names in any hierarchical order, names assigned to hosts must be unique. In the topics that follow, you will find discussions about the overall management of TCP/IP host tables. Instructions for merging host tables and managing a host table from a central site are included.

Successful TCP/IP host table maintenance also includes periodically evaluating whether or not to use a DNS server to manage your network. The DNS server is often the preferred alternative to host tables for the purpose of managing IP addresses and host names, particularly in large network environments. However, even some small organizations that access the Internet require a DNS server to meet their name-service needs.



---

## Managing TCP/IP Host Tables

In a large network, it can be more efficient to administer iSeries TCP/IP from a central site. Working with the host table would be time consuming if each system is individually updated with the TCP/IP configuration menu. Updates can be made more quickly on one system and then copied to others.

iSeries TCP/IP is designed to protect configuration files, including the host table. You cannot change the host table file unless you use the Configure TCP/IP menu or the MRGTCPTH, ADDTCPHT, RNMTCPTH, CHGTCPTH, or RMVTCPTH commands. However, you can still import and use a host table from a central site by using the MRGTCPTH command.

The following host table file types can be imported and merged with the server host table:

- Host table type **\*AS400**, generated by iSeries TCP/IP Version 3 Release 1 Modification 0 (V3R1M0) or later
- Host table type **\*AIX**, generated by iSeries TCP/IP Version 3 Release 0 Modification .5 (V3R0M5), Version 2 Release 3 (V2R3) or earlier, or many other IBM and non-IBM systems
- Host table type **\*NIC**, host table format used by public domain systems

You can merge or replace the local server host table with the imported host table. The name of the database file containing the local host table is QATOCHOST with member HOSTS in library QUSRSYS. This file is used directly by iSeries TCP/IP; no conversion into an internal version takes place.

### Host File Formats

If you receive a host file and want to use it on your system, the MRGTCPTH (Merge TCP/IP Host Table) command allows you to specify which format you are using. You can use host information files that are in either the \*NIC format, the \*AIX format, or the \*AS400 format. The record length of the imported host table file is not limited.

#### Host Table Information with \*AIX Files

Table 4 shows the \*AIX format supported on the server.

Table 4. \*AIX Supported on the AS/400 System

| Delimiter      | Meaning   |
|----------------|---|
| # (pound sign) | Indicates the beginning of a comment. The text following the pound sign is a comment and is not part of the host table. |
| blank, tab     | Indicates a field delimiter.  |

#### Host Table Information with \*NIC Files

The \*NIC format is often used by hosts in the public domain. A record in a \*NIC file has the following format:

```
HOST : 128.12.19.1 : Host2.lan.ibm.com,Host2 : PC-AT : DOS : TCP/IP
```

This entry describes one host (at address 128.12.19.1) with two names (Host2.lan.ibm.com) and (Host2). The host is an IBM Personal Computer AT<sup>®</sup> computer running MS-DOS and supporting TCP/IP.

A complete description of the \*NIC format is found in Request for Comment (RFC) 952, *Internet Host Table Specification*. See the RFC Editor Site (<http://www.rfc-editor.org/rfc.html>) to retrieve this RFC. The subset supported on the server is shown in Table 5. The \*NIC continuation characters are not supported because the record length of the file can be up to 512 bytes.

Table 5. \*NIC Subset Supported on the AS400 System

| Delimiter  | Meaning  |
|--|--|
| ;(semicolon) <sup>1</sup>  | Indicates the beginning of a comment. The text following the semicolon is a comment and is not part of the host table. |
| NET <sup>2</sup>   | A keyword introducing a network entry.   |
| GATEWAY  | A keyword introducing a gateway entry.   |
| HOST   | A keyword introducing a host entry.  |
| :(colon)   | A field delimiter.   |
| ::(two colons)   | Indicates a null field.  |
| ,(comma)   | A data element delimiter.  |
| <b>Notes:</b> <ol style="list-style-type: none"> <li>1. If any line in the *NIC table contains a semicolon as the first column value, then that line is not merged into the server host table.</li> <li>2. These entries are not merged into the server host table.</li> </ol> |  |

### Host Table Information with \*AS400 Files

The \*AS400 file format is the format of the local server host table file used by iSeries TCP/IP directly. The name of the file is QATOCHOST with member HOSTS in library QUSRSYS. A single record contains an Internet address, up to four host/domain names and a text description field. For more details regarding record and file formats, use the DSPFFD (Display File Field Description) command.

This file can be exchanged between iSeries servers. However, there is no function to convert from \*AS400 to \*AIX or \*NIC format.

## Tips for Merging Host Tables

A maximum of four host names per IP address is allowed when host tables are merged. For example, if the local host table already has three host names and the physical file member to be merged has two additional host names, only the first host name in the physical file is merged into the final host table.

Host names that exist for the same Internet address are not duplicated. If the same host name is found for Internet addresses that are different, then that host name is accepted, but a warning message is displayed.

The original copy of the local host table is not saved by the MRGTCPTH (Merge TCP/IP Host Table) command. To save the original host table, create a copy of the file QUSRSYS/QATOCHOST.HOSTS by using the Copy File (CPYF) command. Do this before issuing the MRGTCPTH command.

## Merging TCP/IP Host Tables

You can use imported host tables in two ways:

- Overwrite the current host table. To do this, specify Replace Host Table (\*Yes) on the Merge Host Table display.

- Merge the information of the imported host table with the information that was entered by using option 10 (Work with TCP/IP host table entries) from the Configure TCP/IP menu. To merge the information, specify Replace Host Table (\*No) on the Merge Host Table display.

You can merge an imported host table with the local host table while TCP/IP is running by using the CFGTCP (Configure TCP/IP) command. The changes take affect the next time a TCP/IP application accesses the host table.

Select option 11 to merge an imported host table with the local server host table.

You can also use the Merge TCP/IP Host Table (MRGTCPTH) command from any command line.

### Example: Successful Host Table Merge

The following example shows the command to merge an imported host table with the local host table.

```
MRGTCPTH FROMFILE(QUSRSYS/M02HOSTS) FILEFMT(*AS400) REPLACE(*NO)
```

File M02HOSTS, member \*FIRST, successfully merged with host table.

### Example: Partly Successful Host Table Merge

The following example shows the command to merge an imported host table with the local host table.

```
MRGTCPTH FROMFILE(QUSRSYS/M03HOSTS) FILEFMT(*AS400) REPLACE(*NO)
```

Duplicate host name SPARKY.SYSNAM123.IBM.COM at address 9.4.6.138  
found host table.  
Duplicate host name MVAX.SYSNAM123.IBM.COM at address 9.4.6.252  
found host table.  
File M03HOSTS, member \*FIRST, merged with host table: however,  
error occurred.

In this example, the host table contains entries with the same host name, which shows in the message as duplicate host names.

## Managing the Host Table from a Central Site

If your network has multiple servers, you can define the TCP/IP host table on one system and share that table with the other systems. This saves you the effort of having to define the host table on each system. To do this, follow these steps:

### Step 1—Create the Host Table on Your Central System

Use the CFGTCP command to configure your host table. Select option 10 (Work with TCP/IP host table entries). Your system's host table is stored in member HOSTS of file QATOCHOST in library QUSRSYS.

### Step 2—Start FTP to a Remote System

For example, if your host table defines the remote system as SYSNAM02, type the FTP command as follows:

```
ftp sysnam02
```

### Step 3—Tell FTP to Send the Host File to the Remote System

Type the following FTP subcommand:

```
put qusrsys/qatochost.hosts qusrsys/m03host.hosts
```

**Note:** Do not use FTP to put the host file directly into file QATOCHOST containing the server host table.

#### Step 4—Merge the File

Type the following FTP subcommand:

```
quote rcmd mrgtcph fromfile(qusrsys/m03host) frommbr(host)
```

---

## IP Routing and Internet Control Message Protocol (ICMP) Redirecting

Internet routing tables usually remain static for long periods. TCP/IP generates routing tables at activation time from configuration data and adjusts the routing tables based on ICMP redirects, SNMP manager requests, dead gateway processing and socket routing requests.

If network interconnections change, routing tables in a particular host may become incorrect. Because gateways exchange routing information periodically to accommodate network changes and to keep their routes up to date, a gateway usually knows better routes than a host. When a gateway detects that a host is using a route that is not optimum, the gateway sends an ICMP redirect message to that host. It also forwards the original datagram on to its destination. Redirect messages are limited to interactions between a gateway and a host on the same network.

If the host that sends the original datagram is an iSeries, it receives the ICMP redirect message from the gateway and uses this information to update its internal routing table. The next datagram is then sent using the more optimum route received from the gateway. You can see the updated routing table by using NETSTAT, option 2. A route created by the ICMP redirect mechanism is recorded in the IP dynamic routing table and remains there as long as an upper level protocol is using it. When the last upper-level protocol user has completed its unit of work using a route created by the ICMP redirect mechanism, the route is then removed from the routing table. When TCP/IP is restarted, this process is repeated.

In Figure 46 on page 55, host A1 in network 2 is an iSeries server that sends a message to host A2 in network 3. The routing table in host A1 indicates that the first hop to host A2 is through gateway G1, which connects networks 1 and 2. When this gateway receives the datagram, it forwards the datagram to gateway G2, which sends it to the host A2. Gateway G1 then sends an ICMP redirect message to host A1 to inform it that a better route to host A2 is to use gateway G2 as the first hop. This information updates the internal routing table in host A1, and the next datagram to host A2 in network 3 is sent to gateway G2 as the first hop. The gateway then sends the datagram to host A2. When the TCP/IP services are stopped, the collected routing information is deleted and host A1 starts the learning process again.

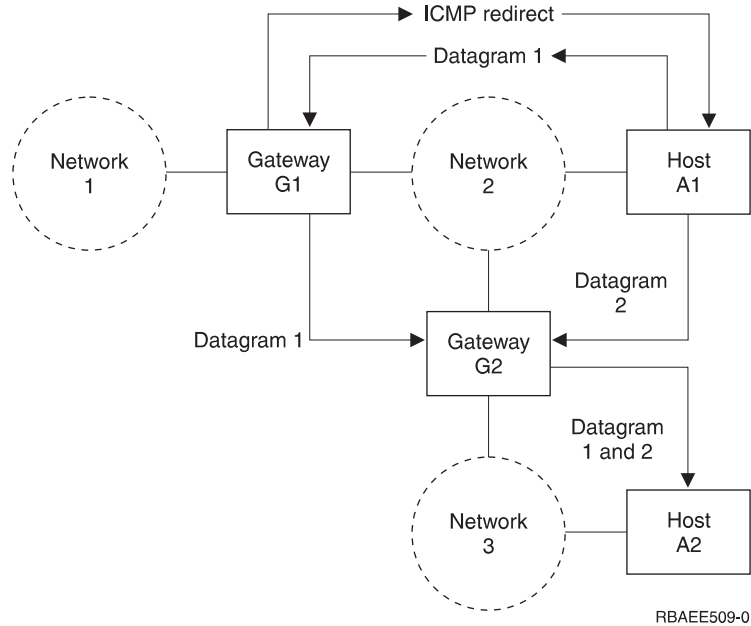


Figure 46. Example of ICMP Redirect

To see routing changes due to ICMP redirect messages, select NETSTAT menu 2 or NETSTAT \*RTE and then press PF11. Comparing the next hop in this display with the next hop present in the routing table, you can verify whether a route has been dynamically changed.

## Dead Gateway Processing

RFC-1122, *Requirements For Internet Hosts - Communication Layers*, requires the IP layer to include a dead gateway algorithm to manage suspected gateway failures. This section is intended to give you an overview of dead gateway processing.

Two types of gateway failures can occur:

- Failure of a first-hop gateway. A first-hop gateway is the gateway that is specified in an IP route. First-hop gateways must be on a directly-connected network. This type of failure can be detected by either TCP or the data link layer.
- Failure of a gateway other than the first-hop gateway. The path between source and destination TCP/IP hosts can traverse multiple gateways. This type of failure can be detected only by TCP.

Dead gateway processing is initiated when IP receives a negative advice indicator from either TCP or the data link layer. These indicators from TCP and the data link layer are referred to as advice since they may result from transient conditions as well as from a serious gateway failure.

## Negative Advice from TCP or the Data Link Layer

Retransmissions on a TCP connection occur as a result of transient or non-transient problems somewhere along the path to a destination host. When TCP notices excessive retransmissions on a TCP connection, a TCP negative advice indicator is sent to IP.

The data link layer passes a negative advice indicator to IP when it is unable to transmit data to a first-hop (directly-connected) gateway. In most cases, negative advice from the data link layer means that the Address Resolution Process (ARP) processing performed by the data link layer was unable to resolve the location of first-hop gateway on the directly connected physical network. (ARP is not performed on all physical network types. Some physical network types, such as X.25, use an alternative scheme for this purpose.)

Negative advice, whether from TCP or the data link layer, is always expressed in terms of the first-hop gateway. Dead gateway processing on a given host only attempts to verify the first-hop gateway. However, gateways also carry out their own dead gateway processing for other adjacent gateways. In this way, all of the gateways along the path to a destination host are taken care of.

## How IP Responds to Negative Advice

When receiving negative advice from TCP or the data link layer concerning a next hop gateway, IP marks all routes that use this gateway as suspect. IP attempts to deliver data destined for the suspect gateway via routes that use other gateways (if any are configured). Next, an IP process is started that uses periodic PING requests to attempt to contact the suspect next-hop gateway. If the suspect gateway continues to be unresponsive for an extended period of time, the frequency of the PING requests is reduced.

When any PING response is received from a suspect gateway, the gateway is considered active and the routes are restored.

### Notes about IP Responses to Negative Advice:

1. If an ICMP redirect message is received during dead gateway processing, routes to a suspect gateway may be temporarily restored. However, dead gateway PING processing is not interrupted, and subsequent negative advice forces the IP routing table back to its previously adjusted state.
2. Responses from user-initiated PINGs can also indicate that a suspect gateway is active.
3. Negative advice is not passed from the UDP or RAW IP protocol machines. Applications using these protocols must use other mechanisms to detect and respond to apparent network problems. However, data link layer-negative advice is still used to manage problems with the first-hop gateway.

---

## Multihoming Function

A multihomed host has multiple IP addresses, which we may think of as logical interfaces. These logical interfaces may be associated with one or more physical interfaces, and these physical interfaces may be connected to the same or different networks.

The iSeries TCP/IP implementation supports multihoming. This allows you to specify either a single interface or multiple interfaces for a line description. You can have your server appear as any one or combination of the following scenarios:

- A single host on a network over a communications line
- Multiple hosts on the same network over the same communications line
- Multiple hosts on the same network over multiple communications lines
- Multiple hosts on different networks over the same communications line
- Multiple hosts on different networks over multiple communications lines

**Note:** The maximum number of interfaces that can be active on a line description at any given time is 128. This is true for all line types (for example, token-ring, Ethernet, frame relay, and so forth).

## Example: A Single Host on a Network over a Communications Line

Your server uses one adapter for TCP/IP to attach to a LAN or WAN network. You add one TCP/IP interface. This TCP/IP interface includes the Internet address of your server. With this single Internet address, your server is part of a single TCP/IP network (Figure 47).

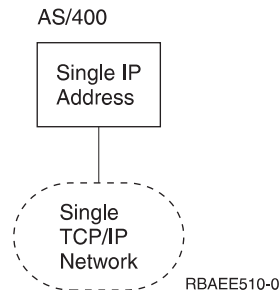


Figure 47. Multihoming - Single Host, Single Network, Single Line

## Example: Multiple Hosts on the Same Network over the Same Communications Line

Your server uses one adapter for TCP/IP to attach to a LAN or WAN network. You add multiple TCP/IP interfaces. Each of these TCP/IP interfaces includes an Internet address of the same TCP/IP network. With these multiple Internet addresses your server appears as multiple hosts in a single TCP/IP network (Figure 48).

This can be a migration scenario.

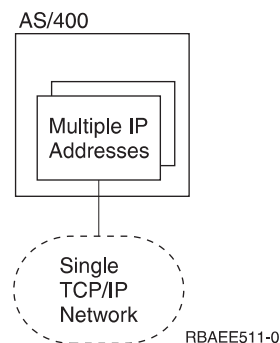


Figure 48. Multihoming - Multiple Hosts, Single Network, Single Line

## Example: Multiple Hosts on the Same Network over Multiple Communications Lines

Your server uses more than one adapter for TCP/IP to attach to the same LAN or WAN network. You add multiple TCP/IP interfaces. At least one interface is assigned to each adapter/line description. Each of these TCP/IP interfaces includes an Internet address of the same TCP/IP networks. With these multiple Internet



addresses, your server appears as multiple TCP/IP hosts in the same TCP/IP network (Figure 49).

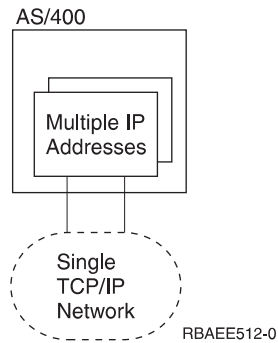


Figure 49. Multihoming - Multiple Hosts, Single Network, Multiple Lines

This scenario can be helpful for backup or to improve performance. However, there is no dynamic backup or performance balance function.

## Example: Multiple Hosts on Different Networks over the Same Communications Line

Your server uses one adapter for TCP/IP to attach to a LAN or WAN network. You add multiple TCP/IP interfaces. Each of these TCP/IP interfaces includes an Internet address of different TCP/IP networks. With these multiple Internet addresses, you participate in different TCP/IP networks (Figure 50).

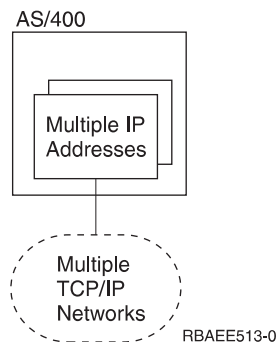


Figure 50. Multihoming - Multiple Hosts, Multiple Networks, Single Line

Imagine a public X.25 network. With this physical network, you can run multiple TCP/IP networks, for example the company intranet, and connections with business partners and service providers. For each of these different TCP/IP networks, your server must configure a unique Internet address.

Running multiple TCP/IP networks within a single local area network (LAN) is also supported. In most situations, however, one designs a single TCP/IP network per physical LAN only.

## Example: Multiple Hosts on Different Networks over Multiple Communications Lines

Your server uses more than one adapter for TCP/IP to attach to multiple LAN or WAN networks. You add multiple TCP/IP interfaces. At least one interface is assigned to each adapter/line description. Each of these TCP/IP interfaces includes



an Internet address of different TCP/IP networks. With these multiple Internet addresses, you take part in different TCP/IP networks (Figure 51).

This example is a combination of all of the previous examples discussed.

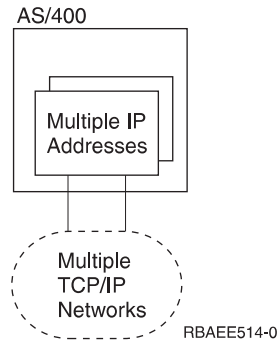


Figure 51. Multihoming - Multiple Hosts, Multiple Networks, Multiple Lines

---

## Example: The Multihoming function

Assume servers SYSNAM02 and SYSNAM03 are connected with a public or private X.25 network. The Internet address of this network is 9.4.73.64.

In this example, the server SYSNAM03 connects with a service provider by using TCP/IP and the same X.25 network attachment (Figure 52). The Internet address assigned by the service provider for the server is 233.1.1.17.

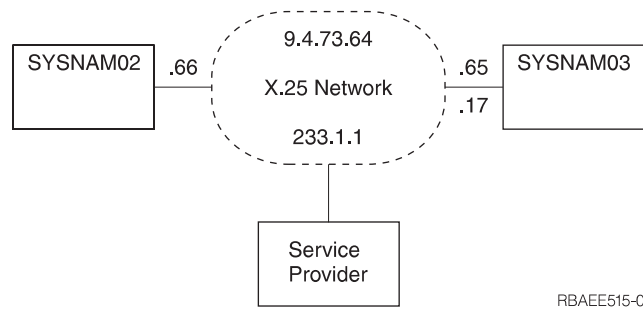


Figure 52. Multihoming TCP/IP Network

The multihoming function supports multiple networks with the same adapter. Server SYSNAM03 must handle two different Internet addresses on the same attachment. To do this, an additional TCP/IP interface needed to be specified (Figure 53 on page 60).

```

Work with TCP/IP Interfaces
System:  SYSNAM03
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display  9=Start  10=End

  Internet      Subnet      Line      Line
  Opt  Address      Mask      Description  Type
  ---  -----
  ---  9.4.73.65      255.255.255.192  X25LINE      *X25
  ---  127.0.0.1      255.0.0.0      *LOOPBACK     *NONE
  ---  223.1.1.17     255.255.255.0  X25LINE      *X25

F3=Exit      F5=Refresh  F6=Print list  F11=Display interface status
F12=Cancel   F17=Top     F18=Bottom

```

Figure 53. Work with TCP/IP Interfaces Display, Multihoming

## Type of Service (TOS)

Type of Service (TOS) is a parameter defined to indicate a quality of the service desired by an application program. It is specified within a single octet of the IP datagram header, and it is used to select Internet service. It denotes how the Internet hosts and routers should make trade-offs between throughput, delay, reliability, and cost.

TOS is used to identify and select the actual transmission characteristics for a particular network, the interface, and the route to be used when routing an Internet datagram. The TOS values are mapped into the actual TOS value of the particular network a datagram is going through. All of the values are mutually exclusive.

The TOS values are defined through the Add TCP/IP Interface (ADDTCPIFC) and Add TCP/IP Route (ADDTCPRTE) commands. The possible selections are as follows:

### \*NORMAL

Normal service is used for delivery of datagrams.

### \*MINDELAY

Minimize delay means that prompt delivery is important for datagrams with this indication.

### \*MAXTHRPUT

Maximize throughput means that high data rate is important for datagrams with this indication.

### \*MAXRLB

Maximize reliability means that a higher level of effort to ensure delivery is important for datagrams with this indication.

### \*MINCOST

Minimize monetary cost means that lower cost is important for datagrams with this indication.

The following table shows which type of services your server uses for some of the TCP/IP applications:

Table 6. AS/400 TCP/IP applications and Type of Services

| Protocol or Application  | Type of Service Used |
|--------------------------|----------------------|
| TELNET                   | Normal               |
| FTP (control connection) | Minimize delay       |
| FTP (data connection)    | Maximize throughput  |
| SMTP (command phase)     | Minimize delay       |
| SMTP (data phase)        | Maximize throughput  |
| POP (all phases)         | Maximize throughput  |
| SNMP                     | Maximize reliability |

Thus, TOS is a suggestion, not a demand, to the interface (if more than one is present in the system) and to the routing algorithms. If a TCP/IP subsystem knows more than one interface and more than one possible route to a given destination, it uses the TOS to select one with characteristics closest to that desired.

### TOS Example

For example, suppose the system can select between a low-capacity nonswitched line or a high-bandwidth (but high delay) satellite connection:

- Datagrams carrying keystrokes from a user to a remote computer could have the type of service set to \*MINDELAY, requesting that they be delivered as quickly as possible.
- Datagrams carrying a bulk file transfer could have the type of service set to \*MAXTHRPUT, requesting that they travel across the high-capacity satellite path.

It is up to the network administrator to define TOS values when defining interfaces and routes in the TCP/IP configuration. Based on the administrator's knowledge of the hardware technologies available on systems and networks used, TOS values for the routes must also be defined according to the interface's TOS value. This means that if a \*MINDELAY value is defined in the interface definition, at least one route definition must have the \*MINDELAY TOS value defined.

**Note:** A TCP/IP network does not guarantee the TOS requested. However, datagram transmission is never denied.

## Multiple Routes

You can have multiple routes in your routing table (by using the ADDTCPRTE command). You can have more than one route for the same destination Internet address with the same type of service or a different type of service. If you have multiple routes with the same types of service, they are used in the order specified. If a particular next hop router is not available, the subsequent specified next hop router is used. This continues until an entry that is active is found or the list of next hop values is exhausted. If you have multiple routes with different TOS, the one with the TOS equal to the one requested by applications with TOS octet in IP datagram is used. If no match is found in any specified routes, the route with the closest TOS or \*NORMAL TOS is used.

You can have \*DFTRROUTE, and specific route destination addresses. Default routes are used only when data is sent to a remote destination system that does not have

a specific route defined. The system allows up to eight default routes, but each route must have a unique next hop value.

An example of a multiple route table can be found in Figure 54.

```

Work with TCP/IP Routes
System:  SYSNAM003
Type options, press Enter.
  1=Add  2=Change  4=Remove  5=Display

Opt      Route      Subnet      Next      Preferred
Destination  Mask        Hop        Interface
-----
-      *DFTRROUTE  *NONE      9.4.73.193  *NONE
-      *DFTRROUTE  *NONE      9.4.73.197  *NONE
-      *DFTRROUTE  *NONE      9.4.73.196  *NONE
-      9.4.70.0    255.255.255.0  9.4.73.194  *NONE
-      9.4.70.0    255.255.255.0  9.4.73.195  *NONE
-      9.4.70.0    255.255.255.0  9.4.73.198  *NONE

F3=Exit  F5=Refresh  F6=Print list      F10=Work with IP over SNA routes
F11= Display type of service  F12=Cancel  F17=Top  F18=Bottom
Bottom

```

Figure 54. Work with TCP/IP Routes Display

## TCP/IP Port Restriction

TCP and UDP protocols use **ports** to identify a unique origin or destination of communication with an application. Each port is assigned a small integer. You can configure port information if you want to restrict the use of a TCP or UDP port to one or more user IDs.

The range of port numbers is from 1 to 65535. However, ports 0-1023 are reserved as well-known port numbers, which are controlled and assigned by the Internet Assigned Numbers Authority (IANA). Only those applications that have been assigned one of these ports should use a number within this range. Refer to the current Assigned Numbers RFC for a list of the port assignments.

Because this range of port numbers, 0-1023, is reserved for the well-known ports, they should not be used by user application programs because it could affect the operation of TCP/IP. For example, restricting the use of ports 21, 23, or 25, prevents other users from using FTP, TELNET, or SMTP, respectively.

The iSeries Add TCP/IP Port Restriction (ADDTCPPORT) command allows you to restrict usage of a single port or a range of ports to a particular iSeries user profile.

Restricting ports is like allocating ports to a specific user profile. When a socket application issues the bind() system call, or when a TCP/UDP Pascal API application issues a call to the TcpOpen, TcpWaitOpen, or UdpOpen function, the job's user profile is checked against the list of user profiles that are associated with

the specified port. If no match is found, the requesting program is not allowed to use the specified port. If any port in the 1-1023 range is restricted, the following message is posted:

```
Port restriction added but may affect TCP/IP processing
```

If no user profiles are associated with a specific port, there are no restrictions.

It is not necessary to configure port restrictions unless you are writing your own TCP/IP applications and you want to reserve the use of the applications to certain user profiles.

**Note:** For an installation in which user-written programs use ports other than the well-known ports, you can consider restricting the use of the well-known ports to the user profiles running the server application. As an example, for File Transfer Protocol (FTP), this would be user profile QTCP.

## Configuring TCP/IP Port Restrictions

To configure TCP/IP port restrictions, type option 4 on the Configure TCP/IP menu. The Work with TCP/IP Port Restrictions display is shown (Figure 55).

```
Work with TCP/IP Port Restrictions                               System:  SYSNAM03
Type options, press Enter.
 1=Add  4=Remove

Opt      --Port Range---
         Lower   Upper   Protocol   User
         -----   -----   -----   -----
         1050    1059    *TCP      PAOLO

F3=Exit  F5=Refresh  F6=Print list  F12=Cancel  F17=Top  F18=Bottom
```

Figure 55. Work with TCP/IP Port Restrictions Display

Type option 1 (Add) at the input-capable top list entry to get to the Add TCP/IP Port Entry (ADDTCPPORT) display shown in Figure 56 on page 64. You can go directly to this display by typing ADDTCPPORT on any command line and pressing F4.

```

Add TCP/IP Port Restriction (ADDTCPPORT)

Type choices, press Enter.

Range of port values:
  Lower value . . . . . 1060          1-65535
  Upper value . . . . . > *ONLY      1-65535, *ONLY
  Protocol . . . . . *tcp             *UDP, *TCP
  User profile . . . . . gerry        Character value

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

```

Figure 56. Add TCP/IP Port Restriction Display

Let us assume we have an application that uses Port 1060 in the TCP layer and we want to restrict its use to user profile GERRY. Type the information as shown in Figure 56.

Figure 57 shows what the display looks like after you enter port information for both user profiles PAOLO and GERRY.

Changes to the port restrictions take effect immediately. However, applications that are already active are not affected until they are restarted.

```

Work with TCP/IP Port Restrictions
System:  SYSNAM03

Type options, press Enter.
  1=Add  4=Remove

Opt  --Port Range---  Protocol  User Profile
     Lower  Upper
-----
-    1050   1059    *TCP      PAOLO
     1060   *ONLY    *TCP      GERRY

Bottom
F3=Exit  F5=Refresh  F6=Print list  F12=Cancel  F17=Top  F18=Bottom

```

Figure 57. Work with TCP/IP Port Restrictions Display

---

## Related Tables and the Host Table

Socket applications require a set of tables from which they can retrieve specific TCP/IP network data when needed. These are as follows:

- Host table
- Service table
- Protocol table
- Network table

The host table contains a list of host names and corresponding Internet addresses. Socket applications requesting host data obtain it either from the server host database file or from the domain name server.

The service table contains a list of services and the specific port and protocol a services uses. The protocol table contains a list of protocols used in the TCP/IP network. The network table contains a list of networks and the corresponding Internet addresses.

UNIX\*\* systems traditionally store this information in the following files:

- /etc/hosts - host table
- /etc/protocols - protocol table
- /etc/services - service table
- /etc/networks - network table

iSeries TCP/IP maintains the service, protocol, and network tables as database files. iSeries TCP/IP refers to these three tables as related tables. To configure or view the protocol, services, or network tables, select option 21 (Configure Related Tables) on the Configure TCP/IP menu. You are shown the display in Figure 58.

```
Configure Related Tables                               System:  SYSNAM03

Select one of the following:

  1. Work with service table entry
  2. Work with protocol table entry
  3. Work with network table entry

Selection or command
===> _____
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
```

Figure 58. Configure Related Tables Menu

You can change the services, protocols, and network files using the options from this display.

The services table stores the mapping of services to ports or ports to services as shown in Figure 59. The mapping information is usually accessed with the `getservbyname()` and `getservbyport()` socket functions.

```

Work with Service Table Entry
System:  SYSNAM03
Type options, press Enter.
  1=Add  4=Remove  5=Display

Opt  Service                Port  Protocol
-----
     echo                    7    udp
     finger                  79    tcp
     finger                  79    udp
     ftp-control             21    tcp
     ftp-control             21    udp
     ftp-data                 20    tcp
     ftp-data                 20    udp
     gopher                  70    tcp
     gopher                  70    udp
     graphics                41    tcp
     graphics                41    udp
     pop3                    110   tcp
                                     More...

Parameters for options 1 and 4 or command
===>
F3=Exit  F4=Prompt  F5=Refresh  F6=Print list  F9=Retrieve  F12=Can
F17=Top  F18=Bottom

```

Figure 59. Work with Service Table Entry Display

The protocol table stores the mapping of protocol names to protocol numbers and protocol numbers to protocol names. Socket applications use `getprotobyname()` and `getprotobynumber()` functions to access this table (Figure 60).

```

Work with Protocol Table Entry
System:  SYSNAM03
Type options, press Enter.
  1=Add  4=Remove  5=Display

Opt  Protocol                Protocol
-----
     icmp                    1
     ip                      0
     tcp                     6
     udp                     17

                                     Bottom

Parameters for options 1 and 4 or command
===>
F3=Exit  F4=Prompt  F5=Refresh  F6=Print list  F9=Retrieve  F12=Cancel
F17=Top  F18=Bottom

```

Figure 60. Work with Protocol Table Entry Display



The network table contains the networks and the Internet address associated with the network. Socket applications use the `getnetbyname()` and `getnetbyaddr()` functions to access the information in the network table (Figure 61).

```

Work with Network Table Entry
System:  SYSNAM03
Type options, press Enter.
  1=Add  4=Remove  5=Display

Opt      Network      Internet
-----  -
-        IBM          9.0.0.0

Parameters for options 1 and 4 or command
===>
F3=Exit  F4=Prompt  F5=Refresh  F6=Print list  F9=Retrieve  F12=Cancel
F17=Top  F18=Bottom
Bottom

```

Figure 61. Work with Network Table Entry Display

The protocols and services tables that are shipped contain standard information. The network tables do not contain any information. The network IBM information has been added in Figure 61, as an example.

For additional information about sockets, refer to *Socket Programming* (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzab6/rzab6soxoverview.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

## Using X.25 PVC instead of SVC

In “Step 5—Configuring TCP/IP Remote System Information (X.25)” on page 16 you were shown how to define the X.25 network address of each system that uses a switched virtual circuit (SVC).

To replace the X.25 SVC with an X.25 permanent virtual circuit (PVC) connection, the example below is helpful. The following CL commands will look different: `CRTLINX25`, `ADDTCPIFC`, and `ADDTCPRSI`.

Use the same X.25 line description, but replace the first of the four SVCs with a PVC.

```

CRTLINX25 LIND(X25LINE) RSRNAME(LIN051)
LGLCHLE((001 *PVC) (002 *SVCBOTH)
(003 *SVCBOTH) (004 *SVCBOTH))
NETADR(40030003) CNNINIT(*LOCAL)
TEXT('ITSO X.25 Network')

```

The TCP/IP interface now points to a specific PVC instead of a pool of SVCs.

```
ADDTCPIFC INTNETADR('9.4.73.65') LIND(X25LINE)
SUBNETMASK('255.255.255.192') PVCLGLCHLI(001)
MAXSVC(0)
```

The TCP/IP remote system information no longer includes the X.25 address to be called. Instead, the entry points to the PVC channel ID.

```
ADDTCPRSI INTNETADR('9.4.73.66')
PVCLGLCHLI(001)
```

---

## IP Multicasting

IP multicasting is the process of transmitting an IP datagram to a host group. The hosts that are in the group may reside on a single subnet or on different subnets that are connected by multicast-capable routers. Hosts may join and leave groups at any time. There are no restrictions on the location or number of members in a host group. For more information about IP multicasting, refer to RFC 1112, *Host Extensions for IP Multicasting* in the RFC Editor Site (<http://www.rfc-editor.org/rfc.html>).

**Note:** The server cannot act as a multicast-capable router.

### Multicast Application Programming Information

An application program can send or receive multicast datagrams by using the Sockets API and connectionless, SOCK\_DGRAM type sockets. Multicasting is a one-to-many transmission method. You cannot use connection-oriented sockets of type SOCK\_STREAM for multicasting. When a socket of type SOCK\_DGRAM is created, an application can use the setsockopt() function to control the multicast characteristics associated with that socket. The setsockopt() function accepts the following IPPROTO\_IP level flags:

- IP\_ADD\_MEMBERSHIP: Joins the multicast group specified.
- IP\_DROP\_MEMBERSHIP: Leaves the multicast group specified.
- IP\_MULTICAST\_IF: Sets the interface over which outgoing multicast datagrams should be sent.
- IP\_MULTICAST\_TTL: Sets the time to live (TTL) in the IP header for outgoing multicast datagrams.
- IP\_MULTICAST\_LOOP: Specifies whether or not a copy of an outgoing multicast datagram should be delivered to the sending host as long as it is a member of the multicast group.

For additional information about sockets, including sample programs, see Sockets Programming (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzab6/rzab6soxoverview.htm>) in the Information Center. The System API Reference (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/apis/api.htm>) documents the sockets API. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

### Multicast Restrictions

Multicast does not map well to all types of physical lines. For this reason, it is not supported on all lines. For example, a switched network such as X.25 does not lend itself to multicast applications because no mechanism exists for transmitting a single packet to all systems in the network that have joined a group. IP multicast is supported on broadcast capable networks and on SLIP/PPP interfaces, but it is not

supported on multi-access nonbroadcast networks. IP multicast is also not currently supported on Frame Relay, FDDI/SDDI, or ATM networks. To determine whether an interface supports multicast, enter option 14 on the Work with TCP/IP Interface Status display. If the interface supports multicast, there will be at least one Host Group entry for the All Hosts group 224.0.0.1. Otherwise, the interface does not support multicast.

The 2626 token-ring input-output processor (IOP) requires manual configuration to receive multicast datagrams. In particular, you must specify the token-ring address, C00000040000, on the functional address parameter for the token-ring line description. To add this address to a line description that is named TRNLINE, use the following command:

```
CHGLINTRN LIND(TRNLINE) FCNADR(C00000040000)
```

The 2617 Ethernet IOP also requires manual configuration in order to receive multicast datagrams. The Ethernet group addresses to be received need to be specified on the group address parameter (GRPADR) for the Ethernet line description. A 4-byte IP multicast address is mapped to a 6-byte Ethernet group address by placing the low-order 23 bits of the IP multicast address into the low-order 23 bits of the Ethernet group address 01005E000000. For example, to receive multicast datagrams with a destination address of 224.255.0.2, the GRPADR parameter for the 2617 Ethernet line description must include 01005E7F0002.



---

## Chapter 3. TCP/IP Performance

The following are performance items that should be considered when using TCP/IP.

---

### \*BASE Pool Size

The TCP/IP protocol and application code always runs in the \*BASE pool on the iSeries 400 server. If the \*BASE pool is not given enough storage, TCP/IP performance, especially SMTP performance, can be adversely affected.

Although it is possible to run in less than 4000 KB of storage to perform well when running both FTP and SMTP sessions, it is suggested that the \*BASE pool be configured to use at least 4000 KB of storage. You can use the WRKSYSSTS to view and change pool sizes on the server. Pool 2 is the base pool. Another alternative is to change the pool in which the TCP/IP jobs run.

---

### TCP/IP Jobs

TCP/IP jobs, like other jobs on your system, are created from job descriptions and associated classes. The job descriptions and classes should be adequate in most cases; however, they may be changed to fit your configuration. The TCP/IP job descriptions, classes, and subsystem descriptions can be found in the QTCP or the QSYS library that was loaded in your system when TCP/IP was installed.

Each application has a job description associated with it. This job description has a number of items associated with it that define how the application runs on the server. One of these pieces of information is the routing entry compare value. This value identifies which routing entry in a subsystem description is used when this job is submitted. By changing that routing entry, you can select in which storage pool to run the jobs for a particular application. For information on compare values, see Work Management (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzaks/rzaks1.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

Other items that can be changed or selected on a job description include the job priority, the logging level for messages, and the initial library list.

If the storage pool that you select to run the TCP/IP application jobs in is not large enough, excessive paging can occur. This directly affects performance on the server and the performance of the applications.

---

### TCP/IP Protocol Support Provided by IOP

iSeries TCP/IP protocol support runs down in the AS/400 System Licensed Internal Code, at the same level as LU 6.2 and APPN\*. One of the goals of integrating TCP/IP into the AS/400 System Licensed Internal Code is to provide performance and capacity comparable to APPC.

Further, moving some functions that are normally done by the TCP/IP software into the IOP reduces interactions between the system and the input/output processor (input-output processor (IOP)). These functions may include:

- Checksum calculation of outgoing TCP and UDP datagrams (prior to V4R4)
- Checksum verification of incoming TCP and UDP datagrams (prior to V4R4)
- Outbound batching of TCP and UDP datagrams.
- Fragmentation of TCP and UDP datagrams into segments that match the MTU size.
- Starting with V4R2, iSeries collects all TCP datagrams in one batch and UDP datagrams in a second batch. Ports and IP addresses are ignored. Releases prior to V4R2 batch together datagrams at the IOP when these conditions are true:
  - The protocol (TCP or UDP) matches
  - The source and destination ports match
  - The source IP address and destination IP address match
  - They arrive consecutively into the IOP

The IOP then passes the datagram batch to IP.

- Handling of IP and ICMP datagrams in error (unless IP NAT, which disables this function, is active)
- Resolving physical addresses using ARP protocol

These functions are called *TCP/IP-assist functions*. Whether these functions are done by the IOP or the System Licensed Internal Code (SLIC), depends on the IOP type, the OS/400 release, and the TCP/IP configuration. For details about specific functions, contact your local service representative. TCP/IP-assist functions are available on these IOPs:

- #2617 Ethernet/IEEE 802.3 adapter/HP
- #2619 16/4 Mbps Token-Ring Network adapter/HP
- #2618 Fiber distributed data interface adapter (FDDI)
- #2665 Shielded distributed data interface adapter (SDDI)
- #2666 High-speed communication adapter that is running frame relay only
- #2668 iSeries wireless LAN adapter

**Note:** You can get the same function without using one of the above IOP adapters (done instead at a higher level in the system (SLIC)). When you use the X.25 protocol, you do not gain the advantage of the TCP/IP-assist function.

The *TCP/IP-assist functions* are also available on the following LAN IOAs and ATM IOAs:

- #2723 PCI Ethernet IOA
- #2724 PCI Token-Ring IOA
- #2838 PCI 100/10 Mbps Ethernet IOA
- #6149 16/4 Mbps Token-Ring IOA
- #2811 PCI 25 Mbps UTP ATM IOA
- #2812 PCI 45 Mbps Coax T3/DS3 ATM IOA
- #2813 PCI 155 Mbps MMF ATM IOA
- #2814 PCI 100 Mbps MMF ATM IOA
- #2815 PCI 155 Mbps UTP 0C3 ATM IOA
- #2816 PCI 155 Mbps MMF ATM IOA
- #2818 PCI 155 Mbps SMF 0C3 IOA
- #2819 PCI 34 Mbps Coax E3 ATM IOA

**Note:** If you configure your 100 Mbps ethernet line for TCPONLY, all IOP assist functions are disabled.

TCP/IP-assist functions that are available on frame relay IOAs are:

- #2699 Two-Line WAN IOA
- #2720 PCI WAN/Twinaxial IOA
- #2721 PCI Two-Line WAN IOA

Communications restrictions apply if any of the following communication functions are required when using the frame relay IOAs, as listed above:

- X.25, Frame Relay, or IPX Protocol
- SDLC protocol, if used to connect to more than 64 remote sites
- Communications line speeds greater than 64 Kbps and up to 2.048 Mbps for the synchronous data link control (SDLC) or frame relay protocols (bisync is always limited to a maximum of 64 Kbps)
- Communications line speeds greater than 64 Kbps and up to 640Kbps for X.25

---

## Merge Host Table Performance

You can use the following data to help you plan for and anticipate performance when merging host tables. The data represents averages of measurements that are taken. The actual time required on your server will be different.

Three cases were measured:

- Small merge—merge a 250-record file into the local host table that currently has 50 entries
- Medium merge—merge a 2000-record file into the local host table that currently has 50 entries
- Large merge—merge a 5000-record file into the local host table that currently has 50 entries.

The results of this test are shown in Table 7.

*Table 7. Merge Host Table Performance*

| Number of records merged | Record format | Elapsed time (min:sec) | CPU percent |
|--------------------------|---------------|------------------------|-------------|
| 250                      | *AIX          | 0:42                   | 43.7        |
| 2000                     | *NIC          | 5:38                   | 49.4        |
| 5000                     | *NIC          | 13:54                  | 48.6        |

This data equates to about 6 records per second and about .07-.08 processing unit seconds per record.

---

## Running TCP/IP Only: Performance Considerations

Certain configurations of 2838 - 10/100 Mbps Ethernet cards allow you to run the IOP with only TCP/IP instead of all protocols for better performance. You need a 2838 Ethernet card with either:

- 2810 IOP
- 2809 IOP (the 2838 must be the only input/output adapter (IOA)IOA on the IOP)

| If you have one of these configurations, you can use the TCPONLY parameter  
| when you create or change your Ethernet line descriptions. Setting TCPONLY to  
| \*YES in other hardware configurations has no effect on the line.



## Appendix A. Configuring a Physical Line for TCP/IP Communication

On the iSeries 400, communication occurs through objects called lines, controllers, and devices. The communications objects for iSeries TCP/IP are the line descriptions, the network controller descriptions, and the network device descriptions.

TCP/IP communicates over a variety of physical line types and network interfaces (NWI). The command that defines the characteristics of the physical line connection or network interface depends on the type of communications adapter, as shown in Table 8.

Table 8. Line Types and Network Interfaces Supported by TCP/IP

| Line type  | Configuration command  |
|--|--|
| Asynchronous   | Create Line Description (Async) (CRTLINASC) See Link Configuration ( <a href="http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzaiy/rzaiylinkline.htm">http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzaiy/rzaiylinkline.htm</a> ) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information. |
| DDI  | Create Line Description (DDI Network) (CRTLINDDI)  |
| Ethernet   | Create Line Description (Ethernet) (CRTLINETH)   |
| Frame relay  | Create Line Description (Frame Relay Network) (CRTLINFR)   |
| Frame relay NWI using a frame relay, token ring, Ethernet, or DDI line description | The frame relay NWI is created using the Create Network Interface Frame Relay Network (CRTNWIFR) command.<br><br>The line description is created using the appropriate Create Line Description command and attached to the frame relay NWI by specifying the NWI and NWIDLCI parameters.   |
| ISDN NWI using an X.25 line description  | The ISDN NWI is created using the Create Network Interface ISDN (CRTNWIISDN) command.<br><br>The X.25 line is created using the Create Line X.25 (CRTLINX25) command and attached to the ISDN NWI by specifying the NWI, NWICHLTYPE, NWICHLNBR, and SWTNWILST parameters.  |
| Point-to-Point   | Create Line Description (PPP) (CRTLINPPP) See Link Configuration ( <a href="http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzaiy/rzaiylinkline.htm">http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rzaiy/rzaiylinkline.htm</a> ) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.   |
| Token-ring   | Create Line Description (Token-Ring Network) (CRTLINTRN)   |
| Twinax   | Create Line Description (TDLC) (CRTLINTDLC)  |
| Wireless   | Create Line Description (Wireless Network) (CRTLINWLS)   |
| X.25   | Create Line Description (X.25) (CRTLINX25)   |

You can describe the characteristics of the communications controllers by using the *Create Controller Description (Network)* (CRTCTLNET) command or by letting the system create the controller automatically when you activate TCP/IP. You only need one network controller to describe all the systems with which you communicate over any given line description.

You can describe the characteristics of the communications devices using the by *Create Device Description (Network)* (CRTDEVNET) command or by letting the system create the device automatically when you activate TCP/IP.

If you want to change controller or device descriptions, use the *Change Controller Description (Network)* (CHGCTLNET) and *Change Device Description (Network)* (CHGDEVNET) commands. For more information on changing controller or device descriptions, see *Control Languages* (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rbam6/rbam6clmain.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

---

## Configuration Steps

To connect any of the communications adapters listed in Table 8 on page 75 to the network, perform the following steps:

1. Create a line description (see “Creating the Line Description”).
2. Set the line description maximum frame size or SSAP maximum frame size. You must consider this value when setting the maximum transmission unit (MTU) of the TCP/IP interface (see “Setting the Maximum Transmission Unit” on page 77). This is not a required step because there are default MTU values for all line types.

### Creating the Line Description

If you have already configured a physical line, this existing line can be shared between TCP/IP data and data from other protocols like SNA or OSI at the same time. There is no need for a separate physical line to support TCP/IP. If a line description does not exist for a physical IOP, you must create a new one. Use one of the commands mentioned in Table 8 on page 75 to create a line description or network interface appropriate for your communications adapter. For more information on creating line descriptions, see *LAN, Frame-Relay and ATM Support*, *X.25 Network Support*, and *Communications Configuration*. Pay particular attention to the following items when creating or changing a line description for TCP/IP communications:

- Line description name.
- Source Service Access Point (SSAP).

#### Line Description Name

You need the name of the line description when you configure TCP/IP on your system (see “Step 1—Configuring a Line Description” on page 10). Remember the name you choose when you create the line description, or use the *Work with Configuration Status* (WRKCFGSTS) command to find the name of an existing line.

#### Source Service Access Point

If the line type supports source service access points (SSAP), you must specify X'AA' as entries in the SSAP list. SSAP examples include Token-ring, Ethernet IEEE802.3, DDI, and wireless. This occurs by default when you create a new line description and leave the SSAP parameter at its default value of \*SYSGEN. If you have an existing line description, use the appropriate change line description command and add X'AA' to the SSAP list.

If the Ethernet standard prompt value is \*ALL or IEEE8023, then you must specify X'AA' as entries in the SSAP list. This occurs by default when you create a new line description and leave the SSAP parameter at its default value of \*SYSGEN.

If the Ethernet standard prompt is \*ETHV2, the system sends and receives all TCP/IP data in Ethernet Version 2 frames. You do not need to configure any additional SSAPs for TCP/IP.

## Setting the Maximum Transmission Unit

The maximum transmission unit (MTU) parameter that you can enter on the *Add TCP/IP Interface* (ADDTCPIFC) command, *Add TCP/IP Route* (ADDTCPRTE) command, *Change TCP/IP Interface* (CHGTCPIFC) command, or *Change TCP/IP Route* (CHGTCPRTE) command depends on the type of line that you use. The following is a list of the maximum MTU values that you can specify, based on the line type:

|                      |       |
|----------------------|-------|
| Asynchronous (SLIP)  | 1006  |
| DDI                  | 4352  |
| Ethernet 802.3       | 1492  |
| Ethernet Version 2   | 1500  |
| Frame relay          | 8177  |
| Point-to-Point (PPP) | 4096  |
| Token ring (4 meg)   | 4060  |
| Token ring (16 meg)  | 16388 |
| Wireless 802.3       | 1492  |
| Wireless Version 2   | 1500  |
| X.25                 | 4096  |

### Notes:

1. TCP/IP processing uses a small part of each datagram. Therefore, the whole datagram size is unavailable for user data.
2. The value of the maximum transmission unit used by TCP/IP processing depends on the value that you specify for the route on the MTU parameter of the route or interface commands mentioned previously. It also depends on the type of physical line that you use, the maximum frame size of the network line, and the SSAP maximum frame size.

## Determining the Maximum Size of Datagrams

For a communications line, specify the maximum frame size on the appropriate *Create Line Description* command. The maximum frame size is compared to the MTU value of the route or interface. TCP/IP uses the lesser of these two values to determine the maximum size of datagrams that it sends by over this line.

For example, if you specify 1024 for the MTU parameter for a route attached to a communications line and the line description contained a value of 512 for a maximum frame size, the maximum datagram size value for the route that TCP/IP uses is 512. If the line is varied *off* and you change the maximum frame size on the Token-ring line description to 1994, and then the line is varied *on*, the maximum transmission unit used for the route is reset to 1024 when the next TCP/IP operation occurs that causes a datagram to be sent.



---

## Appendix B. TCP/IP Application Exit Points and Programs

Certain TCP/IP applications provide exit points that enable them to call customer-written exit programs. This appendix contains the following information:

- Conceptual information on TCP/IP exit points and programs
- General instructions on creating exit programs for TCP/IP applications
- Descriptions of the TCP/IP application exit point interfaces
- Specific instructions on how to prepare exit programs for each TCP/IP application exit point, with examples.

---

### TCP/IP Exit Points and Exit Programs

An **exit point** is a specific point in the TCP/IP application program where control may be passed to an exit program. An **exit program** is a program to which the exit point passes control.

For each exit point, there is an associated programming interface, called an **exit point interface**. The exit point uses this interface to pass information between the TCP/IP application and the exit program. Each exit point has a unique name. Each exit point interface has an **exit point format name** that defines how information is passed between the TCP/IP application and the customer-written exit program.

Different exit points may share the same exit point interface. When this is the case, multiple exit points can call a single exit program.

Figure 62 shows how parameters and control are passed from the TCP/IP application program to the customer-written exit program and back again.

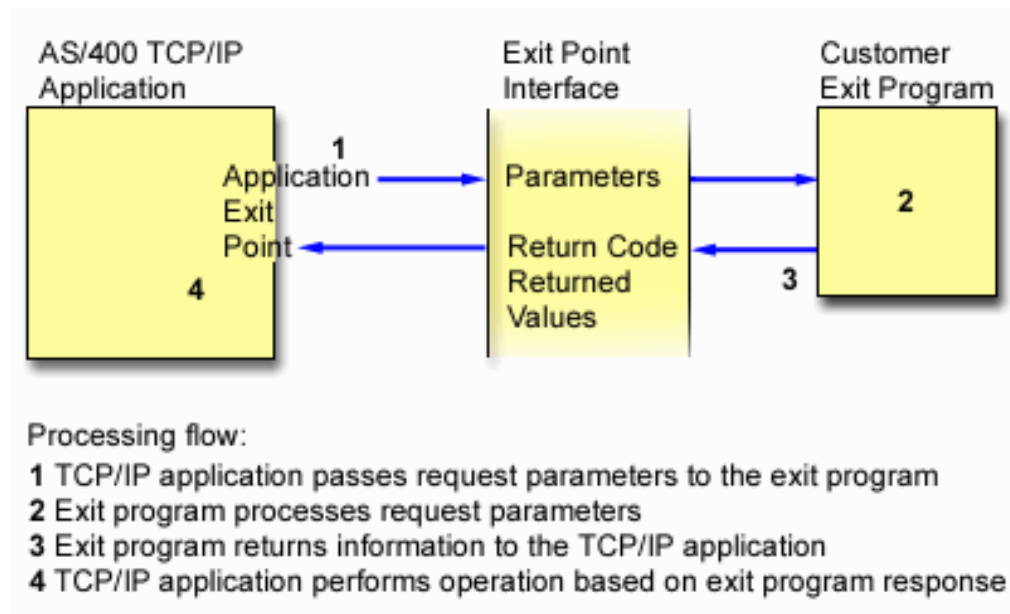


Figure 62. TCP/IP Exit Point Processing

## OS/400 Registration Facility

Exit points for TCP/IP applications are automatically registered when the parent product or option is installed, using the OS/400 **registration facility**. The registration facility contains a repository that allows customers to associate their exit programs with specific exit points. TCP/IP applications check the registration facility repository to determine which exit program to call for a particular exit point.

You must add your exit program to an exit point in the registration repository before a TCP/IP application can call it. Adding the exit program to the repository associates the exit program with a specific exit point.

For security exit programs, the TCP/IP application will typically request the exit program to indicate if a specified operation should be allowed. When no exit program has been added to an exit point, the TCP/IP application assumes that no additional security controls are to be applied.

You can use the Work with Registration Information (WRKREGINF) command to display a list of the exit points in the OS/400 registration facility. Use this list to display information about an exit point or to work with exit programs associated with an exit point. The Work with Registration Information display is shown in Figure 63 on page 82.

## TCP/IP Application Exit Points

The following table lists the exit points provided for each TCP/IP application.

**Note:** If using Distributed Data Management (DDM), see the DDMACC parameter on CHGNETACMD in Control Languages (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/rbam6/rbam6clmain.htm>) for more information. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

Table 9. TCP/IP Application Exit Points

| TCP/IP Application               | Exit Point           | Exit Point Format                   |
|----------------------------------|----------------------|-------------------------------------|
| FTP Client                       | QIBM_QTMF_CLIENT_REQ | VLRQ0100 <sup>1</sup> (see page 85) |
| FTP Server                       | QIBM_QTMF_SERVER_REQ | VLRQ0100 <sup>1</sup> (see page 85) |
| FTP Server                       | QIBM_QTMF_SVR_LOGON  | TCPL0100 <sup>2</sup> or TCP0200    |
| REXEC Server                     | QIBM_QTMX_SERVER_REQ | VLRQ0100 <sup>1</sup> (see page 85) |
| REXEC Server                     | QIBM_QTMF_SVR_LOGON  | TCPL0100 <sup>2</sup>               |
| REXEC Server                     | QIBM_QTMF_SVR_SELECT | RXCS0100 (see page 89)              |
| TFTP Server                      | QIBM_QTOD_SERVER_REQ | VLRQ0100 <sup>1</sup> (see page 85) |
| Workstation gateway (WSG) server | QIBM_QTMT_WSG        | QAPP0100                            |
| DHCP Server                      | QIBM_QTOD_DHCP_REQ   | DHCV0100 <sup>3</sup>               |
| DHCP Server                      | QIBM_QTOD_DHCP_ABND  | DHCA0100 <sup>3</sup>               |
| DHCP Server                      | QIBM_QTOD_DHCP_ARLS  | DHCR0100 <sup>3</sup>               |
| TELNET Server                    | QIBM_QTG_DEVINIT     | INIT0100                            |
| TELNET Server                    | QIBM_QTG_DEVTERM     | TERM0100                            |

Table 9. TCP/IP Application Exit Points (continued)

| TCP/IP Application | Exit Point   | Exit Point Format |
|--------------------|--|-------------------|
| <b>Note:</b>       |  |                   |
| 1                  | The same interface format is used for request validation for the FTP client, FTP server, REXEC server, and TFTP server. This allows the use of one exit program for request validation of any combination of these applications.   |                   |
| 2                  | The same interface format is used for server log-on processing for the FTP server and REXEC server applications. This allows the use of one exit program to process log-on requests for both of these applications.  |                   |
| 3                  | For a detailed description of the DHCP exit points and how to use them, see System API Reference ( <a href="http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/apis/api.htm">http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/apis/api.htm</a> ) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information. |                   |

## Creating Exit Programs

There are several steps involved in designing and writing exit programs. They include:

1. Review the purpose of the exit point and the format of its interface
2. Define the scope and operation of your exit program
3. Design the exit program
4. Code the exit program
5. Add the exit program to the appropriate exit point in the registration facility. (See "Adding Your Exit Program to the Registration Facility" for instructions on how to do this.)

**Note:** Only users with both \*SECADM and \*ALLOBJ authority are allowed to add and remove TCP/IP application exit programs.

6. Test your exit program
  - Tests for each user ID
  - Tests for each operation

The most important step in establishing security exit programs is verifying that the exit program works. You must assure that the security wall works and does not have any weaknesses.

### Notes:

1. If the exit program fails or returns an incorrect output parameter, the operation will not be allowed by the TCP/IP application.
2. To ensure the highest level of security, create the exit program in a library that has \*PUBLIC authority of \*EXCLUDE and give the exit program itself a \*PUBLIC authority of \*EXCLUDE. The TCP/IP application adopts authority when it is necessary to resolve and call the exit program.

## Adding Your Exit Program to the Registration Facility

To add your exit program, run the Work with Registration Information (WRKREGINF) command. The following display is shown:

```

Work with Registration Information

Type options, press Enter.
 5=Display exit point  8=Work with exit programs

  Opt  Exit Point      Exit Point      Format  Registered  Text
      QIBM_QRQ_SQL      RSQL0100      *YES   Original Remote SQL Server
      QIBM_QSY_CHG_PROFILE CHGP0100      *YES   Change User Profile Exit Poin
      QIBM_QSY_CRT_PROFILE CRTP0100      *YES   Create User Profile Exit Poin
      QIBM_QSY_DLT_PROFILE DLTP0100      *YES   Delete User Profile Exit Poin
      QIBM_QSY_DLT_PROFILE DLTP0200      *YES   Delete User Profile Exit Poin
      QIBM_QSY_RST_PROFILE RSTP0100      *YES   Restore User Profile Exit Poi
      QIBM_QTF_TRANSFER  TRAN0100      *YES   Original File Transfer Functi
      QIBM_QTMF_CLIENT_REQ VLRQ0100      *YES   FTP Client Request Validation
      QIBM_QTMF_SERVER_REQ VLRQ0100      *YES   FTP Server Request Validation
      QIBM_QTMF_SVR_LOGON TCPL0100      *YES   FTP Server Logon
      QIBM_QTMT_WSG      QAPP0100      *YES   WSG Server Sign-On Validation

                                                                 More...

Command
===>
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel

```

Figure 63. Work with Registration Information Display — Display 1

### Step 1. Select your exit point

Type 8 next to the exit point to which you want to add an exit program. For example, to associate a program with the WSG server sign-on validation exit point, type an 8 next to this exit point, as shown.

```

      QIBM_QSY_RST_PROFILE RSTP0100      *YES   Restore User Profile Exit Poi
      QIBM_QTF_TRANSFER  TRAN0100      *YES   Original File Transfer Functi
      QIBM_QTMF_CLIENT_REQ VLRQ0100      *YES   FTP Client Request Validation
      QIBM_QTMF_SERVER_REQ VLRQ0100      *YES   FTP Server Request Validation
      QIBM_QTMF_SVR_LOGON TCPL0100      *YES   FTP Server Logon
8  QIBM_QTMT_WSG      QAPP0100      *YES   WSG Server Sign-On Validation

                                                                 More...

Command
===>
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel

```

Figure 64. Work with Registration Information Display — Display 2

The Work with Exit Programs display is shown.



```

Work with Exit Programs
Exit point:  QIBM_QTMT_WSG          Format:  QAPP0100
Type options, press Enter.
  1=Add  4=Remove  5=Display  10=Replace

      Exit
      Program      Exit
Opt      Number      Program      Library

      (No exit programs found.)

```

Figure 65. Adding an Exit Program — Display 1

### Step 2: Select the Add Exit Program option

Select the add option by typing a 1 (Add) in the Opt column as shown in Figure 66.

```

Work with Exit Programs
Exit point:  QIBM_QTMT_WSG          Format:  QAPP0100
Type options, press Enter.
  1=Add  4=Remove  5=Display  10=Replace

      Exit
      Program      Exit
Opt      Number      Program      Library
  1

      (No exit programs found.)

```

Figure 66. Adding an Exit Program — Display 2

### Step 3: Add your exit program

Fill in the exit program information as shown in Figure 67 on page 84 and Figure 68 on page 84, then press enter.

#### Notes:

1. You can bypass Steps 1 and 2 by using the Add Exit Program (ADDEXITPGM) command.
2. You must set the Program number parameter of the Add Exit Program (ADDEXITPGM) command to 1 when adding exit programs to FTP exit points.
3. When you add exit programs for FTP clients, these programs take effect as soon as you start additional sessions. Changes do not affect client sessions that are already running.
4. When you add FTP server exit programs, end and restart the FTP servers to ensure that all servers are using the exit programs.

When you add workstation gateway server exit programs, you do not need to end and restart the workstation gateway server. The WSG server checks for the exit program dynamically.

When you add REXEC server exit programs, you do not need to end and restart the REXEC server. The REXEC server checks for the exit programs dynamically.

```

Add Exit Program (ADDEXITPGM)

Type choices, press Enter.

Exit point . . . . . > QIBM_QTMT_WSG
Exit point format . . . . . > QAPP0100      Name
Program number . . . . . > 1                1-2147483647, *LOW, *HIGH
Program . . . . . > YOURPGM                Name
Library . . . . . > YOURLIB                Name, *CURLIB
Text 'description' . . . . . > 'Description of your exit program'

Additional Parameters

Replace existing entry . . . . . > *NO          *YES, *NO
Create exit point . . . . . *NO            *YES, *NO

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
More...

```

Figure 67. Adding an Exit Program — Display 3

```

Add Exit Program (ADDEXITPGM)

Type choices, press Enter.

Exit program data:
Coded character set ID . . . . . *JOB          Number, *NONE, *JOB
Length of data . . . . .                0-2048, *CALC
Program data . . . . .

...

```

Figure 68. Adding an Exit Program — Display 4

## Removing Exit Programs

To remove an exit program from an exit point, do one of the following:

- Follow the steps for adding an exit point until the Work with Exit Programs display is shown. Select option 4 (Remove) to remove the exit program.
- Use the Remove Exit Program (RMVEXITPGM) command.

When you remove an exit program that performs a security-related operation, this operation is no longer performed. Remove security-related exit programs with caution.

---

## Exit Point Interfaces for TCP/IP Application Exit Points

The exit point interfaces for TCP/IP application exit points are:

- TCP/IP application request validation exit point interface
- TCP/IP remote execution server command processing selection exit point interface

**Note:** For a detailed description of the DHCP exit points and how to use them, see System API Reference (<http://publib.boulder.ibm.com/pubs/html/as400/v5r1/ic2924/info/apis/api.htm>) in the Information Center. If you are using the Supplemental Manuals CD, then switch to the iSeries Information Center CD to access this information.

### TCP/IP Application Request Validation Exit Point Interface

Required Parameter Group:

|   |  |        |           |
|---|--|--------|-----------|
| 1 | Application identifier                   | Input  | Binary(4) |
| 2 | Operation identifier                     | Input  | Binary(4) |
| 3 | User profile                             | Input  | Char(10)  |
| 4 | Remote IP address                        | Input  | Char(*)   |
| 5 | Length of remote IP address              | Input  | Binary(4) |
| 6 | Operation-specific information           | Input  | Char(*)   |
| 7 | Length of operation-specific information | Input  | Binary(4) |
| 8 | Allow operation                          | Output | Binary(4) |

Exit Point Name: QIBM\_QTMF\_CLIENT\_REQ

Exit Point Name: QIBM\_QTMF\_SERVER\_REQ

Exit Point Name: QIBM\_QTMX\_SERVER\_REQ

Exit Point Name: QIBM\_QTOD\_SERVER\_REQ

Exit Point Format Name: VLRQ0100

The TCP/IP request validation exit point enables additional control for restricting an operation. Any restrictions that are imposed by the exit program are in addition to any validation that is performed by the application program, such as normal server object security. When an exit program is added to the exit point, it is called by the TCP/IP application to validate the requested action specified by the operation identifier and other input parameters in the required parameter group. The exit program sets the output parameter, Allow operation, to indicate if the TCP/IP application is to perform the operation.

**Note:** All character data passed to the exit program is in the coded character set ID (CCSID) of the job, or if the job CCSID is 65535, the default CCSID of the job.

### Required Parameter Group

#### Application identifier

INPUT; BINARY(4) Identifies the application program from which the request is being made. The valid values are as follows:

- 0 FTP client program
- 1 FTP server program
- 2 REXEC server program

### 3 TFTP server program

#### Operation identifier

INPUT; BINARY(4) Indicates the operation that the user is attempting to perform. When the application identifier indicates the FTP client or FTP server program, the valid values are as follows:

- 0 Session initialization
- 1 Directory/library creation
- 2 Directory/library deletion
- 3 Set current directory
- 4 List files
- 5 File deletion
- 6 Sending file
- 7 Receiving file
- 8 Renaming file
- 9 Execute CL command

When the application identifier indicates the REXEC server program, valid values are as follows:

- 0 Session initialization
- 9 Perform CL command

When the application identifier indicated the TFTP server program, the valid values are as follows:

- 6 Sending file (RRQ)
- 7 Receiving file (WRQ)

#### User profile

INPUT; CHAR(10) The user profile under which the requested operation is run (if it is allowed).

#### Remote IP address

INPUT; CHAR(\*) The Internet Protocol (IP) address of the remote host system. This string is in dotted decimal format, left justified. The remote host may be a client or a server based on the setting of the *application identifier* parameter.

#### Length of remote IP address

INPUT; BINARY(4) Indicates the length (in bytes) of the remote IP address.

#### Operation specific information

INPUT; CHAR(\*) Information that describes the operation being attempted. The contents of this field are dependent on the value of the operation identifier.

For operation identifier 0 and application identifier 0, there is no operation-specific information. This field is blank.

For operation identifier 0 and application identifier 1, the operation-specific information contains the IP address that identifies the TCP/IP interface through which the connection to the local host (server) system is established. This string is in dotted decimal format, left justified.

For operation identifiers 1 through 3, the operation-specific information contains the name of the directory or library on which the operation is to be performed. The directory or library name is formatted as an absolute path name.

For operation identifiers 4 through 8, the operation-specific information contains the name of the file on which the operation is to be performed. The file name is formatted as an absolute path name.

For operation identifier 9, the operation-specific information contains the iSeries Control Language (CL) command which is to be run at the user's request.

**Note:** See "Usage Notes" for a summary of the operation-specific information that is required for each operation identifier.

#### **Length of operation-specific information**

INPUT; BINARY(4) Indicates the length (in bytes) of the operation-specific information, or 0 if no operation-specific information is provided.

#### **Allow operation**

OUTPUT; BINARY(4) Indicates whether the operation should be accepted or rejected. The valid values are as follows:

- 1 Never allow this operation identifier:
  - This operation identifier is to be unconditionally rejected for the remainder of the current session.
  - The exit program will not be called again for this operation identifier.
- 0 Reject the operation
- 1 Allow the operation
- 2 Always allow this operation identifier.
  - This operation identifier is to be allowed unconditionally for the remainder of the current session.
  - The exit program will not be called again with this operation identifier.

#### **Usage Notes**

For FTP, if the returned Allow operation output parameter is not valid, the FTP application will not allow the operation and the message "Data from exit program for exit point &1; is missing or not valid" will be issued to the job log.

For FTP, if any exception is encountered when calling the exit program, the FTP application will issue the message: Exception encountered for FTP exit program &1; in library &2; for exit point &3;

Two different exit points are provided for the FTP application. Exit point QIBM\_QTMF\_CLIENT\_REQ is used to validate requests processed by the FTP client program. Exit point QIBM\_QTMF\_SERVER\_REQ is used to validate requests processed by the FTP server program. If desired, the same exit program can be used to validate requests from both of these exit points.

Table 10 on page 88 summarizes the operation-specific information required for each operation identifier.

Table 10. Application Request Validation Operation-Specific Information

| Operation Identifier | Operation-Specific Information   |
|----------------------|--|
| 0                    | NONE if application ID=0   |
| 0                    | Dotted decimal format IP address of client host when application ID=1 or 2   |
| 1-3                  | Absolute path name of library or directory<br>/QSYS.LIB/QGPL.LIB <sup>1</sup><br>/QOpenSys/DirA/DirAB/DirABC <sup>2</sup>                |
| 4-8                  | Absolute path name of file<br>/QSYS.LIB/MYLIB.LIB/MYFILE.FILE/MYMEMB.MBR <sup>1</sup><br>/QOpenSys/DirA/DirAB/DirABC/FileA1 <sup>2</sup> |
| 9                    | CL command string  |
| :                    |  |
| <sup>1</sup>         | QSYS.LIB file system pathnames are always in uppercase   |
| <sup>2</sup>         | QOpenSys file system pathnames are case sensitive and may be in either upper or lower case.  |

Table 11 defines the FTP client and server subcommands that are associated with each operation identifier.

Table 11. FTP Client and Server Subcommands Associated with Operation Identifiers

| Operation Identifier  | Client Subcommands             | Server Subcommands                            |
|---|--------------------------------|---|
| 0 - Initialize Session  | OPEN                           | new connection <sup>1</sup>                   |
| 1 - Create Directory/Library  |                                | MKD, XMKD                                     |
| 2 - Delete directory/library  |                                | RMD, XRMD                                     |
| 3 - Set current directory   | LCD                            | CWD, CDUP, XCWD, XCUP                         |
| 4 - List directory/library  |                                | LIST, NLIST                                   |
| 5 - Delete files  |                                | DELE  |
| 6 - Send files  | APPEND, PUT, MPUT <sup>2</sup> | RETR  |
| 7 - Receive files   | GET, MGET <sup>2</sup>         | APPE, STOR, STOU                              |
| 8 - Rename files  |                                | RNFR, RNTO                                    |
| 9 - Execute CL commands   | SYSCMD <sup>3</sup>            | RCMD, ADDM, ADDV, CRTL, CRTP, CRTS, DLTF, DLT |
| :   |                                |   |
| <b>Notes:</b>   |                                |   |
| 1. The exit program is called with this operation identifier each time the FTP server receives a connection request.  |                                |   |
| 2. For the MGET and MPUT subcommands, the exit program is called once for each file that is sent or retrieved.  |                                |   |
| 3. If an exit program is associated with exit point QIBM_QTMF_CLIENT_REQ, the F21 (CL command line) key is disabled and the user must use the System Command (SYSCMD) subcommand to run a CL command. |                                |   |

**The following notes apply to the REXEC server (application identifier 2):**

1. The only valid values for the operation identifier are 0 and 9.
2. If the returned Allow operation output parameter is not valid, the REXEC server will not allow the operation and the message "Data from exit program for exit point &1 is missing or not valid" is issued to the job log.

3.

If any exception is encountered when calling the exit program, the REXEC server will not allow the operation and the message "Exception encountered for REXEC exit program &1 in library &2 for exit point &3." is issued to the job log.

**The following note applies to the TFTP server (application identifier 3):**

1. For the TFTP server program, operation identifier 6 indicates the TFTP Read Request (RRQ) operation; operation code 7 indicates the TFTP Write Request (WRQ) operation.

## Remote Execution Server Command Processing Selection Exit Point

The REXEC server command processing selection exit program enables you to select:

- Which command processor runs the command that the REXEC client user provides
- Whether the REXEC server converts data between ASCII and EBCDIC (for Qshell commands or spawn path names)

Required Parameter Group:

|   |                              |        |           |
|---|------------------------------|--------|-----------|
| 1 | User profile                 | Input  | Char(10)  |
| 2 | Remote IP address            | Input  | Char(*)   |
| 3 | Length of remote IP address  | Input  | Binary(4) |
| 4 | Command string               | Input  | Char(*)   |
| 5 | Length of command string     | Input  | Binary(4) |
| 6 | Command processor identifier | Output | Binary(4) |
| 7 | Character conversion option  | Output | Binary(4) |

Exit Point Name: QIBM\_QTMF\_SVR\_SELECT

Exit Point Format Name: RXCS0100

**Note:** Character data passes to the exit program in the coded character set identifier (CCSID) of the job. If the job CCSID is 65535, the server uses the default CCSID of the job.

### Required Parameter Group

#### User profile

INPUT; CHAR(10) The user profile under which the requested operation is run.

#### Remote IP address

INPUT; CHAR(\*) The Internet Protocol (IP) address of the REXEC client system. This string is in dotted decimal format, left justified.

#### Length of remote IP address

INPUT; BINARY(4) Indicates the length (in bytes) of the remote IP address.

#### Command string

INPUT; CHAR(\*) The command to be run as specified by the REXEC client.

#### Length of command string

INPUT; BINARY(4) Indicates the length (in bytes) of the command string.

### Command processor identifier

OUTPUT; BINARY(4) Indicates the command processor that you want the server to use for interpreting and running the command. The following values are valid:

- 0 iSeries Control Language  
The server processes the command as an iSeries control language (CL) command. This is the default value.
- 1 Qshell command  
The Qshell command interpreter processes the command. The server uses the spawn() application program interface (API) to call QShell as a child job.
- 2 Spawn path name  
The server treats the command name as a path name and passes it to the spawn() application program interface (API), which runs as a child job.

### Character conversion option

OUTPUT; BINARY(4) Indicates whether the REXEC server performs ASCII-EBCDIC character conversion for data that is passed on the stdin, stdout, and stderr streams. These values are valid:

- 0 Do not convert data. The server transfers all data on the stdin, stdout, and stderr streams without converting it.
  - 1 Convert data.
    - The server converts data in the stdin stream from the ASCII CCSID that the CHGRXCA command specifies to the job CCSID. If the job CCSID is 65535, the server uses the default CCSID of the job.
    - The server converts data in the stdout and sterr streams from the job CCSID to the ASCII CCSID that the CHGRXCA command specifies. If the job CCSID is 65535, the server uses the default CCSID of the job.
- This is the default value.

### Usage Notes

- If you add exit programs to both the QIBM\_QTMX\_SERVER\_REQ and QIBM\_QTMX\_SVR\_SELECT exit points, REXEC server first calls the exit program that you add to the QIBM\_QTMX\_SERVER\_REQ exit point. If this program allows the operation, the server then calls the exit program that you add to the QIBM\_QTMX\_SVR\_SELECT exit point.
- When you set the Command processor identifier parameter to 0 (iSeries Control Language command), the conversion option is ignored. The server always performs character conversion for CL commands.
- When you set the command processor identifier to 1 (Qshell Command), the server sets these environment variables:
  - TERMINAL\_TYPE= REMOTE
  - PATH= /usr/bin:
  - LOGNAME= *user* (where *user* is the user profile)
  - HOME= *homedir* (where *homedir* is the user's home directory)



| If the Qshell Interpreter option of OS/400 is not installed, the REXEC client  
| receives (in the stdout stream) a REXEC protocol diagnostic message that says  
| "Qshell interpreter not installed".

- | • When you set the Command processor identifier parameter to 1 or 2:
  - | – The server maps the REXEC stdin, stderr, and stdout streams to file  
| descriptors 0, 1, and 2, respectively.
  - | – The server sets the QIBM\_USE\_DESCRIPTOR\_STDIO environment variable to  
| Y.

| Any other environment variables that the exit program sets are inherited by the  
| child job.

- | • If you set the Command processor identifier parameter to 2 and the command  
| string is not a valid path name for the spawn() API, the message "Incorrect  
| command or path name specified" is returned to the REXEC client in the stderr  
| stream.



---

## Notices

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

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

IBM Director of Licensing  
IBM Corporation  
500 Columbus Avenue  
Thornwood, NY 10594  
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, 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.

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  
3605 Highway 52 N  
Rochester, MN 55901-7829  
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 or any equivalent agreement between us.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates 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. 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 IBM's application programming interfaces.

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

---

## Programming Interface Information

This publication is intended to help you to use the TCP/IP function with the IBM iSeries server. This publication documents General-Use Programming Interface and Associated Guidance Information provided by TCP/IP Connectivity Utilities for iSeries licensed program and the OS/400 licensed program.

General-Use programming interfaces allow the customer to write programs that obtain the services of the TCP/IP Utilities licensed program and the OS/400 licensed program.

---

## Trademarks

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

400  
Advanced Function Printing  
AFP  
AIX  
AnyNet  
Application System/400  
APPN  
AS/400

| AS/400e  
| AT  
| C/400  
| CICS/400  
| Client Access  
| CT  
| DB2  
| Distributed Relational Database Architecture  
| DRDA  
| e (Stylized)  
| IBM  
| IBM Global Network  
| Integrated Language Environment  
| Intelligent Printer Data Stream  
| IPDS  
| iSeries  
| iSeries 400  
| Netfinity  
| Network Station  
| OfficeVision  
| OfficeVision/400  
| Operating System/400  
| OS/2  
| OS/400  
| Print Services Facility  
| Proprinter  
| RISC System/6000  
| RPG/400  
| RS/6000  
| S/390  
| SecureWay  
| SP  
| System/36  
| System/38  
| System/370  
| System/390  
| ThinkPad  
| WebExplorer  
|

| Microsoft<sup>®</sup>, Windows<sup>®</sup>, Windows NT<sup>®</sup>, and the Windows logo are registered  
| trademarks of Microsoft Corporation in the United States, other countries, or both.

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

| UNIX<sup>®</sup> is a registered trademark in the United States, other countries, or both and  
| is licensed exclusively through X/Open Company Limited.

| Lotus<sup>®</sup> Notes<sup>™</sup> is a registered trademark, and Notes and Domino<sup>™</sup> are trademarks  
| of Lotus Development Corporation in the United States, other countries, or both.

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



# Index

## Special Characters

- \*AIX format 51
- \*AS400 format 51
- \*BASE pool size 71
- \*IOSYSCFG authority 10
- \*NIC format 51
- \*SYSGEN default value 10, 76  
(Transmission Control Protocol/Internet Protocol)  
attributes 16

## A

- AA entry 76
- Add TCP/IP Remote System Information (ADDTCPRSI) command 17
- Add TCP/IP Route (ADDTCPRTE) command 14
- adding
  - default routes 15
  - TCP/IP remote system information 17
  - TCP/IP route 12
- ADDTCPRSI (Add TCP/IP Remote System Information) command 17
- ADDTCPRTE (Add TCP/IP Route) command 14
- application
  - exit points 80
    - exit point interface 85
    - exit programs 79, 89
  - application request validation
    - exit point interface 85
- attribute
  - TCP/IP
    - Change TCP/IP Attributes (CHGTCPA) command 16
    - IP datagram forwarding 16
- authority
  - \*IOSYSCFG 10
- automatic configuration
  - creating controllers 75

## B

- binding, route-to-interface 36

## C

- CFGTCP (Configure TCP/IP) command 7
- Change TCP/IP Attributes (CHGTCPA) command 16
- changing
  - TCP/IP attributes 16
- CHGTCPA (Change TCP/IP Attributes) command 16
- command, CL
  - Add TCP/IP Remote System Information (ADDTCPRSI) 17

- command, CL (*continued*)
  - Add TCP/IP Route (ADDTCPRTE) 14
  - ADDTCPRSI (Add TCP/IP Remote System Information) 17
  - ADDTCPRTE (Add TCP/IP Route) 14
  - Change TCP/IP Attributes (CHGTCPA) 16
  - CHGTCPA (Change TCP/IP Attributes) 16
  - Create Controller Description (Network) (CRTCTLNET) 75
  - Create Device Description (Network) 75
  - CRTCTLNET (Create Controller Description (Network)) 75
  - CRTDEVNET (Create Device Description (Network)) 75
  - End TCP/IP (ENDTCP) 26
  - End TCP/IP Connections (ENDTCPCNN) 41
  - ENDTCP (End TCP/IP) 26
  - ENDTCPCNN (End TCP/IP Connections) 41
  - Remove Exit Program (RMVEXITPGM) 84
  - RMVEXITPGM (Remove Exit Program) 84
  - Start TCP/IP (STRTCP) 24
  - STRTCP (Start TCP/IP) 24
  - Verify TCP/IP Connection (VFYTCPCNN) 27
  - VFYTCPCNN (Verify TCP/IP Connection) 27
  - Work with Registration Information (WRKREGINF) 81
  - Work with TCP/IP Network Status (WRKTCPPSTS) 33
  - WRKREGINF (Work with Registration Information) 81
  - WRKTCPPSTS (Work with TCP/IP Network Status) 33
- command, TCP/IP
  - Network Status (NETSTAT) 33
  - Packet Internet Groper (PING) 27
- command processing selection
  - exit point interface 89
- Configure TCP/IP (CFGTCP) command 7
- configuring
  - Configure TCP/IP menu 7
  - default routes 15
  - host table 18
  - interface 10
  - IP datagram forwarding 16
  - line 10
  - line description 76
  - local domain and host name 22
  - maximum transmission unit (MTU) 13

- configuring (*continued*)
    - multiple-network example 2
    - multiple systems 53
    - next hop 12
    - planning for X.25 2
    - ports 62
    - remote system (X.25) information 16
    - routes 12
    - single-network example 9
    - subnet mask 12
    - TCP/IP Administration menu 2
    - TCP/IP attributes 16
    - TCP/IP interfaces 10
    - TCP/IP menu 7
  - connection
    - display TCP/IP connections 48
    - displaying totals 49
    - End TCP/IP Connections (ENDTCPCNN) command 41
    - status, work with TCP/IP connection 38
    - verify TCP/IP connection 27
  - connection-oriented sockets
    - SOCK\_STREAM 68
  - connection type
    - Ethernet 10
    - fiber distributed data interface (FDDI) 10
    - frame relay 10
    - shielded twisted pair distributed data interface (SDDI) 10
    - token-ring 10
    - wireless LAN 10
    - X.25 PVC 10
    - X.25 SVC 10
  - converting
    - files 54
  - Create Controller Description (Network) (CRTCTLNET) command 75
  - Create Device Description (Network) (CRTDEVNET) command 75
  - creating
    - exit point programs 81
    - line description 76
  - CRTCTLNET (Create Controller Description (Network)) command 75
  - CRTDEVNET (Create Device Description (Network)) command 75
- ## D
- datagram
    - forwarding 16
  - datagram size
    - determining the maximum 77
  - DDI (distributed data interface)
    - fiber distributed data interface (FDDI) 2
    - shielded twisted pair distributed data interface (SDDI) 2
  - DDN (Defense Data Network) conversion algorithm 17

- dead gateway processing 55
- default route
  - adding 15
- display
  - TCP/IP connections 48
- displaying
  - system name and address 19
- distributed data interface (DDI)
  - fiber distributed data interface (FDDI) 2
  - shielded twisted pair distributed data interface (SDDI) 2
- domain name 22

## E

- End TCP/IP Connections (ENDTCPENN)
  - command 41
- End TCP/IP Interfaces (ENDTCPIFC)
  - command 36
- ending
  - interfaces, route-to-interface
    - binding 36
    - TCP/IP connections 41
- ENDTCPENN (End TCP/IP Connections)
  - command 41
- ENDTCPIFC (End TCP/IP Interfaces)
  - command 36
- Ethernet
  - \*SYSGEN default value 76
  - AA entry 76
  - Version 2 76
- example
  - multihoming 57, 58, 59
  - multiple network configuration 2
  - partly successful host table merge 53
  - single network configuration 9
  - successful host table merge 53
  - using X.25 permanent virtual circuit (PVC) 67
  - verifying connections
    - host name 29
    - Internet address 30
    - PING LOOPBACK 26
- exit point
  - application 80
  - description 79
  - interface 79
  - programs, creating 81
  - registration facility 80
  - REXEC server 89
- exit point interface 85
  - application request validation 85
  - command processing selection 89
- exit program 79, 89
  - adding to registration facility 81
  - application validation 85
  - description 79
  - File Transfer Protocol (FTP)
    - request validation 85
  - removing from exit point 84

## F

- fiber distributed data interface (FDDI) 2
- File Transfer Protocol (FTP)
  - exit program 79, 85

- File Transfer Protocol (FTP) (*continued*)
  - request validation exit program 85
  - starting
    - to remote system 53
- format
  - \*AIX 51
  - \*AS400 51
  - \*NIC 51
- frame relay 2
- FTP (File Transfer Protocol)
  - exit program 79, 85
  - request validation exit program 85
  - starting
    - to remote system 53

## G

- gateway
  - processing dead 55

## H

- hops 13
- host
  - multihomed 56
- host file
  - sending to remote system 53
- host information 51
- host name
  - configuring 22
  - definition 22
- host table
  - adding entry 18
  - before using STRTCP command 25
  - configuring 18
  - conversion 25
  - creating 53
  - displaying 19
  - duplicate host names 52
  - listing 19
  - managing 51
  - merge file 54
  - merging 52
  - more than four host names 52
  - performance when merging 73
  - sending host file to remote system 53
  - sending information 51
  - sharing with multiple systems 53
  - socket applications 65
  - starting FTP to remote system 53
  - successful merge 53
  - unsuccessful merge 53
  - using \*AIX files 51
  - using \*NIC files 51

## I

- ICMP (Internet Control Message Protocol)
  - redirect message 54
- interface
  - binding with routes 36
  - definition 10
  - End TCP/IP Interfaces (ENDTCPIFC)
    - command 36
  - exit point 79

- interface (*continued*)
  - Start TCP/IP Interfaces (STRTCPICF)
    - command 35
- Internet address
  - displaying 19
  - listing 19
- Internet Control Message Protocol (ICMP)
  - redirect message 54
- IP datagram forwarding 16
- IP multicasting
  - host group
    - multicast capable routers 68
    - subnet 68
- IP Routing and Internet Control Message Protocol (ICMP) redirecting 54

## J

- job log
  - associated with host table merge 52
- jobs
  - TCP/IP 25, 71

## L

- line description
  - configuring 76
  - creating 76
  - definition 10
  - maximum transmission unit 77
  - types supported 75
- local domain and host name
  - configuring 22
  - definition 22
- local domain name 22
- local host name 22
- LOCALHOST host name 20

## M

- managing
  - host tables 51
  - multiple systems 53
- maximum transmission unit (MTU)
  - configuring 13
  - definition 13
  - parameter description 77
- merging host tables 52
  - performance 73
- MTU (maximum transmission unit)
  - configuring 13
  - definition 13
  - parameter description 77
- multicast application programming
  - information 68
- multicast datagrams 68
- multicast restrictions 68
- multihoming 56
- multiple hosts 56
- multiple logical interfaces 56
- multiple routes
  - description 61
- multiple systems
  - configuring 53



## N

NETSTAT (Network Status)  
command 33  
network interface  
types supported 75  
Network Status (NETSTAT)  
command 33  
network status for TCP/IP  
connections  
display 40, 48  
display totals 49  
end 40  
general information 38  
ending interfaces 36  
interface  
display associated routes 44  
work with configuration status 41  
interface status  
display 43  
work with 34  
route information, display 37, 46  
starting interfaces 35  
work with 33  
next hop 13  
definition 13  
Notices 93

## P

packet forwarding 16  
Packet Internet Groper (PING)  
command 27  
packet routing 16  
parameter  
maximum transmission unit (MTU) 77  
MTU (maximum transmission unit) 77  
TCPONLY 73  
performance  
\*BASE pool size 71  
merging host tables 73  
TCP/IP jobs 71  
permanent virtual circuit (PVC)  
example 67  
obtaining a network address 2  
physical line 75  
PING (Packet Internet Groper)  
command 27  
planning  
TCP/IP installation and configuration 2  
pool size 71  
port  
definition 62  
restriction 62  
preferred binding interface 13  
profile 64  
PVC (permanent virtual circuit)  
example 67  
obtaining a network address 2

## Q

QAPP0100 81  
QAPPCTCP server job 25

QSNMPA server job 25  
QSYSWRK subsystem 25  
QTCPIP server job 25  
QFTFPxxxxx server job 25  
QTGTELNETS server job 25  
QTLPDxxxxx server job 25  
QTMSNMP server job 25  
QTMSNMPRCV server job 25  
QTSMTPBRCV job 25  
QTSMTPBRSR job 25  
QTSMTPLCLNT job 25  
QTSMTPSRVR job 25

## R

registration facility  
adding exit program to 81  
exit point 80  
related tables 65  
Remote Execution (REXEC) server  
exit programs 89  
remote system  
definition 2  
determining address on X.25 network 2  
Remove Exit Program (RMVEXITPGM)  
command 84  
removing  
exit program 84  
request validation  
application exit point interface 85  
exit program, FTP 85  
REXEC (Remote Execution) server  
exit programs 89  
RMVEXITPGM (Remove Exit Program)  
command 84  
route  
default 15  
TCP/IP route information, display 37, 46  
route destination  
definition 13  
route-to-interface binding, ending interfaces 36

## S

sending  
host file to remote system 53  
host information  
using \*AIX format 51  
using \*AS400 format 51  
using \*NIC format 51  
server job  
QAPPCTCP 25  
QSNMPA 25  
QTCPIP 25  
QFTFPxxxxx 25  
QTGTELNETS 25  
QTLPDxxxxx 25  
QTMSNMP 25  
QTMSNMPRCV 25  
QTSMTPBRCV 25  
QTSMTPBRSR 25  
QTSMTPLCLNT 25  
QTSMTPSRVR 25  
TCP/IP 25

setsockopt() function 68  
shielded twisted pair distributed data interface (SDDI) 2  
Simple Mail Transfer Protocol (SMTP)  
performance 71  
SMTP (Simple Mail Transfer Protocol)  
performance 71  
sockets  
SOCK\_DGRAM 68  
source service access point (SSAP)  
AA entry 76  
Ethernet line 76  
special authority, \*IOSYSCFG 10  
SSAP (source service access point)  
AA entry 76  
Ethernet line 76  
Start TCP/IP Interfaces (STRTCPIFC)  
command  
TCP/IP interfaces 35  
starting  
TCP/IP and TCP/IP servers 24  
STRTCPIFC (Start TCP/IP Interfaces)  
command 35  
subnet  
addressing  
definition 13  
mask  
definition 13  
routing  
definition 13  
subnetting  
definition 13  
SVC (switched virtual circuit)  
obtaining a network address 2  
switched virtual circuit (SVC)  
obtaining a network address 2  
system name  
displaying 19  
listing 19

## T

tables  
required for socket applications 65  
TCP/IP (Transmission Control Protocol/Internet Protocol)  
attributes 16  
ending  
End TCP/IP (ENDTCP)  
command 26  
installation and configuration  
planning 2  
interface  
entry 10  
job  
description 71  
QAPPCTCP 25  
QSNMPA 25  
QTCPIP 25  
QFTFPxxxxx 25  
QTGTELNETS 25  
QTLPDxxxxx 25  
QTMSNMP 25  
QTMSNMPRCV 25  
QTSMTPBRCV 25  
QTSMTPBRSR 25  
QTSMTPLCLNT 25

- TCP/IP (Transmission Control Protocol/Internet Protocol) *(continued)*
  - QTSMTPSRVR 25
  - planning for installation and configuration 2
  - QSYSWRK subsystem 25
  - starting 24
- TCP/IP Administration (TCPADM)
  - menu 2
- TCP/IP servers
  - starting 24
- TCPONLY parameter 73
- Transmission Control Protocol/Internet Protocol (TCP/IP)
  - attributes 16
  - interface
    - entry 10
  - job
    - description 71
    - QAPPCTCP 25
    - QSNMPSA 25
    - QTCPIP 25
    - QTFTPxxxxx 25
    - QTGTELNETS 25
    - QTLPDxxxxx 25
    - QTMSNMP 25
    - QTMSNMPCV 25
    - QTSMPBRCL 25
    - QTSMPBRSL 25
    - QTSMPCLNT 25
    - QTSMTPSRVR 25
  - QSYSWRK subsystem 25
  - starting 24
- X.25 *(continued)*
  - DDN conversion algorithm 17
  - obtaining network addresses 2
  - permanent virtual circuit (PVC) 2
  - switched virtual circuit (SVC) 2

## U

- user profile
  - definition 64

## V

- Verify TCP/IP Connection (VFYTCPCNN) command 27
- verifying
  - TCP/IP connections 27
- VFYTCPCNN (Verify TCP/IP Connection) command 27

## W

- wireless LAN 2
- Work with Registration Information (WRKREGINF) command 81
- work with TCP/IP connection status 38
- Work with TCP/IP Network Status (WRKTCPSTS) command 33
- WRKREGINF (Work with Registration Information) command 81
- WRKTCPSTS (Work with TCP/IP Network Status) command 33

## X

- X.25
  - configuring X.25 remote system information 16





Printed in the United States of America  
on recycled paper containing 10%  
recovered post-consumer fiber.

SC41-5420-04



## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>