Intermec
Technologies Corporation

6400 Computer TCP/IP Client

USER'S GUIDE

P/N 961-054-012
Revision D
October 2000

▶ NOTICE

The information contained herein is proprietary and is provided solely for the purpose of allowing customers to operate and service Intermec manufactured equipment and is not to be released, reproduced, or used for any other purpose without written permission of Intermec.

We welcome your comments concerning this publication. Although every effort has been made to keep it free of errors, some may occur. When reporting a specific problem, please describe it briefly and include the book title and part number, as well as the paragraph or figure number and the page number.

Send your comments to:
Intermec Technologies Corporation
Publications Department
550 Second Street SE
Cedar Rapids, IA 52401

INTERMEC, NORAND are registered trademarks of Intermec Technologies Corporation.

INTERMEC, NORAND, and PEN*KEY are registered trademarks and ENTERPRISE WIRELESS LAN, UAP, and UNIVERSAL ACCESS POINT are trademarks of Intermec Technologies Corporation.

© 1998 Intermec Technologies Corporation. All rights reserved.

This publication printed on recycled paper.

Acknowledgments

FTP Software and *PC/TCP* are registered trademarks of FTP Software, Inc.
HP is a registered trademark and *HP OpenView* is a trademark of Hewlett-Packard Company.
IBM is a registered trademark of International Business Machines Corporation.
MS-DOS is a registered trademark of Microsoft Corporation.
Proxim is a registered trademark of Proxim, Inc.
UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

FCC Computer Compliance

▶ NOTICE

This equipment meets Class B digital device limits per Part 15 of FCC Rules. These limits protect against interference in a residential area. It emits, uses, and can radiate radio frequency energy. If you do not install and use the equipment according to its instructions, it may interfere with radio signals. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning our equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the radio or television receiving antenna.
- Increase the separation between the computer equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the radio or television receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

FCC Spread Spectrum Radio Certification

▶ **NOTICE**

This device is certified to operate under Part 15, Subpart C, Section 15.247 of the FCC rules for Intentional Radiation Products. This certification includes Docket 87-389 covering rules effective June 1994. It may not cause interference to authorized radio communication devices, and must accept any interference caused by those devices.

Antenna Requirements

▶ **NOTICE**

FCC rules section 15.203 and Canada's RSS-210 require that this device be operated using an antenna furnished by the manufacturer. The antenna coupling on this product has been designed to accept only antennas manufactured by us. Use of an antenna other than that furnished with the equipment is prohibited by FCC and Industry Canada rules.

Canadian Computer Compliance

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Reglèment sur le material boilleur du Canada.

Canadian Spread Spectrum Radio Certification

▶ **NOTICE**

This device complies with RSS-210 of Industry Canada. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Canadian 2.4 GHz Radio License

▶ **NOTICE**

This device requires a radio license, unless it is installed totally inside a building. (Users must obtain this license.)

Une licence radio est requise pour ces dispositifs, sauf pour ceux installés tout à fait à l'intérieur d'un bâtiment. (Il faut que l'utilisateur obtienne cette licence.)

Telephone Installation Warning Notices

The following notices apply to equipment that may be connected to telephone lines or systems. For your personal safety, and to protect this equipment from potential electrical or physical damage, do NOT connect equipment to telephone lines or data communication equipment unless the following warnings have been read, understood, and complied with.

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using a telephone (other than cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.

Installation du téléphone : avertissements

Les avertissements qui suivent s'appliquent à tout équipement qui peut être branché aux lignes ou systèmes téléphoniques. Pour votre sécurité personnelle et pour protéger l'équipement de tout dommage électrique ou physique potentiel, NE PAS brancher un ordinateur tablette électronique ou ses périphériques aux lignes téléphoniques ou équipements avant que les avertissements suivants aient été lus, compris et observés :

- Ne jamais installer de câblage téléphonique pendant un orage électrique.
- Ne jamais installer de prise téléphonique dans un endroit humide à moins que la prise ait été spécifiquement conçue pour être utilisée dans les endroits humides.
- Ne jamais toucher les fils de téléphone ou de l'équipement terminal non isolés à moins que la ligne téléphonique n'ait été débranchée de l'interface réseau.
- User de prudence lors de l'installation ou de la modification de lignes téléphoniques.
- Éviter d'utiliser un téléphone (autre qu'un appareil téléphonique sans fil) pendant un orage électrique. Il pourrait y avoir un faible risque d'électrocution par la foudre.
- Ne pas utiliser le téléphone afin de signaler une fuite de gaz à proximité de la fuite.

CAUTION: **Intermec Technologies Corporation suggests you buy cables from us to connect with other devices. Our cables are safe, meet FCC rules, and suit our products. Other cables may not be tested. They may cause problems from electrostatic discharge or induced energy. Our warranties do not cover loss, injury, or damage from other cables.**

CONTENTS

SECTION 2

Quick Start

Configure the 21XX or 6710 Access Point

1. Set the following TCP/IP options:
   - IP Address *(default: 0.0.0.0)*
   - IP Subnet Mask *(default: 255.255.255.255)*
   - IP Router *(default: 0.0.0.0)*
2. Set the following radio options:
   - *2.4 GHz OpenAir radio:* LAN ID *(default: 0)*
   - *2.4 GHz OpenAir radio:* radio channel and subchannel to be unique for each closely located access point *(default: 1)*
   - *802.11 DS radio:* Network name *(default: INTERMEC)*
3. Set ARP Server Mode to No Flooding *(default: Disabled)*.
4. Use the default settings for the global flooding options.

For the 21XX UAP:

Global Flooding Option	Default
Multicast Flood Mode	Hierarchical
Multicast Outbound to Terminals	Enabled
Multicast Outbound to Secondary LANs	Set locally
Unicast Flood Mode	Disabled

For the 6710 Access Point:

Global Flooding Option	Default Multicast	Default Unicast
Inbound	Primary	Disabled
Outbound to Secondaries	Disabled	Disabled
Outbound to Stations	Disabled	Disabled

5. Do not set any filters *(default: no filtering)*.

   For complete information about access point options, refer to the *21XX Universal Access Point Technical Reference Manual* (P/N 067150) or the *6710 Access Point User's Guide* (P/N 961-047-081).

   For information about fine-tuning access point options for use with the 6400 TCP/IP client, see Section 2 in this user's guide.

Configure the 6400 TCP/IP Client

1. Open the 6400 computer's TCP/IP client DOS configuration menus by typing **`chgparms`** at the 6400 computer's DOS prompt. The following screen appears:

```
Chgparms v4.260
Sep 23 1999
10:33:24
802.11 DS or 2.4 Open Air version

1.  IP Config Parms
2.  DHCP Client
3.  SNMP Agent
4.  Advanced
5.  Exit
```

2. Select IP Config Parms to set these options:
   - *2.4 GHz OpenAir radio:* LAN ID, which must match the access point's LAN ID. *(Default: 0.)*
   - 6400 computer's IP address *(default: 000.000.000.000)*.
   - Subnet mask *(default: 255.255.255.255)*.
   - Router (optional) *(default: 000.000.000.000)*.
   - Domain server (optional) *(default: 000.000.000.000)*.
3. Optionally, set the DHCP Client or SNMP Agent, or both. *(Default for both options: Disabled.)*
4. Select Advanced to set the following:
   - Sleep timeout *(default: 24 seconds)*.
   - *2.4 GHz OpenAir radio:* Security ID, which must match the access point's security ID. (Default: INTERMEC for the 6710 Access Point, and no security ID for the 21XX UAP.)
   - *802.11 DS radio:* Network name, which must match the 21XX UAP's network name. (Default: INTERMEC.)
5. If you are also using 3270, 5250, or VT/ANSI terminal emulation, are using port 23 *(default)* for the host application, and are not using DHCP, do the following:
   a. Enter the host's IP address for the "host name" parameter in the 6400 TCP/IP client's terminal emulation menus. (To open the menus, press the yellow shift and blue shift keys.)
   b. Configure the other terminal emulation parameters as desired.

   If the host application is residing on a port other than 23, configure the 6400 TCP/IP client as follows:

   a. For the "host-table=" parameter in PCTCP.INI, enter the path of the host table file.

b. In the host table file, enter the following:

127.0.0.1 **LOCALHOST**
<host IP address> ***<variable>***
(For example: `192.168.5.40 x`*)*

c. For the "host name" parameter in the terminal emulation configuration menus, enter the variable located in the host table file followed by a space and then the port number on which the host application resides. (To open the menus, press the yellow shift and blue shift keys.) Example: **`x 1234`**

d. Configure the other terminal emulation parameters as desired.

For more information about 6400 TCP/IP client options, see Section 2 in this user's guide.

Verify the Network Configuration

▶ **NOTE:** *The access point must be properly configured and running before you can use the 6400 computer for communication.*

- *2.4 GHz OpenAir radio:* To verify that the 6400 computer is synchronizing with an access point, type **`proxstat`** at the 6400 computer's DOS prompt.
- Type **`chgparms`** to open the 6400 TCP/IP client DOS configuration menus. Verify all configuration settings.
- Perform **ping** tests:
  - Ping the access point from the server (host).
  - Ping the access point from the 6400 TCP/IP client.
  - Ping the server (host) from the 6400 TCP/IP client.
  - Ping the 6400 TCP/IP client from the server (host).

For more information about troubleshooting network connections, see Section 3 in this manual.

Section 1
Introduction

6400 TCP/IP Client Software

Following are part numbers for the 6400 TCP/IP client. Contact your Sales Representative for ordering information.

Item	2.4 GHz OpenAir	802.11 DS
6400 TCP/IP client:		
Flash	209-350-001	209-366-001
Disk kit	215-851-001	215-914-001
Terminal emulation over 6400 TCP/IP client:		
Flash	209-364-001	209-367-001
Disk kit	215-916-001	215-915-001

Product Overview

Summary

The 6400 TCP/IP client program contains products from the PC/TCP for DOS TCP/IP kernel and application suite from FTP Software, Inc.

Configuration files for the FTP Software TCP/IP kernel, radio, and 6400 computer are optimized for a wireless TCP/IP network environment. Following is an overview of the components of the 6400 TCP/IP client.

6400 TCP/IP Client Software

The 6400 TCP/IP client software contains DOS 5.0 and the 6400 BIOS. It also contains the driver for the radio.

TCP/IP Kernel

The 6400 TCP/IP client software provides the TCP/IP stack. The kernel is the basis of the networking software that passes information between connected hosts. The kernel manages such things as system resources, network hardware devices, and memory.

The kernel is a terminate-and-stay resident (TSR) program that loads into memory when you execute it and then returns a DOS prompt, letting you perform other tasks. Using the TSR kernel, you can run network programs in DOS.

The TSR kernel is stored in system memory and is always available. The kernel supports DIX Ethernet network connections.

Network Services

The following chart lists network services provided with the kernel.

Service	Description
FTP client	The FTP client transfers files between your 6400 computer and remote hosts running an FTP server.
TFTP client and server	The TFTP client and server transfers a single file between your 6400 computer and a remote TFTP server, without requiring authentication.

Network Utilities

The following chart lists network utilities provided with the kernel.

Utility	Description
DHCP and Bootp clients	Dynamic Host Configuration Protocol (DHCP) and Bootstrap protocol (Bootp) clients obtain IP addresses for your 6400 computer from a remote server.
Inet	Inet displays network statistics from the TCP/IP kernel, or unloads the TCP/IP kernel from memory.
Ping	Ping tests network connectivity by sending an Internet Control Message Protocol (ICMP) echo-request datagram to obtain an echo-response datagram from another host or gateway.
Setclock	Setclock obtains the date and time from a network time server, and sets your 6400 computer's date and time.
Snmpd	Snmpd lets other hosts and network management stations using the Simple Network Management Protocol (SNMP) examine 6400 computer statistics and configuration information.

Custom Applications

The Software Development Kit (SDK) for DOS by FTP Software, Inc., enables you to write custom client-server applications for the 6400 TCP/IP client. The kit contains comprehensive application libraries and sample source code. The SDK can be ordered from FTP Software. See "FTP Software Resources" later in this section for details about where you can find more information.

FTP Software Resources

Refer to the following web sites for more information about PC/TCP network software for DOS. Note that the URLs were current when this user's guide was printed.

FTP Software, Inc.: http://www.netmanage.com/index.asp

Maintenance and support:
http://www.netmanage.com/servicesnow/

Technical support:
http://supportweb.netmanage.com/index.asp

SDK for DOS: http://www.netmanage.com/products/pctcp5/

Structure of This User's Guide

This user's guide is organized as follows.

Section 2, "6400 TCP/IP Client"

Section 2 describes how to install and configure the 6400 TCP/IP client, configure the 21XX Universal Access Point (UAP) and 6710 Access Point, and share files. Section 2 also describes DOS command line options for network services and network utilities.

Section 3, "Troubleshooting Network Connections"

Section 3 discusses problems you might encounter when trying to connect with another host across a network.

Appendix A, "INTERSVR/INTERLNK Connection"

Appendix A shows how to connect your 6400 computer to a desktop or laptop personal computer to exchange files and edit the 6400 computer's configuration files.

Appendix B, "Tuning the 6400 TCP/IP Client"

Appendix B describes how to tune power management, kernel, and radio settings for optimal network performance.

Appendix C, "6400 TCP/IP Client Bar Code Scanning"

Appendix C briefly describes bar code scanning hardware and software for the TCP/IP client.

Appendix D, "RFC 1156, Section 6"

Appendix D is Section 6 of RFC 1156, *Management Information Base for Network Management of TCP/IP-Based Internets*.

Related Publications

To order a printed manual, contact your Intermec Sales Representative. Several online manuals are also available in Portable Document Format (PDF) on the Intermec web site. The list of online manuals is at:

http://www.intermec.com/manuals/english.htm

You must download the free Adobe Acrobat Reader to view the PDF manuals. Instructions are at:

http://www.intermec.com/manuals/manuals.htm#reader

Following are related INTERMEC manuals and part numbers (P/N).

21XX Universal Access Point Technical Reference Manual (P/N 067150)

This manual provides information about the features of the 21XX UAP, and how to install, configure, and troubleshoot it.

6710 Access Point User's Guide (P/N 961-047-081)

This user's guide describes how the 6710 Access Point operates on the Enterprise Wireless LAN (also called open wireless LAN) network. The guide also shows how to install and configure the access point.

INCAView for HP OpenView for Windows User's Guide (P/N 961-051-010)

This user's guide contains information on using INCAView to view network topology and device status.

Open Wireless LAN With HP OpenView for Windows User's Guide (P/N 961-051-009)

This user's guide describes how to install and use the OpenView application by Hewlett-Packard.

*PEN*KEY 6400 Computer Programmer's Reference Guide* (P/N 977-054-004)

This programmer's reference guide contains information about windows applications, power management, system and device support, and system messages for the 6400 computer. The guide also covers tool kits.

*PEN*KEY Model 6400 Hand-Held Computer User's Guide* (P/N 961-047-093)

This user's guide describes how to set up, operate, and maintain the 6400 computer.

Customer Support

Customer Support's on-going objective is to provide quality support to all of our customers worldwide.

Factory Service

If your unit is faulty, you can ship it to the nearest authorized Service Center for factory-quality service. The addresses and telephone numbers are included in the Warranty Card shipped with your product.

Customer Response Center

The Customer Response Center (technical support) telephone number is 800-755-5505 (U.S.A. or Canada) or 425-356-1799. The facsimile number is 425-356-1688. Email is *support@intermec.com*.

If you email or fax a problem or question include the following information in your message: your name, your company name and address, phone number and email to respond to, and problem description or question (the more specific, the better). If the equipment was purchased through a Premier Solution Partner, please include that information.

Web Site

The Customer Support File Libraries, including Hot Tips and Product Awareness Bulletins, are available on the Internet. New users start at the Intermec web site: www.intermec.com. Choose "Support," then "Product Support," then "Conference Area." Look on the main page for a link to register new customers.

Bulletin Board Service

The Customer Support Bulletin Board (BBS), maintained by the Norand Mobile Systems Division of Intermec Technologies Corporation, provides software and documentation:

- **Phone number:** 319-369-3515 (14.4 Kbps modem)
  319-369-3516 (28.8 Kbps modem)
- **Protocol:** Full duplex, ANSI or ANSI-BBS; 300 to 28,800 bps; v.32bis; 8 bits, no parity, 1 stop bit. *For high-speed modems, disable XON/XOFF and enable RTS/CTS.*

This is the same location available via the web site. If your web access uses high-speed phone lines, the web interface provides a faster response.

Wireless Client-Server Networking

Components

Wireless client-server networking components include the *client*, the *server*, and the 21XX UAP or 6710 Access Point.

The *client* is the communications program that runs on the 6400 computer. The *server* is the communications program that runs on a host attached to the wired network. The access point is a radio-enabled network device that relays information between the wireless client and the physical network.

The client program runs on your 6400 computer and communicates through the computer's radio over a wireless link to an access point. The access point then sends the client data to the server on the wired LAN.

The server communicates with the client by sending its data to the access point. The access point then forwards the server data to the client program via the 6400 computer's radio.

When access points are powered on, they begin communicating with each other to facilitate the best communication route from a wireless station to a server or host. The wireless access point community establishes a hierarchy called a *spanning tree*, a distributed data structure that optimizes the forwarding of messages to wireless stations.

The Enterprise Wireless LAN spanning tree dynamically organizes the network into a loop-free structure for efficient message forwarding. For connectivity, there must be at least one physical path (Ethernet or radio) to each node. If multiple possible paths exist between nodes, the network autoconfigures so the most efficient link is used. If a link is lost, the network dynamically reconfigures to provide an alternative path.

Characteristics Unique to Wireless Networking

Characteristics unique to wireless networking include roaming, out-of-range communications, and power management.

Roaming

The 6400 computer's radio can connect to only one access point at a time. As a user walks around with a 6400 computer, the computer's radio must detach from the previous access point and attach to a new, physically closer access point to maintain a communications link with good signal quality. The process of detaching and attaching is called *roaming*.

Roaming is automatic and invisible, and generally occurs in a fraction of a second. Neither the user nor the client program is aware of the radio roaming among access points. The communications link remains active and performance is not significantly affected while the 6400 computer is roaming.

Out-of-Range Communications

A wireless client-server network should be designed so that the 6400 computer is always in communications range of an access point. This ensures that the client and server can communicate with each other at any time. If a user takes a 6400 computer out of the range of an access point for a significant time, the client-server communication connection is put at risk.

Many client-server communication protocols include *keep-alive* or *watchdog* solicitation messages intended to determine the status of the computer on the other end. When a 6400 computer is out of range, it is unable to respond to (or initiate) these solicitation messages. The server (or client) concludes that the other end is no longer viable, and breaks the connection.

When the 6400 computer is in range again, the client and server are now out of synch and communications must be reestablished, either manually or through a relogin (depending on the server application). The best operational scenario is one where the 6400 computer is never out of range.

Power Management

The 6400 computer's radio requires significant energy to communicate. A radio can quickly consume the majority of a battery's charge if left on all the time.

Most client-server communications are intermittent. The 6400 computer's radio takes advantage of pauses by powering down during idle times to prolong battery life. The radio resumes full power when the client has data to send, or when the access point notifies the radio that it has data for the 6400 computer to receive.

The 6400 computer also has different power states it cycles through to conserve battery life. When the 6400 computer goes into its *off* (suspend) state, power to the radio is removed. The off state can put a client-server communication connection at risk, just as in the out-of-range situation.

The client and server may not be able to exchange their keep-alive and watchdog packets to indicate connection status. Generally, this is an issue only when the 6400 computer is turned off in the middle of a communications session, and if the 6400 computer is left off for a long period of time.

▶ **NOTE:** *Appendix B, "Tuning the 6400 TCP/IP Client," lists additional power states.*

Client-server communication sessions can generally withstand brief periods of being out of contact, especially during periods of idle communications. However, if one station is actively sending data to the other, and the 6400 computer is left off long enough, the connection eventually fails. The access point cannot wake up the 6400 computer if it has data to deliver from the server. The best operational scenario prevents the 6400 computer from being turned off during a transaction between it and the server.

Section 2

6400 TCP/IP Client

Installing the 6400 TCP/IP Client

Verifying System Requirements

Following are 6400 Computer hardware and software options. Contact your Sales Representative for configuration or ordering information. Configuration information is also listed in the Intermec Price Guide.

Hardware Options

Hardware options are 4 MB RAM/2 MB Flash and 8 MB RAM/4 MB Flash.

Radio Option

Radio options are 2.4 GHz OpenAir (RM180) and 802.11 Direct Sequence (DS).

6400 TCP/IP Client Software

Section 1 lists part numbers for the 6400 TCP/IP client Flash and disk kit.

▶ NOTE: *Appendix C, "6400 TCP/IP Client Bar Code Scanning," lists required hardware and software for bar code scanning.*

Preparing for an Upgrade

Before you can upgrade your 6400 TCP/IP client software, you must configure INTERLNK on a desktop or laptop. INTERLNK, a part of MS-DOS, is a device driver that connects your 6400 computer and personal computer through their serial ports. This connection enables you to exchange files and edit 6400 computer configuration files.

INTERSVR is the INTERLNK server and is a communications option on your 6400 computer. INTERLNK and INTERSVR are provided with DOS and shipped with your 6400 computer toolkit.

Appendix A, "INTERSVR/INTERLNK Connection," shows how to connect your 6400 computer to a personal computer. It also contains complete INTERSVR and INTERLNK installation instructions.

▶ **NOTE:** *The README.TXT file on the 6400 TCP/IP client disk also contains complete INTERSVR and INTERLNK installation instructions.*

Installing the 6400 TCP/IP Client

The 6400 TCP/IP client is preinstalled at the factory. If you need to install 6400 TCP/IP client Flash onto your 6400 computer or upgrade to another version, see Appendix A for instructions.

Configuring the 6400 TCP/IP Client

You can configure the 6400 TCP/IP client through its DOS configuration menus (page 2-3) or by manually editing its configuration files (page 2-15). You can also automatically assign IP addresses through DHCP and Bootp (page 2-46).

Using the DOS Configuration Menus

To access the configuration menus' Main Menu, type the following at the 6400 computer's DOS prompt:

```
C:\>chgparms
```

The Main Menu screen lists 6400 TCP/IP client options:

```
Chgparms v4.260
Sep 23 1999
10:33:24
802.11 DS or 2.4 Open Air version

1.  IP Config Parms
2.  DHCP Client
3.  SNMP Agent
4.  Advanced
5.  Exit
```

The Main Menu screen (and some other screens) also displays the command prompt (_). At the prompt, type the number of the option you want to view or modify and then press [ENT]. The following chart describes how to use 6400 TCP/IP client options.

Use	To
1. IP Config Parms	Set these configuration parameters: ▶ *2.4 GHz OpenAir radio:* LAN ID (default: 000) ▶ IP address (default: 000.000.000.000) ▶ Subnet mask (default: 255.255.255.255) ▶ Router (default: 000.000.000.000) ▶ Domain server (default: 000.000.000.000) Parameter descriptions start on page 2-5.
2. DHCP Client	Enable your 6400 computer (the client) to obtain IP addresses from a DHCP or Bootp server on the network. By default, DHCP is disabled. DHCP settings are described on page 2-8.
3. SNMP Agent	Enable other hosts and network management stations using SNMP to examine 6400 computer statistics and configuration information over the network. By default, SNMP is disabled. SNMP settings are described on page 2-9.
4. Advanced	Set these advanced parameters: ▶ *2.4 GHz OpenAir radio:* Security ID (default: INTERMEC) ▶ *802.11 DS radio:* Network name (default: INTERMEC) ▶ 6400's sleep timeout (default: 24 seconds) Parameter descriptions start on page 2-9.
5. Exit	Return to the DOS prompt.

Setting Configuration Parameters

The IP Config Parms screen shows the radio's configuration parameters:

2.4 GHz OpenAir Radio

```
Lan ID: 000
IP address:
000.000.000.000

subnet mask:
255.255.255.255

router:
000.000.000.000

domain server:
000.000.000.000
Press <ENT> to exit
```

802.11 DS Radio

```
IP address:
000.000.000.000

subnet mask:
255.255.255.255

router:
000.000.000.000

domain server:
000.000.000.000
Press <ENT> to exit
```

To modify parameter settings, do the following:

1. Read the descriptions on the following pages to determine the correct settings for your system.
2. Press arrow keys [▶] and [◀] to tab between parameters and the four 8-bit numbers in IP addresses.
3. Enter the correct settings for parameters by
   - pressing the appropriate number keys, or
   - pressing [▼] for a lower number and [▲] for a higher number.
4. Press [ENT] to exit the screen.

Lan ID

▶ **NOTE:** *LAN ID applies only to the 2.4 GHz OpenAir radio. The 802.11 DS 21XX UAP also has a LAN ID option, but the radio ignores it.*

The LAN ID (also called *domain*) is a number that logically isolates adjacent but independent open wireless LAN networks. The range is 0 to 15.

Your 6400 computer **must** have the same LAN ID as the 21XX UAP or 6710 Access Point. The default LAN ID for the 6400 computer and access point is 0.

IP Address

The IP address is the unique address locally assigned to your 6400 computer. Each 6400 computer must have a unique IP address.

The default setting of 000.000.000.000 disables the ability to use TCP/IP. Note the following:

- If the IP address is 000.000.000.000 *and* the DHCP client is enabled, this IP address is obtained through DHCP.
- If the IP address is 000.000.000.000 *and* the DHCP client is disabled, TCP/IP access to this 6400 computer is disabled.

Subnet Mask

A subnet is the bitwise logical AND of the IP address and subnet mask. For example, a typical subnet mask is 255.255.255.0. All IP addresses in the range xxx.xxx.xxx.0 to xxx.xxx.xxx.254 are members of the same subnet.

IP subnets partition traffic and are connected by routers. The subnet mask parameter indicates how many bits of the IP address represent a network number and how many indicate a host number. The default subnet mask for the 6400 computer is 255.255.255.255.

▶ **NOTE:** *The default subnet mask of 255.255.255.255 disables the use of TCP/IP. It is not a valid subnet mask.*

If you are using DHCP to automatically obtain an IP subnet mask for this 6400 computer, the subnet mask obtained from DHCP overrides the setting for the subnet mask parameter (and all other IP settings).

Router

▶ **NOTE:** *An IP router address is required only if your 6400 computer will communicate with IP hosts that can be reached only through a router.*

The router parameter identifies the default IP router used to forward data frames to addresses on another subnet. The default is 000.000.000.000, which disables the ability to exchange TCP/IP traffic with another subnet or network.

IP routers are usually configured so your 6400 computer only needs to know one router's address. This is true even if several routers on the segment connect to several other segments.

If you are using DHCP to obtain an IP router address, and the DHCP server specifies a default IP router, the server specification overrides the setting for the router parameter.

Domain Server

A Domain Name System (DNS) server maps IP addresses to hostnames. If your network uses a domain name server, enter the server's IP address for the domain server parameter. The default IP address is 000.000.000.000.

Enabling or Disabling the DHCP Client

Settings for the DHCP Client option are as follows:

```
1. Enable
2. Disable
3. Exit
```

Use	To
1. Enable	Enable the DHCP client, which allows your 6400 computer to retrieve an IP address, IP subnet mask, IP router address, and domain server address from a DHCP server. The 6400 computer ignores other configuration options. Note that if you enable DHCP, the 6400 computer's IP address is ignored. Enabling the DHCP client creates DHCPFILE.BAT, which contains DHCP.EXE.
2. Disable *(default)*	Disable the DHCP client. You must manually set IP addresses before the TCP/IP stack is enabled. Disabling the DHCP client deletes DHCPFILE.BAT.
3. Exit	Return to the Main Menu.

DHCP is described in detail on page 2-46, "Using DHCP and Bootp for IP Configuration."

Enabling or Disabling the SNMP Agent

Settings for the SNMP Agent option are as follows:

```
1. Enable
2. Disable
3. Exit
```

Use	To
1. Enable	Enable the SNMP agent and create SNMPFILE.BAT, which contains SNMPD.EXE.
2. Disable *(default)*	Disable the SNMP agent and delete SNMPFILE.BAT.
3. Exit	Return to the Main Menu.

SNMP is described in detail on page 2-59, "Configuring the SNMP Agent."

Setting Advanced Parameters

Configuration parameters for the Advanced option are as follows:

2.4 GHz OpenAir Radio

```
1. Security ID
2. 6400's Sleep Timeout
3. Exit
```

802.11 DS Radio

```
1. Network Name
2. 6400's Sleep Timeout
3. Exit
```

Security ID

▶ **NOTE:** *The security ID applies only to the 2.4 GHz OpenAir radio.*

2.4 GHz OpenAir radios have a privacy mechanism that prevents unauthorized radios from eavesdropping. This mechanism is a security ID used by every radio in the Enterprise Wireless LAN system.

The security ID prevents a 6400 computer from synchronizing with an access point with a different security ID. All access points and 6400 computers in the network **must** have the same security ID to communicate.

Security ID settings are:

```
1. INTERMEC
2. Custom
3. Exit
```

Use	To
1. INTERMEC *(default)*	Set the security ID to INTERMEC. This is also the default security ID for the 6710 Access Point. The default for the 21XX UAP is no security ID.
2. Custom	Enter a new security ID of 20 or fewer characters. The security ID is case sensitive; if the security ID for the access point is in uppercase, your 6400 computer's security ID must match and also be in uppercase.
3. Exit	Return to the Advanced menu.

For security reasons, you cannot display the current security ID.

Network Name

▶ **NOTE:** *Network name applies only to the 802.11 DS 21XX UAP.*

The network name prevents a 6400 computer from synchronizing with an access point with a different network name. All access points and 6400 computers in the network **must** have the same network name to communicate.

Options are:

```
1. INTERMEC
2. Custom
3. Exit
```

Use	To
1. INTERMEC *(default)*	Set the network name to INTERMEC. This is also the default network name for the 21XX UAP.
2. Custom	Enter a new network name of 32 or fewer characters. The network name is case sensitive; if the network name for the access point is in uppercase, your 6400 computer's network name must match and also be in uppercase. If you enter a custom name of ANY for the 6400 computer (must be uppercase), it attempts to attach to any 802.11 DS 21XX UAP that provides good communications quality, regardless of the access point's network name. Intermec does not recommend this method; instead, you should enter the access point's network name.
3. Exit	Return to the Advanced menu.

The Network Name option does not display the current name. To see the name, refer to NET.CFG.

6400's Sleep Timeout

The sleep timeout is the number of seconds it takes an inactive 6400 computer to enter autosuspend mode. The current time appears on the Sleep Timeout screen:

```
Current sleep time =
   24 seconds
New sleep time:
   ______ seconds
Press enter to set
```

The default sleep timeout is 24 seconds. The range is 0, or 4 to 1024 in increments of 4 seconds. A value of 0 disables the sleep timeout. A new sleep timeout is used immediately after you exit the menu. It is also preserved after you reboot the 6400 TCP/IP client.

Because the 2.4 GHz OpenAir radio periodically generates background radio attachment activity (which resets the autosuspend timer about every 30 seconds), a sleep timeout of 25 seconds or more will not allow your 6400 computer to autosuspend. For your 6400 computer to autosuspend, set the sleep timeout to 24 seconds or less if the 6400 computer has a 2.4 GHz OpenAir radio. (The 802.11 DS radio does not allow autosuspend.)

Configuring TE/IP

For 3270, 5250, or VT/ANSI terminal emulation (TE) over TCP/IP, the host is usually specified by an IP address (unless you are using a domain name server). However, often the 6400 TCP/IP client needs to know the port on which the host application is residing. The default port number (23) is automatically assumed in TE/IP.

If the application is residing on the default port (23), you need to enter only the host IP address for the terminal emulation program's "host name" parameter. If the application resides on a port other than 23, specify the IP address and other port as follows.

▶ **NOTE:** *If you are using DHCP, you do not need to specify a host IP address and a port number for the host name parameter.*

1. Configure the 6400 TCP/IP client with an IP address, subnet mask and, if necessary, a router address. If your network uses a domain name server, configure an IP address for it. For more information about setting IP addresses, see pages 2-6 through 2-7.
2. Open the 6400 TCP/IP client's PCTCP.INI file. In the [pctcp kernel] section, enter the following:

   `host-table = c:\<pathname>\<host table filename>`

   For example:

   `host-table=c:\hosts`

3. Open the 6400 TCP/IP client's host table file and enter the following:

   ```
   127.0.0.1              LOCALHOST
   <host IP address>      <variable>
   ```

   For example:

   ```
   127.0.0.1              LOCALHOST
   192.168.5.40           x
   ```

4. Open the 6400 TCP/IP Client's terminal emulation menus by pressing the yellow shift key and then the blue shift (MENU) key. For help, refer to the *PEN*KEY Model 6400 Hand-Held Computer User's Guide*.

5. Go to the host name parameter. Enter the variable located in the host table file followed by a space and then the port number to which the terminal connects to the host. For example:

   ```
   x 1234
   ```

▶ **NOTE:** *You cannot enter the host IP address, a space, and the port number for the host name parameter because its field is not long enough.*

6. Configure the other terminal emulation parameters as desired.

Editing the Configuration Files

To set up your 6400 computer 6400 TCP/IP client by manually editing its configuration files, see the following procedures. Note that to edit the files, you must have INTERLNK and INTERSVR configured on the personal computer and 6400 computer. For instructions, see Appendix A, "INTERSVR/INTERLNK Connection."

Setting the LAN ID

▶ **NOTE:** *LAN ID applies only to the 2.4 GHz OpenAir radio.*

1. Use a text editor to open NET.CFG.
2. In NET.CFG, the LAN ID is called DOMAIN. Modify the setting for the DOMAIN option.

For more information about the LAN ID, see page 2-6.

Setting IP Addresses

1. Use a text editor to open PCTCP.INI.
2. Modify the settings for the following parameters, located in the [pctcp *interface n*] section:

   ```
   ip-address=
   subnet-mask=
   router=
   ```
   (if applicable)

3. If applicable, modify the following parameter, located in the [pctcp addresses] section:

   ```
   domain-name-server=
   ```

For more information about IP addresses, see pages 2-6 through 2-7.

Enabling or Disabling the DHCP Client

To execute a DHCP request, type the following at the DOS prompt:

```
C:\>dhcp
```

▶ **NOTE:** *You can automatically execute a DHCP request when you start your 6400 computer by entering the **dhcp** command in AUTOEXEC.BAT. The **dhcp** command must be located after ETHDRV.EXE.*

To disable DHCP, reboot your 6400 computer or type the following command at the DOS prompt:

```
C:\>dhcp -u
```

For more information about the DHCP client, see page 2-8.

Enabling or Disabling the SNMP Agent

To enable the SNMP agent, type the following at the DOS prompt:

```
C:\>snmpd
```

▶ **NOTE:** *You can automatically enable the SNMP agent when you start your 6400 computer by entering the **snmpd** command in AUTOEXEC.BAT. The **snmpd** command must be located after ETHDRV.EXE.*

To disable the SNMP agent, reboot your 6400 computer. For more information about the SNMP agent, see page 2-9.

Setting the Security ID

▶ **NOTE:** *Security ID applies only to the 2.4 GHz OpenAir radio.*

1. Type the following at the DOS prompt:

   `C:\>`**`proxstat -s<security_id>`**

   where <*security_id*> is the set of characters to be used as the security ID. If you do not specify a setting for the **-s** switch, the security ID is set to "" (deleted).
2. Reboot your 6400 computer for the change to take effect.

For more information about the security ID, see page 2-10.

Setting the Network Name

▶ **NOTE:** *Network name applies only to the 802.11 DS radio..*

1. Use a text editor to open NET.CFG.
2. Modify the setting for WaveLAN_Network_Name (default: "INTERMEC"). Note that the network name is in quotes.

For more information about the name, see page 2-11.

Setting the Sleep Timeout

1. Use a text editor to open AUTOEXEC.BAT.
2. Modify the /D switch for ELANCFG. Following is a sample command line:

   `elancfg /V1 /T2 /D24 /L1 /H1`

   The range is 0, or 4 to 1024 in increments of 4 seconds. A value of 0 disables autosuspend.
3. Reboot your 6400 computer for the change to take effect.

For more information about sleep timeout, see page 2-12.

Using DHCP or Bootp for IP Addressing

To automatically assign IP addresses using DHCP or Bootp, see “Using DHCP and Bootp for IP Configuration” on page 2-46.

Configuring the Access Point

The 6400 TCP/IP client is supported with the following versions of the Enterprise Wireless LAN access point system software.

Access Point	Version
21XX UAP, 2.4 GHz OpenAir radio	All releases
21XX UAP, 802.11 DS radio	3.92
6710 Access Point, 2.4 GHz OpenAir radio	1.32 or greater

The following pages briefly describe some access point configuration options. For complete information, refer to the *21XX Universal Access Point Technical Reference Manual* (P/N 067150) or the *6710 Access Point User’s Guide* (P/N 961-047-081).

Access Methods

The access point can be configured locally through its diagnostics port, or remotely through Telnet or a Web browser. Remote access requires an IP address that must be initially set through the access point’s diagnostics port.

IP Addresses

The access point can be configured with an IP address, subnet mask, and IP router address. It can also be configured to automatically obtain IP addresses through DHCP or Bootp. The default setting for all IP addresses is 0.0.0.0.

If the access point's IP address is 0.0.0.0 and its DHCP client is enabled, the access point retrieves IP addresses and the lease expiration time from a DHCP or Bootp server.

LAN ID

▶ **NOTE:** *The LAN ID applies only to the 2.4 GHz OpenAir radio.*

The access point LAN ID is a number that logically isolates adjacent but independent open wireless LAN networks. You should change the default of 0 to another number to avoid a potential conflict with an adjacent network. The LAN ID for all access points and 6400 computers in the same network must match.

Channel and Subchannel

▶ **NOTE:** *Subchannel does not apply to the 802.11 DS 21XX UAP.*

The channel sets the radio hopping sequence. The subchannel enables access points to share the same channel without receiving another access point's frames. To maximize the available bandwidth, the channel and subchannel should be unique for each closely located access point. The default setting for the channel and subchannel is 1.

ARP Server Mode

ARP (Address Resolution Protocol) Server Mode converts multicast ARP requests to unicast ARP requests for stations in the forwarding database, which can significantly improve wireless network performance in busy IP networks.

By default, ARP Server Mode is disabled in the access point. For 6400 TCP/IP client communications, ARP Server Mode must be enabled. The enabled setting of No Flooding is recommended for almost all installations.

► **NOTE:** *Page 3-20 in Section 3 contains information about troubleshooting ARP Server Mode.*

Flooding

To allow performance tuning, the access point provides separate flooding control options for unicast and multicast frames. Access points serving as designated bridges connecting wired LAN segments may be configured to use different flooding settings than access points serving only 6400 computers.

For 6400 TCP/IP client communications, it is recommended that you use the access point's default settings for multicast and unicast frames types, as shown in the following charts.

For the 21XX UAP:

Global Flooding Option	Default Setting
Multicast Flood Mode	Hierarchical
Multicast Outbound to Terminals	Enabled
Multicast Outbound to Secondary LANs	Set locally
Unicast Flood Mode	Disabled

For the 6710 Access Point:

Global Flooding Option	Default Multicast	Default Unicast
Inbound	Primary	Disabled
Outbound to Secondaries	Disabled	Disabled
Outbound to Stations	Disabled	Disabled

▶ **NOTE:** *Page 3-19 in Section 3 contains information about troubleshooting flooding levels.*

Filtering

The access point's Ethernet port can be configured to support preconfigured and custom input filters. Setting filters prevents unnecessary traffic from the wired LAN from being forwarded onto the wireless medium. This is important because common wireless technologies operate at data rates below Ethernet speeds.

By default, the access point is configured for no filtering. For 6400 TCP/IP client communications, it is recommended that you not set any filters.

▶ **NOTE:** *Page 3-19 in Section 3 contains information about troubleshooting filtering levels.*

Verifying Your Network Configuration

To verify that your network configuration is properly set, do the following:

- *2.4 GHz OpenAir radio:* Use the PROXSTAT.EXE utility to verify synchronization with an access point
- *802.11 DS radio:* Use the LSTAT.EXE utility to display the radio's firmware versions and current radio operating statistics
- Verify your 6400 TCP/IP client configuration settings.
- Perform **ping** tests.

The access point must be properly configured and running before you can use your 6400 computer for communication.

Using PROXSTAT.EXE

▶ **NOTE:** *PROXSTAT.EXE is supported only on the 2.4 GHz OpenAir radio.*

To verify synchronization with a 2.4 GHz OpenAir access point, type the following at your 6400 computer's DOS prompt:

```
C:\>proxstat
```

PROXSTAT displays a screen similar to the following:

```
Access Point:
    ↑ In Synch
    Signal:   <High, medium, or low>
    AP MAC:   <Unique MAC address>
    Master:

Radio:
    LAN ID:   <Range: 0 to 15>
    ROM:   <Version>
    MAC:   <Unique MAC address>
    Sleep Time:   <Seconds>
```

The screen contains the following information:

- A message that indicates whether your 6400 computer is "In Synch" or "Out of Synch" with the access point
- A high, medium, or low signal strength
- The unique MAC address of the radio in the access point with which your 6400 computer is synchronized
- The LAN ID, ROM version, and unique MAC access of the radio in your 6400 computer
- A radio sleep time, which is not related to the autosuspend sleep time

If PROXSTAT.EXE displays the message "↓ Out of Synch," ensure your 6400 computer's LAN ID matches the access point's LAN ID. If the LAN IDs match, ensure your 6400 computer's security ID matches the access point's security ID.

To modify your 6400 computer's LAN ID:

Use the 6400 TCP/IP client DOS configuration menus to modify the IP Config Parms/Lan ID parameter (page 2-6).

Or, modify the setting for the DOMAIN option in NET.CFG (page 2-15).

To modify your 6400 computer's security ID:

Use the 6400 TCP/IP client DOS configuration menus to modify the Advanced/Security ID parameter (page 2-10).

Or, use the PROXSTAT.EXE utility (page 2-17).

To modify the access point's LAN ID or security ID:

For instructions, refer to the *21XX Universal Access Point Technical Reference Manual* (P/N 067150) or the *6710 Access Point User's Guide* (P/N 961-047-081).

Using LSTAT.EXE

▶ **NOTE:** *LSTAT.EXE is supported only on the 802.11 DS radio.*

To display the 802.11 DS radio's firmware versions and current operating statistics, type the following commands at your 6400 computer's DOS prompt:

```
C:\>lsl
C:\>wvlan43
C:\>lstat
```

A screen similar to the following appears:

```
PRI: v4.0
SEC: v4.52

RFLink: Excellent
SNR:    48dBm
SSID:   INTERMEC
BSSID:  00601d040f96
TXRate: 2Mb/s std
```

For complete information about each field, refer to the *6400 Computer TCP/IP Client Technical Reference* (P/N 977-054-008).

Verifying 6400 TCP/IP Client Settings

To verify 6400 TCP/IP client settings through the DOS configuration menus, open the menus by typing the following at the DOS prompt:

```
C:\>chgparms
```

Navigate through the menus and ensure that

- *2.4 GHz OpenAir radio:* your 6400 computer has the same LAN ID and security ID as the access point.
- *802.11 DS radio:* your 6400 computer has the same network name as the 21XX UAP.
- the IP addresses for the 6400 computer and subnet mask are properly set.
- the IP addresses for the router and domain server are properly set *(if applicable)*.
- the DHCP client and SNMP agent are enabled or disabled as appropriate.

To check 6400 TCP/IP client settings in your 6400 computer's configuration files, do the following:

- Use a text editor to open PCTCP.INI. Ensure the following parameters are properly set:

  ```
  ip-address=
  subnet-mask=
  router= (if applicable)
  domain-name-server= (if applicable)
  ```

- Use a text editor to open NET.CFG.

  2.4 GHz OpenAir radio: Ensure your computer has the same LAN ID and security ID as the access point. Note that in NET.CFG, the LAN ID is called DOMAIN.

  802.11 DS radio: Ensure your computer has the same network name as the 21XX UAP.

- Use a text editor to open AUTOEXEC.BAT. The /D switch for ELANCFG sets your 6400 computer's sleep timeout. The default is 24 seconds. The range is 0, or 4 to 1024 in increments of 4 seconds. A value of 0 disables the sleep timeout. Ensure the /D switch is properly set.

  If you want the **dhcp** command to run when you start your 6400 computer, ensure the command is entered in AUTOEXEC.BAT, *after* the ETHDRV.EXE command.

  If you want the **snmpd** command to run when you start your 6400 computer, ensure the command is entered in AUTOEXEC.BAT, *after* the ETHDRV.EXE command.

Performing Ping Tests

Do the following in the order given:

1. Ping the access point from the server (host).
2. Ping the access point from the 6400 TCP/IP client.
3. Ping the server (host) from the 6400 TCP/IP client.
4. Ping the 6400 TCP/IP client from the server (host).

Usage and command line options for the **ping** command start on page 2-34.

6400 TCP/IP Kernel Command Summaries

The TCP/IP kernel refers to the TCP/IP communications stack. The following pages describe usage and command line options for these DOS commands, included with the kernel: **inet**, **ethdrv**, **ping**, and **setclock**.

Related commands are **bootp** (page 2-56), **dhcp** (page 2-58), and **snmpd** (page 2-63).

Inet

inet [**arp**] [**debug**] [**pap**] [**ppp**] [**route**] [**slip**] [**stats**] [**tcp**] [**version**] [**unload**]
inet [**config** [**advanced | security**]]
inet [**ipcp** (**stats | config**)]
inet [**lcp** (**stats | config**)]

The **inet** command displays network statistics from the kernel, or unloads the kernel from memory.

arp Displays the current contents of the kernel's ARP cache.

config [advanced | security]

Displays configuration information and kernel activity. You may supply one of the following arguments:

advanced Shows advanced kernel configuration parameters.

security Shows kernel security configuration parameters.

▶ ***NOTE: Security** is not related to the 2.4 GHz OpenAir radio's security ID or the 802.11 DS radio's network name.*

debug	Displays information about packet receipt and transmission, interrupts, ARP statistics, etc. The **debug** argument also displays the physical address of the interface. This argument is useful when troubleshooting network performance, tuning the kernel, and analyzing remote transfers.
route	Displays the current contents of the kernel's routing cache. The routing cache contains the information learned through ICMP Host Redirect packets. The routing cache holds 16 entries.
stats	Displays network statistics about the network interface. The statistics include the name of the interface, its network (IP) address, the subnet mask, and the total number of packets sent out and received on this interface. **Inet stats** also displays a number of TCP, IP, ICMP, and User Datagram Protocol (UDP) counters, including bad incoming packets and messages broken down by type.
tcp	Displays the contents of the kernel's TCP connections table, a set of statistics for each active connection.
unload	Unloads the kernel from memory. If you use **inet unload**, you must use **ethdrv** to reload the kernel into memory. See the **ethdrv** command for details (page 2-31).
version	Displays the version number of the active kernel, not the version number of the **inet** command.
-?	Displays and explains the usage line of this command.
-version	Displays the version and patch level of this command. Refer to this information if you call Technical Support.

EXAMPLE 1: To display configuration information about your kernel, enter:

```
C:\>inet config
kernel active since: Thu  March 30 17:37:15 1997
1 TCP connections open/listening of 4 allowed
0 UDP connections in use, of 6 allowed
3 IP connections in use, of 7 allowed
0 Global and 1 local network descriptors active
Using 255.255.255.255 as IP broadcast address.
Domain: abc.com
Hosttable file:  c:\norand\host.tab
Router(s); 128.127.50.10
Domain name completion list(s); <None Configured>
Domain name server(s): 128.127.50.105
Default TCP window size: 2048
Default low window size: 0
Chain vector: 0xb
MAC Address: 00 00 f6 18 50 46
Packet Driver Class: 1
```

EXAMPLE 2: To display advanced configuration information, enter:

```
C:\>inet config advanced
Time to Live: 64
Type of service: Normal
Precedence:  Routine
Will do lax precedence matching.
Maximum Transmissions Unit (MUT):  1480
Round trip time multiplier: 1
Kernel is not using expanded memory.
```

EXAMPLE 3: To display the current contents of your kernel's ARP cache, enter:

```
C:\>inet arp
ARP cache:
  128.127.50.137: 00de2000037ff  expires: 773 sec.
  128.127.50.105: 08004C002C6A   expired
```

EXAMPLE 4: To display statistics about the network interface, enter:

```
C:\>inet stats
Interface  address       subnet mask  pkts in  pkts out  errs in errs out
ifcust0   128.127.50.141 255.255.0.   157057   2555      0       0
Kernel TCP stats: 2530 pkts sent, 1869 pkts rcvd, 0 bad checksums
   943197 bytes sent, 138587 bytes rcvd, 56 rexmits, 52 duplicate pkts
   0 protocol errs, 0 resets, 0 timeouts
Kernel IP stats:  2537 pkts sent, 137419 pkts rcvd, 0 frags, 5 err
   5 protocol errs, 0 timeouts, 0 bad checksums, 0 security errs
Kernel UDP stats:  6 pkts sent, 6 pkts rcvd, 0 no  port listening
   0 bad checksums, 0 truncated rcvs
Kernel ICMP stats:  1 pkts sent (0 errs), 1 pkts rcvd (0 bad)
   DestUn:  0 sent, 0 rcvd, ParamProb:  0 sent, 0 rcvd
   TimeEx:  0 sent, 0 rcvd, Redir:  0 rcvd, SourceQ:  0 rcvd
```

***SEE ALSO*:** **Ethdrv** (page 2-31) and **Ping** (page 2-34).

Ethdrv

ethdrv [**-B**] [**-b** *broadcast_addr*] [**-i** *interrupt*] [**m**]
[**-p** *lg_pkt_count*] [**-s** *sm_pkt_count*]
[**-t** *max_tcp_conn*] [**-u** *max_udp_conn*]

The **ethdrv** command loads the TSR kernel into memory. Use **inet unload** to unload the kernel from memory.

The kernel is the central part of the network software. Loading the TSR kernel lets you use TCP/IP applications. The **ethdrv** TSR kernel supports DIX Ethernet.

The TSR kernel supports upper memory (UMB) and expanded memory loading options that you can specify on the command line or in the [pctcp kernel] section of PCTCP.INI. (The kernel loads its code and data segments into upper memory by default.)

The size of the kernel varies, depending on the driver, the command line, and configuration options you select. When you load the kernel, it displays a report of its memory usage. Using **ethdrv** without arguments results in a configuration that uses a moderate amount of memory, and is adequate for most users.

Kernel command line options override configuration parameter settings in the [pctcp kernel] section of PCTCP.INI.

-B	Specifies that Berkeley UNIX-type urgent pointers are used. Use this type of out-of-band urgent pointer when communicating with Berkeley UNIX hosts. Without this option selected, RFC 1122 urgent pointers are used; this is the default. RFC 1122 is *Requirements for Internet Hosts − Communication Layers*.

-b *broadcast_addr* Specifies a broadcast address other than 255.255.255.255. Other useful values are:

net_addr.**255**
net_addr.subnet_addr.**255**
net_addr.**0**
net_addr.subnet_addr.**0**

Net_addr and *subnet_addr* are your network and subnet addresses. Broadcast addresses that use the **0** value are unusual and generally used by older networks.

▶ ***NOTE:*** *If you use this mechanism, you may have problems with your network. FTP does not guarantee performance or compatibility with other TCP/IP implementations.*

-m Allows the kernel to use expanded memory if a properly configured expanded memory manager is also running. This option overrides the default `use-emm=no` parameter in the [pctcp kernel] section of PCTCP.INI.

-p *lg_pkt_count* Specifies the number of large packet buffers to reserve when loading the kernel into memory. The size of a large packet is equivalent to the Maximum Transmission Unit (MTU) allowed in your network. Default: 5 or the number of TCP connections plus 1 (whichever is larger).

This option overrides the `large-packets=`*`number`* setting in the [pctcp kernel] section of PCTCP.INI.

-s *sm_pkt_count*	Specifies the number of small packet buffers to reserve when loading the kernel into memory. Typically, small packets carry protocol or other handshaking data between systems, and large packets carry application data. Default: 5 or the number of TCP connections plus 1 (whichever is larger). This option overrides the `small-packets=`*`number`* setting in the [pctcp kernel] section of PCTCP.INI.
-t *max_tcp_conn*	Specifies the maximum number of simultaneous TCP connections to allow. The maximum number of TCP connections is 64. Default: 4.
-u *max_udp_conn*	Specifies maximum number of simultaneous UDP connections to allow. Default: 4.
-?	Displays and explains the usage line of this command.
-version	Displays the version and patch level of this command. Refer to this information if you call Technical Support.

EXAMPLE 1: To unload the TSR, enter:

```
C:\>inet unload
```

EXAMPLE 2: To load the DIX Ethernet TSR kernel TSR into conventional memory with 8 TCP and 8 UDP connections, enter:

```
C:\>ethdrv -t 8 -u 8
```

***SEE ALSO*:** **Inet** (page 2-27).

Ping

ping [*options*] *host*
ping [**-?** | **-version**]

Use **ping** to determine if a host is active and to isolate host connection problems. **Ping** sends an echo request to another host and waits for a response, using ICMP.

Ping reports success with a "Host responding" message followed by statistics for the host that initiated the connection. The command may also report failure with a "Ping failed" or "Cannot resolve hostname" message followed by statistics about the host that initiated the connection.

Options **-j**, **-k**, **-o**, **-r**, **-s**, and **-x** add IP options to the packet header. Options can be combined, and space is allotted to a variable length option depending on what else is selected. Variable length options take up three bytes of header space in addition to whatever is used up by the data. If the selected combination totals no more than 40 bytes, **ping** prints an error message and fails.

When typing options on the command line, leave a space between the option and any values or arguments that correspond to it.

When using **ping** with a 6400 computer, a useful command line option for minimal output is **-z**. This option enables you to easily view statistics on your 6400 computer's small display. You can add **-n 5** to generate five pings in succession. An example is on page 2-39.

-d [*bytes*]	Displays header and debugging information about the incoming packet. Use the *bytes* value to specify the number of bytes to display in hexadecimal notation. If you specify the **-t** option with the **-d** option, the program repeatedly contacts the target host and displays the first input packet along with a changing display of the number of echoes.

-d# [*bytes*]	Displays header and debugging information about the outgoing packet. Use *bytes* to specify the number of bytes to display in hexadecimal notation. If you specify **-t** with the **-d#** option, the program repeatedly contacts the target host and displays the first output packet along with a changing display of the number of echoes. If you specify both the **-d#** and **-d** options, **ping** displays information for the outgoing packet first.
-e	Cancels any configured IP extended security levels or authority that **ping** would otherwise insert.
host	Specifies the name or Internet address of the remote host.
-i *value*	Sets IP Time-to-Live (TTL) value on the outgoing packet and displays TTL value for the incoming packet. The range is 1–255. Default: 64.
-j *dest1 ... destn*	Turns on the IP Loose Source Routing option, which lets the packet pass through unlisted routers between destinations. Each destination is the IP address of a router through which the packet must pass on the way to the final destination. The **-j** option cannot be used with the **-k** option.
-k *dest1 ... destn*	Turns on the IP Strict Source Routing option, which does not let the packet pass through unlisted routers between destinations. Each destination is the IP address of a router through which the packet must pass on the way to the final destination. The **-k** option cannot be used with the **-j** option.
-l *length*	Sets the length in bytes of data in a packet. Default: 256. You can use this option to send longer packets through the network if the transport to which your 6400 computer is connected supports a data length greater than 256 bytes.

-n times
Sends the specified number of echo requests and then stops. By default, **ping** sends only one echo request. The **-t** option overrides this option.

-o
Turns on IP No-Op option, which has no effect on the transmission but is sometimes used for alignment purposes. It uses 1 byte of option space.

-p *precedence*
Sets the IP Precedence level. The variable *precedence* is a number in the 0–7 range. This option overrides any Precedence options configured in PCTCP.INI. The IP precedence levels and descriptions are as follows:

0	Routine	4	Flash override
1	Priority	5	CRITIC/ECP
2	Immediate	6	Internetwork control
3	Flash	7	Network control

-Q
Turns on Trace Route option, which performs like the **-q** option except that IP addresses are not translated to domain names.

-q
Turns on the Trace Route option. The option increments the TTL to identify all of the routers encountered when trying to reach the target host, and denotes each router by its IP address and domain name. The option displays the number of hops required to reach the target host. If it does not reach a host after 96 hops, **ping** times out.

-r
Turns on the IP Record Route option.

-t
Continuously sends echo requests to the target host, each time waiting for a response before sending the next request. When in this request-response-request loop, **ping** reports all echo failures and an incremental summary of trials and successes. To exit from this command, type **q**. The **-t** option overrides the **-n** option, if specified.

-v *type*

Requests an IP Type of Service option. The variable *type* is a number in the 0–15 range. This option overrides any Type of Service options configured in PCTCP.INI. The service depends on the router and is not guaranteed; therefore, requesting this option may have no effect on the performance of **ping**.

The value and description for each valid *type* are as follows:

0 Normal
1 Low cost (LC)
2 High reliability (HR)
3 LC, HR
4 High throughput (HT)
5 LC, HT
6 HR, HT
7 LC, HR, HT
8 Low delay (LD)
9 LC, LD
10 HR, LD
11 LC, HR, LD
12 HT, LD
13 LC, HT, LD
14 HR, HT, LD
15 LC, HR, HT, LD

-w *seconds*

Specifies a number of seconds to wait for a response before giving up. The range for *seconds* is 1–32767. Default: 6.

-x

Turns on the IP timestamp option. All routers that implement Timestamp stamp the packet when encountered.

-x 1

Specifies that each time stamp is preceded by the IP address of the recording entity. Each recorded time stamp takes 8 bytes of option space.

-x 3 *dest1...destn*	Specifies that time stamps will be filled in only by designated routers (including the final host on the route). Each recorded time stamp takes 8 bytes of option space.
-z	Specifies quiet mode, which reports success or failure rather than full statistics.
-?	Displays and explains the usage line of this command.
-version	Displays the version and patch level of this command. Refer to this information if you call Technical Support.

EXAMPLE 1: To send an echo request to the host lee.xyz.com and display network debugging information, enter:

```
C:\>ping lee.xyz.com
host responding, time = 25 ms
Debugging information for interface ifcust Addr(6): 00 00 c0 ea 93 10
interrupts: 49 (0 receive, 0 transmit)
packets received: 42, transmitted: 7
receive errors: 0, unknown types: 14
          runts: 0, aligns: 0, CRC: 0, parity: 0, overflow: 0
          too big: 0, out of buffers: 0, rcv timeout: 0, rec reset: 0
transmit errors: 0
          collisions: 0, underflows: 0, timeouts: 0, resets: 0
          lost crs: 0, heartbeat failed: 0
ARP statistics:
arps received: 9 (7 requests, 2 replies)
          bad: opcodes: 0, hardware type: 0, protocol type: 0
arps transmitted: 2 (2 requests, 0 replies)
3 large buffers; 2 free now; minimum of 0 free
3 small buffers; 3 free now; minimum of 1 free
```

EXAMPLE 1: To easily view statistics on your 6400 computer's small display, enter:

```
C:\>ping -z -n 5 godzilla.xyz.com
host responding, time = 25 ms
host responding, time = 25 ms
host responding, time = 25 ms
host responding, time = 25 ms
host responding, time = 25 ms

Pinged host 5 times with 0 failures, round-trip
average (ms) = 25
```

EXAMPLE 2: To trace the route an echo request takes to get to a target host, enter:

```
C:\>ping -q 128.127.53.118
hop 1:128.127.55.10    router-55.xyz.com
hop 2:128.127.52.7     router-52.xyz.com
hop 3:128.127.53.11    router-53.xyz.com

Target (128.127.53.118) reached on hop 4,
round-trip time 160 ms.
```

***SEE ALSO*:** **Inet** (page 2-27).

Setclock

▶ **NOTE:** *This command works only with network time servers.*

setclock [*time_server*]

The **setclock** command obtains the date and time from a network time server, and sets your 6400 computer's time and date.

time_server	Specifies the hostname or IP address of the remote host that provides UDP time service.

Sharing Files

The following pages describe usage and command line options for these DOS commands:

- **Ftp**
- **Tftp**

Ftp

ftp [**-d**] [**-u** *userid password*] [**-p** *port_no*] [*host*] [*command*]

The **ftp** command transfers files between your 6400 computer and remote hosts running an FTP server. This command is the easiest to use for transferring files between hosts.

command	Specifies an **ftp** interactive command.
-d	Displays all **ftp** network commands and responses sent over the **ftp** control connection. This option displays your password after you enter it.
host	Specifies the hostname or IP address of the remote host.
-p *port_no*	Specifies a port number on the remote host.
-u *userid password*	Logs you in to the remote host using your username and password.

Setting Up and Ending Ftp Sessions

Use	To
acct [*account_name*]	Change to another account.
bye, **exit**, or **quit**	End session and exit from **ftp**.
close or **disconnect**	Close a connection without leaving the FTP client.
help or **?** [*command*]	Display help from the FTP server.
login or **user** *user*	Restart the login procedure.
open [*hostname*] [*port_no*]	Open a connection after FTP client has been started or after disconnecting from an FTP server.
take *local_file*	Read commands from a local file.

Debugging Ftp

Use	To
abort	Stop an FTP service command.
debug or **verbose** (**on** | **off**)	Set debugging either on or off.
quote or **server** *command*	Send the command verbatim.
stat	Display the state of remote host.
version	Display the version and patch level of the **ftp** command.

Executing DOS Commands From Ftp

Use	To
! [command]	Switch to a nested DOS command interpreter or execute a single DOS command.
exit	Return to the **ftp** session from a nested DOS command interpreter.

Transferring Files With Ftp

Use	To
allocate *n*	Allocate storage for a forthcoming transfer.
append *local_file* [*remote_file*]	Append local file to remote file.
delete *filename*	Delete remote file.
get *remote_file* [*local_file*]	Transfer a file to your 6400 computer.
iget [*remote_file local_file*]	Transfer a file to your 6400 computer using image (binary) type.
iput [*local_file remote_file*]	Transfer a file to the remote host using image type.
mdelete *pattern_wildcard*	Delete multiple remote files.
mget *pattern_wildcard*	Transfer multiple files to your 6400 computer.
mput *pattern_wildcard*	Transfer multiple files to the remote machine.
passive	Transfer the next file in passive mode.
put *local_file* [*remote_file*]	Transfer a file to the remote host.
reinit	Reset a connection to its initial state following a file transfer.
rename [*old_name new_name*]	Rename a remote file.
show *filename*	Display a remote file.
site free	Find out how many bytes of space are available on the FTP server.
tget [*remote_file local_file*]	Transfer a file to your 6400 computer using tenex type.
tput [*local_file remote_file*]	Transfer a file to the remote host using tenex type.

Working in Directories

Use	To
cd or **fcd** *path*	Change current remote directory.
dir or **fdir** [*argument* [*filename*]]	List the contents of the current directory on the remote machine (sending the results to a file).
drive *driveletter*	Change the current local drive.
lcd *local_directory*	Change the current local directory.
lmkdir *directory_name*	Create a new local directory.
lpwd	Display the pathname of the current local directory.
ls or **ldir** [*path**filename*]	List only files in the remote directory (sending results to a file).
mkdir *directory_name*	Create a new remote directory.
parent	Change the current remote directory to its parent directory.
pwd or **fpwd**	Display the pathname of the current remote directory.
rmdir *directory_name*	Delete a remote directory.

Resetting Options

Use	To
ascii [**nonprint** | **telnet** | **carriage**]	Set the transfer mode to ASCII (text).
binary, **image**, **local** *n* or **tenex**	Set the transfer mode to binary.
mount *pathname*	Change the server's file system mount information.
option	Display current option settings.
option ask (**on** | **off**) or **option prompt** (**on** | **off**)	Prompt or do not prompt before each transfer. Default: off.
option casehack (**on** | **off**)	Create or do not create filenames in the specified case. Default: on.
option hash (**on** | **off** | *n*) or **hash** (**on** | **off** | *n*)	Display or do not display a number sign (#) each time data is read from the network. Default: off.
option page (**on** | *n* | **off**)	Prevent or do not prevent the display from scrolling off the screen. Default: off. Use *n* to specify the number of lines to display.
option pathhack (**on** | **off**)	Remove or keep path for a destination filename. Default: on.
sunique [**on** | **off**]	Store a file on a server with a unique filename.
type (**ascii** | **binary** | **image** | **tenex**)	Display or set the transfer mode.

Tftp

tftp (**get | overwrite| put**) *local_file host remote_file* [**image**]
tftp serve

The **tftp** command transfers a single file between your 6400 computer and a remote TFTP server, without requiring authentication.

get	Transfers a file from a remote machine to your 6400 computer.
host	Specifies the hostname or IP address of the remote host.
image	Transfers a binary file.
local_file	Specifies a local 6400 computer filename.
overwrite	Overwrites the existing local file on your 6400 computer.
put	Transfers a file to the remote machine.
remote_file	Specifies a remote filename.
serve	Starts a TFTP server on a local 6400 computer.

To end the server program, use the interactive command **q**.

Using DHCP and Bootp for IP Configuration

You can use the DHCP and Bootp programs to obtain a 6400 computer's network configuration from a server each time you start your 6400 computer, regardless of its location. To get configuration information from a server, the network administrator must have set up a DHCP or Bootp server. The setup determines which protocol you use. DHCP is usually preferred because it is more flexible. By centralizing administration for several 6400 computers, this method of configuration makes information easier to update.

DHCP and Bootp Clients

DHCP provides a simple and reliable way for you to configure 6400 computers from a server. DHCP centralizes TCP/IP configuration, manages the location of static and dynamic IP addresses, and automates much of the configuration process. DHCP can configure any parameter needed for a 6400 TCP/IP client.

DHCP simplifies 6400 computer configuration by allowing your 6400 computer, as a DHCP client, to access network configurations with common characteristics that are shared across multiple 6400 computers.

DHCP is an extension of Bootp and can interoperate with Bootp participants. The DHCP client can get network information from either a Bootp server or a DHCP server.

When a DHCP or a Bootp client program starts on your 6400 computer, the program sends a broadcast request for configuration information (such as an IP address and the addresses of network resources, such as printers, servers, routers, and so forth) out to the network.

If a DHCP or Bootp server is available, the server responds to the client request and sends configuration information to the client. The DHCP or Bootp client can also specify the address of a known server that the client wants to use for configuration.

The client request may contain values for any of the items in Table 2-1.

Table 2-1
DHCP Client Request Values

Value	Description
MAC address	The physical address of the 6400 computer on the network. The hardware address is guaranteed to uniquely identify the requesting client. MAC addresses are shown as hexadecimal numbers. A sample MAC address is 0x0020A633F2BA. To find the MAC address of a 6400 computer with the 2.4 GHz OpenAir radio, use the **proxstat** utility (see page 2-22). Note that **proxstat** enables you to easily view statistics on your 6400 computer's small display. You can also use the **inet config** command for the 2.4 GHz OpenAir or 802.11 DS radio (see page 2-29).
Subnet number	A number derived from the incoming DHCP client request (and not specifically entered by the client).
Client ID	A string that uniquely identifies your 6400 computer, such as a user name.

Table 2-1 (Continued)
DHCP Client Request Values

Value	Description
Client ID *(continued)*	This value can be used in place of the MAC address to identify a client configuration so that the same configuration is issued to a client regardless of the MAC address. (This feature supports the changing of the hardware without reconfiguring the server or assigning the 6400 computer client a different IP address.) By default, the DHCP client uses a client ID based on the MAC address.
Class ID	A string that identifies the class to which the client belongs. A system administrator can choose to group sets of 6400 computers into separate classes, and return different configuration information for each separate class. Examples of a class would be all 6400 computers, or all machines belonging to a given department.

A DHCP or Bootp server compares the information provided in the client request to a database to select a defined configuration, called a “profile.” When the server receives a request from a client, the server determines if the client has previously received configuration information and an address.

If the Client	The Server Then
Has previously received configuration information and an IP address	Assigns the same configuration to the client.
Has not requested configuration information before	Uses the information in the client request to select a configuration.

After the server determines the configuration values and IP address, the server sends this information back to your 6400 computer. The information sent from the server includes the following:

- A set of configuration parameters, called "options." Options define network resources (such as servers and printers) and site-specific information.
- A set of valid values for the options (such as IP addresses for servers).
- An IP address that is either a predetermined, permanent address, called a *static* address, or an address that is dynamically allocated. Bootp servers can return only static addresses.

  For information about dynamic and static address allocations, see "Assigning IP Addresses with DHCP" on page 2-50.
- The duration of the *lease* offered by the server (if the IP address is a dynamically allocated address) that determines the length of time that you can keep the address. Bootp servers do not return a lease time, because all Bootp responses are considered to be permanent.

  For information about leases, see "Assigning DHCP Leases" on page 2-51.

The client uses the information it receives to update the kernel on your system. These values can change each time you start your 6400 computer. The accuracy of the value is verified every time the DHCP or Bootp client obtains or renews a lease.

▶ **NOTE:** *If you have an IP address and other network configuration values set in your PCTCP.INI file and you use the DHCP or Bootp client program to get new information, the new information replaces the existing information in the kernel. These programs do not update PCTCP.INI unless the* ***-w*** *switch is used when the programs are started.*

Assigning IP Addresses With DHCP

DHCP supports the following mechanisms for IP address allocation:

Dynamic:	An address allocated to your 6400 computer from a pool of available IP addresses at the time of the client's request.
Static:	An address reserved for a specific 6400 computer.

The type of address you receive is determined by the DHCP server configuration.

Dynamic Address Allocation

Dynamic address allocation allows automatic reuse of an address that is no longer needed by the 6400 computer to which it was assigned. Dynamic allocation is particularly useful for a client that connects to the network only temporarily.

Each dynamically allocated address has a lease associated with it that determines the length of time you can keep the address. For information about DHCP leases, see "Assigning DHCP Leases" on page 2-51.

Static Address Allocation

With static address allocation, the client always gets the same IP address identified by its MAC address or by its client ID. For dynamic address allocation, the DHCP server identifies the client configuration by its subnet number.

Assigning DHCP Leases

DHCP leases offer an automated mechanism for the safe distribution and reuse of IP addresses. A DHCP server assigns a lease to your 6400 computer when the server assigns a temporary IP address. The lease can vary in time from a few minutes to several years.

The server sets a default value for the lease time. When the DHCP client requests an address, the client also can request a lease time. If the requested lease time is equal to or less than the server default value, the DHCP client gets the amount it requests. If the client requests more than the default value for its profile, the server assigns the default value. The DHCP client then

- maintains the lease time granted by the server.
- automatically tries to contact the DHCP server halfway through that lease time to renew the lease; under most circumstances, the server renews the lease successfully.

If the server is unavailable or will not renew the lease, the DHCP client continues to try to contact the server until the lease time has expired. When the lease expires, the client stops using the leased address and begins broadcasting to find another server willing to grant a new lease. The new server can issue your 6400 computer a new lease, which may or may not be a lease for your 6400 computer's previous IP address.

▶ **NOTE:** *When a lease expires, network connections are lost. However, the DHCP client continues to broadcast over the network to discover another DHCP server that will grant it a lease.*

Configuring the DHCP Client

You can obtain network configuration information in DOS with the **dhcp** command by doing one of the following:

- Enabling the DHCP client through the 6400 TCP/IP client DOS configuration menus
- Typing the **dhcp** command at the DOS prompt
- Entering the **dhcp** command in AUTOEXEC.BAT (after the ETHDRV.EXE command) so the command runs when you start your 6400 computer

The command line interface for **dhcp** is similar to that of the **bootp** command (discussed on page 2-54, "Configuring the Bootp Client"). The primary difference is that, with DHCP, addresses are leased — while in Bootp, the address assignment is considered permanent. Because of this difference, the DOS **dhcp** command installs a TSR module so that the lease can be renewed automatically.

The **dhcp** command can handle replies from either DHCP or Bootp servers. If a Bootp server reply is received, or if the DHCP server reply indicates an infinite lease, no TSR module is loaded since there is no lease to maintain.

While **dhcp** properly handles Bootp replies, you should use **bootp** when you will be receiving replies from Bootp servers and not from DHCP servers. **Bootp** provides some Bootp-specific options that are not available with **dhcp**.

Configuration parameters for **dhcp** are located in the [pctcp bootp] section of PCTCP.INI. The *Configuration Parameter Reference* on the FTP Software, Inc. Web site lists **dhcp** configuration parameters. The URL for FTP Software is http://www.ftp.com.

The **dhcp** command has the format:

dhcp [*options*] [*config file*]

For a complete listing of **dhcp** options, see page 2-58.

Allowing DHCP to Modify PCTCP.INI

To allow DHCP to modify PCTCP.INI, use **dhcp** with the **-w** *write* option.

Testing DHCP Without Reconfiguring the Kernel

To test DHCP without reconfiguring the kernel, use **dhcp** with the **-n** option. The **-n** option prevents **dhcp** from loading the DHCP TSR module.

Specifying a Lease Time

To specify a lease time, use **dhcp** with the **-l** *lease* option and specify the length of time (in seconds) you want to keep your IP address for the lease.

▶ **NOTE:** *Without the -l option, the DHCP server determines the length of time for the lease, based on how the network administrator configured the server. Although you may use this option, be aware that the server may ignore it. For this reason, use of the -l option is not recommended unless the network administrator considers it necessary.*

Unloading the DHCP TSR Module

Use **dhcp** with the **-u** option to unload the DHCP TSR module and to send a message to the server allowing it to release the IP address. The client discontinues use of that address, and shuts down any network connections that may exist.

Configuring the Bootp Client

The **bootp** command stores the information it receives from a Bootp server in PCTCP.INI. Configuration parameters for **bootp** are located in the [pctcp bootp] section of PCTCP.INI. The *Configuration Parameter Reference* on the FTP Software, Inc. Web site lists **bootp** configuration parameters.

The **bootp** command has the format:

bootp [*options*] [*config file*]

For a complete listing of **bootp** options, see page 2-56.

You can run the **bootp** command by doing one of the following:

- Typing the **bootp** command at the DOS prompt
- Entering the **bootp** command in AUTOEXEC.BAT (after the ETHDRV.EXE command) so the command runs when you start your 6400 computer

Allowing Bootp to Modify PCTCP.INI

To allow Bootp to modify PCTCP.INI, use **bootp** with the **-w** *write* option.

Testing Bootp Without Reconfiguring the Kernel

To test Bootp without reconfiguring the kernel, use **bootp** with the **-n** option.

Specifying the IP Address of the Bootp Server

To specify the IP address of the Bootp server, use **bootp** with the **-d** *address* option. The address specified with this option overrides the `server-address=ip_address` setting in the [pctcp bootp] section of PCTCP.INI. If your 6400 computer's address is not configured, the Bootp client broadcasts its request to the network and disregards this option.

Replacing Your 6400 Computer's Current IP Address

To replace your 6400 computer's current IP address with a new address from the Bootp server, use **bootp** with the **-f** option.

▶ **NOTE:** *Never use the* ***-f*** *option with the* ***bootp*** *command if you have network applications already running on your 6400 computer. Your applications may lose their TCP connections.*

Typically, a server does not give an IP address to a client that already has an address. If the server does not reply with a new IP address, the old address stays in use. The **bootp** command disregards this option if you also use the **-n** option.

Viewing Detailed Information About the Server's Reply

To view detailed information about the server's reply, use **bootp** with the **-v** *verbose* option.

Command Summaries

The following pages describe usage and command line options for these DOS commands, included with the kernel:

- **Bootp**
- **Dhcp**

Bootp

bootp [**-fnvw**] [**-d** *address*] [**-r** *retries*] [**-t** *seconds*] [*pctcp.ini_file*]
bootp [**-?** | **-version**]

The **bootp** command runs the Bootp client program on your 6400 computer to obtain network configuration information from a remote server.

-d *address* — Specifies the IP address of the server to which the Bootp client sends its request. The address specified with this option overrides the `server-address=`*ip_address* parameter setting in the [pctcp bootp] section of PCTCP.INI. If the server's address is not set, the Bootp client broadcasts its request to the network and ignores this option.

-f — Forces **bootp** to replace your 6400 computer's current IP address with a new one from the Bootp server. (Typically, a server does not give an IP address to a client that already has one.) If the server does not reply with a new IP address, the old address stays in use. **Bootp** ignores this option if you also use the **-n** option.

▶ ***NOTE:*** *Never use the –f option if you have network applications already running on the 6400 computer. Your applications may lose their TCP connections.*

-n	Does not update PCTCP.INI or the kernel. Use this option with the **-v** option to view the information retrieved from the server without changing your kernel parameters.
pctcp.ini_file	Specifies the complete path of a PCTCP.INI file from which **bootp** reads information and to which **bootp** writes information (if **-w** option is used). This optional setting overrides the `PCTCP=` environment variable setting.
-r *retries*	Retries sending a **bootp** request the number of times specified by *retries*. Default: 4.
-t *seconds*	Times out the **bootp** command process after waiting *seconds* seconds for the **bootp** reply to be sent from the server. Default: 60.
-v	Displays detailed (verbose) information about the server's reply.
-w	Writes configuration information received from the server into PCTCP.INI.
-?	Displays and explains the usage line of this command.
-version	Displays the version and patch level of this command. Refer to this information if you call Technical Support.

EXAMPLE: To retrieve your 6400 computer's IP address and other network configuration information, timing out if no reply is received within 15 seconds, enter:

```
C:\>bootp -t 15
```

***SEE ALSO*:** **Dhcp** (page 2-58) and these RFCs:

RFC 951, *Bootstrap Protocol (Bootp)*
RFC 1531, *Dynamic Host Configuration Protocol*
RFC 1533, *DHCP Options and Bootp Vendor Extensions*
RFC 1534, *Interoperation Between DHCP and Bootp*

Dhcp

dhcp [**-nuvw**] [**-l** *seconds*] [**-r** *retries*] [**-t** *seconds*] [*pctcp.ini_file*]

The **dhcp** command obtains network configuration information for your 6400 computer from a remote server.

-l *seconds*	Specifies the length of the lease requested by the client in seconds. A lease is the length of time a client can keep an IP address. Note that it is the responsibility of the DHCP server to decide the lease duration, and a DHCP server may return a lease time different from that specified by the client, depending on how the server is configured. The lease duration specified with this option overrides the `lease-time=` parameter in PCTCP.INI. If neither is specified, the DHCP server sets the lease time.
-n	Does not update your PCTCP.INI file or the kernel. Use this option with the **-v** option to view the information retrieved from the server without changing your kernel parameters.
pctcp.ini_file	Specifies the complete path of PCTCP.INI, from which **dhcp** reads information and to which **dhcp** writes information. This optional setting overrides the `PCTCP=` environment variable setting.
-r *retries*	Retries sending a **dhcp** request the number of times specified by *retries*. Default: 4.
-t *seconds*	Times out the **dhcp** command process after waiting *seconds* seconds for the **dhcp** reply to be sent from the server. Default: 60.
-u	Unloads the DHCP module and releases the current IP address being leased. The kernel reverts to using the IP address that was in use before the DHCP TSR module was installed.

-v	Displays verbose information about the server's reply.
-w	Writes configuration information received from the server into PCTCP.INI.
-?	Displays and explains the usage line of this command.
-version	Displays the version and patch level of this command. Refer to this information if you call Technical Support.

EXAMPLE: To set your 6400 computer's IP address and other network configuration information with a 1 hour lease (3600 seconds), timing out if no reply is received within 15 seconds, enter:

```
C:\>dhcp -l 3600 -t 15
```

***SEE ALSO*:** **Bootp** (page 2-56) and these RFCs:

RFC 1531, *Dynamic Host Configuration Protocol*
RFC 1532, *Clarifications and Extensions for the Bootstrap Protocol*
RFC 1533, *DHCP Options and Bootp Vendor Extensions*
RFC 1534, *Interoperation Between DHCP and Bootp*

Configuring the SNMP Agent

The SNMP agent lets other hosts and network management stations using SNMP examine your 6400 computer's statistics and configuration information over the network. An SNMP management station gets this information from the 6400 computer's MIB for use in troubleshooting and tuning network operations and for determining network performance. In terms of the client-server paradigm, an SNMP agent is a server, while an SNMP management station is a client.

The **snmpd** command starts a TSR program that provides an agent for SNMP requests that follow RFC 1065, *Structure and Identification of Management Information for TCP/IP-Based Internets*, and RFC 1067, *A Simple Network Management Protocol*.

The DOS SNMP agent supports most of the MIB-1 SNMP MIB defined in RFC 1156, *Management Information Base for Network Management of TCP/IP-Based Internets*. Appendix D is Section 6 of the RFC (Definitions).

Before You Use the SNMP Agent

Ensure the kernel is installed and that

- the COMMUNIT.CNF and TRAPCOMM.CNF files are in the same directory as the DOS SNMP agent, SNMPD.EXE.
- for another host to access your 6400 computer's SNMP agent, that host has an SNMP network management product (such as HP OpenView, or software from another vendor).
- you load the TSR kernel before you invoke the **snmpd** command.

An SNMP network management product (such as a personal computer running the PC/SNMP Tools applications) displays the object IDs (associated text names) for the MIB variables. If you are using another network management product, refer to its documentation to determine if that product supports nonnumeric names or MIB variables.

As an add-on agent for kernels, the **snmpd** program requires two UDP connections. The kernel allows only four UDP connections by default. You should increase the number of available UDP connections if you use the **snmpd** program when you use other programs that use UDP connections. For more information, see the **ethdrv** command (page 2-31).

Configuring the SNMP Agent

You can run the SNMP agent using its default configurations, or you can modify those configurations. SNMP configuration files are

- COMMUNIT.CNF, the SNMP community file
- TRAPCOMM.CNF, the SNMP error condition (trap) file

The 6400 TCP/IP client software files contain samples of TRAPCOMM.CNF and COMMUNIT.CNF, each containing configuration instructions. If the configuration files are not formatted correctly, the SNMP agent displays various error messages and aborts.

To configure an SNMP agent for your system:

1. Use a text editor to add entries to COMMUNIT.CNF.

   The file contains entries that define SNMP community names, IP addresses, and privileges (NONE, READ, and WRITE) used to validate incoming SNMP request packets.

   If a community specified in an incoming packet is not authorized for the operation that it requests, the request is discarded and an SNMP error condition message (trap) may be sent (if specified in TRAPCOMM.CNF).

▶ **NOTE:** *To allow an SNMP management station to set values in your read-write–accessible MIB variables, you must set your community privilege type to* `WRITE`.

   Each entry in COMMUNIT.CNF must define a community name, an IP address (in dot notation), and the appropriate privilege (in uppercase). For example:

```
interop 128.127.53.190 READ
```

▶ **NOTE:** *Most SNMP agents use the default community name "public."*

2. Use a text editor to add entries to TRAPCOMM.CNF.

   The file contains entries that define the IP addresses, SNMP communities, and UDP port numbers to use when sending SNMP trap packets. The SNMP agent collects three kinds of error condition messages (or traps):

   - "ColdStart" when the agent is loaded
   - "WarmStart" when the agent is restarted
   - "AuthenticationFailure" when a query specifies an unknown SNMP authentication community

   To receive AuthenticationFailure traps, set variable **snmpEnableAuthenTraps** to 1.

   You can specify up to five entries in the file. Each entry must define a community name, an IP address (in dot notation) and a UDP port number where you want to send error condition messages. For example:

   ```
   newcommunity 128.127.59.154 162
   ```

Enabling the DOS SNMP Agent

To load the DOS SNMP agent, enable it through the 6400 TCP/IP client DOS configuration menus (see page 2-9). Or, type the following command at the DOS prompt:

```
C:\>snmpd
Copyright 1990 by SNMP Research, Inc.
communit.cnf not found; Using community "public",
  read-only
trapcomm.cnf not found; No Traps will be sent.
System Description = SNMPD v2.1 (9.3.1)
System Object Identifier = 1.3.6.1.4.1.121.1.1
Communities:  1 authentication, 0 trap
agent occupies 37680 bytes
```

Disabling the DOS SNMP Agent

To unload the DOS SNMP agent, you must unload the TSR kernel and remove the **snmpd** program from memory. To unload the SNMP agent, do one of the following:

- If you enabled the SNMP agent through the DOS configuration menus, disable it through the DOS configuration menus and then reboot your 6400 computer. For more information, see page 2-9.
- If you manually started the SNMP agent at the DOS prompt, disable the agent by rebooting your 6400 computer.

SNMP Command Summary

snmpd
snmpd [**? | -version**]

The **snmpd** command lets other hosts using SNMP examine your 6400 computer's statistics and configuration information. **Snmpd** starts an SNMP agent.

-?	Displays and explains the command's usage line.
-version	Displays the version and patch level of this command. Refer to this information if you call Technical Support.

***SEE ALSO*:** **Inet** (page 2-27), **Ethdrv** (page 2-31), and these RFCs:

RFC 1065, *Structure and Identification of Management Information for TCP/IP–Based Internets*
RFC 1067, *A Simple Network Management Protocol*

Section 3

Troubleshooting Network Connections

This section discusses problems you may encounter when you try to connect with another host across a network. This section also describes DOS commands you can use to understand and solve problems, such as **ping**, **inet**, and **arp**. If your 6400 computer has a 2.4 GHz OpenAir radio, you can also use **proxstat**.

When you encounter a problem with connecting to another network host, it may be the result of

- a physical problem with the network (such as insufficient access point signal strength), or an incorrectly configured radio, access point, or IP parameter.
- network congestion.
- faulty host or router configuration.
- incorrect or missing entries in name translation tables on the 6400 computer, or on the DNS servers on your network.

Before You Start Troubleshooting Host Connections

Investigating and solving problems with host connections is not difficult, but it may take you down several paths. You should have a basic understanding of your network and be able to restore your system to its original configuration if necessary. For those reasons, ensure you do the following:

- Make backup copies of AUTOEXEC.BAT and PCTCP.INI. With these copies, you can compare and test incremental changes to your configuration. In addition, you can restore your original configuration if you are not satisfied with the new configuration.
- Understand basic Internet features and addressing schemes if you are accessing the Internet.
- Understand the basic setup and components of your local network.

Testing Your 6400 Computer's IP Address

To test your 6400 computer's IP address:

Use **ping -z** and specify your 6400 computer's IP address. For example:

```
C:\>ping -z 128.127.50.182
```

To verify your 6400 computer's IP address:

1. Open the 6400 TCP/IP client DOS configuration menus by typing the following at the DOS prompt:

   chgparms

2. Ensure the setting for the Config Parms/IP address parameter is correct.

Or, type **inet stats** at the DOS prompt to display the address:

```
C:\>inet stats
```

To correct an invalid IP address:

1. Open the 6400 TCP/IP client DOS configuration menus by typing the following at the DOS prompt:

   chgparms

2. Modify the setting for the Config Parms/IP address parameter.

Or, open PCTCP.INI and modify the setting for the `ip_address=` parameter.

Troubleshooting Host and Network Connections

If you have problems making a network connection, use **ping** to send an echo request to a remote host to test host and network availability.

- If the target host is active and sends a reply to your ping request, you know that the network media forming the path to that host is working.
- If a host fails to respond to a network request, it means a failure has occurred at one of several points from your 6400 computer to the remote host.

  The host may not be working and is unable to respond, some network or gateway in the path between your 6400 computer and the target host may not be working, or the host may not implement the service you are requesting.

For more information about Ping messages, see "Interpreting Ping Messages" on page 3-11.

To send an ICMP echo request and receive debugging information:

Use **ping** *IP address* and specify the target host's IP address. For example:

```
C:\>ping 123.456.78.910
```

▶ NOTE: *Various options are available with **ping**. For a list of options that may provide useful information for your specific case, type **ping -?** at the DOS prompt.*

To diagnose simple network congestion:

- Use **ping -n** *value* **-z** *hostname* | *IP address* to send echo requests to the remote host a specific number of times. For example:

```
C:\>ping -n 2 -z vex
host responding, time = 25 ms
host responding, time = 75 ms
Pinged host 2 times with 0 failures,
round-trip average (ms) = 50
```

- Or, use **ping -t** *hostname* | *IP address*. For example:

```
C:\>ping -t vex
Pinging host vex.xyz.com repeatedly
To exit, type q
# of tries=635, failures=0, time=60;
round-trip average (ms)=36
```

To analyze packet loss and network load:

Use **inet stats**:

```
C:\>inet stats
```

To display header information from incoming and outgoing packets:

1. Use **ping -d -z** *hostname* | *IP address* to display header information from the *incoming* packet. For example:

```
C:\>ping -d -z chaco
Dump of incoming packet
Version=4 IP header length=5 Precedence=Routine
Type of service=Normal
Total length=284 Protocol=1 TTL=255
```

2. Use **ping -d# -z** *hostname* | *IP address* to display header information for the *outgoing* packet. For example:

```
C:\>ping -d# -z chaco
Dump of outgoing packet
Version=4 IP header length=5 Precedence=Routine
Type of service=Normal
Total length=284 Protocol=1 TTL=64
```

Confirming ARP Requests

The following machines can accept ARP requests:

- Another 6400 TCP/IP client
- A UNIX host
- Any other host that supports a TCP/IP protocol stack

If you are unsure if your 6400 computer is sending ARP requests to these hosts, test the transmission and receipt of requests.

To test transmission of ARP requests:

- Use **ping -z** *IP address*.
- Use **inet arp**. For example:

```
C:\inet arp
ARP cache:
   128.127.52.141: 0080c0205516 expires: 259 sec.
   128.127.52.30: 08004c5e8c1a expires: 782 sec.
   128.127.57.30: 08006a022aea expires: 527 sec.
```

The ARP cache displays entries for each network device that has recently sent or replied to an ARP request. The entries specify each host's IP address, the corresponding hardware address, and expiration information.

Look in the ARP cache listing for the target computer's IP address and MAC address. If this information is in the listing, your 6400 computer is sending ARP requests and the target machine received those requests.

Many conditions cause ARP reply failure, including the following:

- Your 6400 computer sent the ARP request to the LAN, but the request did not reach the target host.

  If your local LAN segment contains any repeaters or bridges, and if any of these devices connects your 6400 computer to the remote host, problems with these devices can cause ARP failure. Notify your system administrator.

- The ARP request successfully reached the target host but was not read off the network by the target host's network interface card, or your 6400 computer did not receive the ARP reply.

  This may indicate a problem with the network interface card in the target host. Contact the administrator of the remote host for help. This may also indicate problems with intervening repeaters or bridges. See your system administrator to investigate any suspected problems with local repeaters and bridges.

Also do the following:

- Ensure ARP Server Mode is enabled for the access point. For almost all installations, the No Flooding setting is recommended.
- *2.4 GHz OpenAir radio:* Ensure the OWLATTCH module is entered in AUTOEXEC.BAT. The command line is:

  owlattch

- *802.11 DS radio:* Ensure the WVLANATT module is entered in AUTOEXEC.BAT. The command line is:

  wvlanatt

- If using DHCP or Bootp, ensure your 6400 computer successfully obtained an IP address.

Troubleshooting Router Connections

An IP router (gateway) usually connects two *different* types of network media; for instance, Ethernet to Token Ring. The router has at least two network interface devices installed, each with a unique IP address, which allows you to access another part of the network.

If a router is on your network, PCTCP.INI should list the IP address of the router through which you can access the rest of the network. If you are having problems accessing other hosts on your network, it may be because of problems with your router configuration or service.

Testing Router Configuration

Use **ping** *IP address* and specify the IP address assigned to a router on your network segment. If you cannot reach the router, view the router entries in PCTCP.INI and make sure they are correct.

▶ **NOTE:** *Though only one address is necessary, you can list a maximum of three routers in PCTCP.INI. If the first router is disabled, the second router on the list is used; if that one is disabled, the third is used.*

Testing Router Service

You can test the router service by tracing the route of a packet through the network by using **ping**, as follows:

- The **ping -q** command traces the route of the packet and lists the number of hops, the domain name (if supported) and IP addresses of the hosts that handled the packet, and the round-trip time.
- The **ping -i** *n* command follows an ICMP packet as it makes its way through the network. The command output summarizes the success (or failure) of the echo request, the round-trip time, and the packet's TTL.

To test IP routing:

- Use **ping -i** *n* **-z** *hostname* | *IP address*. For example:

```
C:\>ping -i 300 -z owl.com
host responding, time=50 ms, Time to live=236
```

To test IP router hops:

- Use **ping -q -z** *hostname* | *IP address* to get a full listing of the routers between your 6400 computer and the target host. For example:

```
C:\>ping -q -z owl
hop 1:128.127.50.4 router -54a.ddd.com
hop 2:128.127.5x.1 router-2a.ddd.com
Target (128.124.5x.23) reached on hop 3,
round-trip time 60 ms.
```

To see if the router is disabled:

- Use **ping**. Specify the IP address assigned to a host on your local network segment.

  If the **ping** request succeeds, use **ping** and specify the IP address assigned to a known host on the remote side of the router. If this request succeeds, the router is up; if this does not succeed, the router is probably down; contact your system administrator.

Using Output from Ping as Debugging Information

Each IP router that handles the packet must decrement the TTL by 1. If the TTL for a packet is 0 after being decremented, the router returns a "Time To Live Exceeded" ICMP message to your 6400 computer, displaying the IP address of the router sending the ICMP message.

To determine the point of failure:

1. Use **ping -i** *n hostname | IP address* with the IP address of the router returning the ICMP message.
2. Increase the **-i** *n* value by 1.
3. If you continue incrementing the TTL by 1 up to the point of failure, you can determine where your transmission fails.

Troubleshooting the Local Network Configuration

Networking problems can result from an incorrectly configured kernel. If your examination of the kernel configuration and the configuration files does not pinpoint any obvious errors or omissions, the problem may be related to the local network configuration. You can pinpoint problems and define solutions by monitoring network traffic and displaying network statistics.

To monitor the network configuration and statistics, and analyze errors:

- Use **inet config** to monitor the number and type of connections and connection statistics for the lower-layer transmission control protocols.
- Use **inet debug** to display the radio's MAC address and information about every ARP and unknown packet type sent and received by the kernel.
- Use **inet stats** to display network statistics for the top-layer transmission control protocols. By displaying the network statistics, you can account for every known non-ARP packet in each layer.
- Use **inet arp** to display the current contents of the kernel's ARP cache.

To analyze TCP connections:

- Use **inet tcp** to display the contents of the kernel's TCP connection table, including statistics for each active connection.

Interpreting Ping Messages

Ping prints messages in a standard form, as follows:

```
Ping failed:  <error message>
```

The first part of the message specifies a Ping condition ("Ping failed"); the second part defines the condition. Some messages have additional text that suggests a possible cause, as listed in Table 3-1.

Table 3-1
Ping Messages

Condition	Message and Interpretation

Low ARP timeout value	If **ping** fails with one of the following messages:
	`Ping failed:  ARP failed`
	`Ping failed:  ARP timeout`
	You may need to set your ARP timeout parameter to a higher value. The default is 1500 ms. For more information about modifying the value, see page 3-17.

No reply	If the other end of the connection does not reply, you may get the following message: `Ping failed: Timeout.` Possible causes are: ▶ The target host failed. ▶ The network path to the target host failed. ▶ The target host may be turned off. ▶ Conflict on the local 6400 computer due to an incorrect configuration.

Cannot reach host	If the connection fails because the target host cannot be reached, you may get the following message:
	`Ping failed: host unreachable:`
	`Dest. Unreachable.`
	Following are probable causes:
	▶ This condition can occur if the IP router returns an ICMP message with a code of host unreachable. This normally means the host's local network can be reached, but the target host is unavailable.

Table 3-1 (Continued)
Ping Messages

Condition	Message and Interpretation
Cannot reach host *(continued)*	▶ Your default router does not have a router table entry for your target IP host. ▶ Your default router has a router table entry for your target IP host, but determines that it cannot find the optimal pathway for accessing your target IP host; your router sends your packet to the destination anyway. Your router also sends an ICMP redirect message back to the source node (the 6400 computer) that suggests the optimal routing path. ▶ **NOTE:** *This does not signal that an error has occurred, but indicates that you could more efficiently transmit your packets by using a different router.*
Packet not forwarded	If the IP router could not forward a packet and returned an ICMP message, you may get the following message: `Ping failed: Network unreachable.` The message indicates that the destination address is nonexistent or that a network link between your 6400 computer and the destination is not available.
TTL = 0	If the IP time-to-live field in a datagram reaches zero before the datagram reaches the final destination, you may get the following message: `Ping failed: got ICMP error: Time to Live exceeded.` This condition can occur if the TTL value is less than 64.

If you cannot establish a connection to the remote host by using its IP address, the cause of failure could be that the remote network or its gateway is not operating. Try using **ping** to contact the remote host.

If you think one of these problems is causing the connection failure, you probably cannot solve the problem alone. Contact the remote host's system administrator or the network administrator for help.

Using the SNMP MIB Browser

An SNMP agent resides at the 6400 computer. The agent accepts SNMP requests from an SNMP network management platform and responds with the requested data. The SNMP agent also services SNMP SET requests and sends unsolicited messages (traps) when a predefined event occurs.

Identifying TCP/IP Client Issues

When troubleshooting network connections, you may also need to

- *2.4 GHz OpenAir radio:* verify that the LAN ID and security ID are correct.
- *802.11 DS radio:* verify that the network name is correct.
- understand how power management affects communications.
- modify IP addresses.
- increase the ARP timeout value.

Verifying LAN ID and Security ID

▶ **NOTE:** *LAN ID and security ID apply only to the 2.4 GHz OpenAir radio.*

The PROXSTAT.EXE utility for the 2.4 GHz OpenAir radio displays the radio level connectivity between your 6400 computer and the access point. Use the utility to verify that your LAN ID and security ID are correct. For instructions, see page 2-22.

Verifying the Network Name

▶ **NOTE:** *LAN ID and security ID apply only to the 802.11 DS radio.*

To verify that the network name for the 802.11 DS radio is correct, open NET.CFG and check the name.

Understanding Power Management

Power management is the process of putting the radio and 6400 computer into low power states to conserve battery life. These low power states are limited communication connectivity states that can lead to unexpected results when testing your network connection for the first time.

The radio spends most of its time in either the *on* or the *snooze* power state. While in the on state, its response time is very fast and it receives all types of data frames, including unicast, multicast, and broadcast.

If the radio is idle for more than 5 seconds (or, for the 2.4 GHz radio, the time specified by the sum of INACTIVITY_SEC and INACTIVITY_MIN in NET.CFG), it switches to its *snooze* power state. While in the snooze state, it receives only unicast frames; it does not receive multicast or broadcast frames.

The inability to receive broadcast frames can result in failed attempts to ping the 6400 TCP/IP client from a server. The Proxy ARP Server feature in the 6710 Access Point solves the problem of receiving ARP request broadcast frames, but not the other types of broadcasts.

If you suspect that the inability to receive broadcast or multicast frames may be the problem, try to temporarily disable radio power management by doing the following:

- *2.4 GHz OpenAir radio:* set INACTIVITY_SEC to 0 and INACTIVITY_MIN to 0 in NET.CFG
- *802.11 DS radio:* disable Card_Power_Management in NET.CFG

For more information about power management, see Appendix B, "Tuning the 6400 TCP/IP Client." For more information about configuring the Proxy ARP Server, refer to the *21XX Universal Access Point Technical Reference Manual* (P/N 067150) or the *6710 Access Point User's Guide* (P/N 961-047-081).

Modifying IP Addresses

If you are unable to ping the access point or a host on the wired LAN, you may have an IP addressing problem.

To check IP addressing:

- Ensure your 6400 computer has an IP address.

  The address can be set through the 6400 TCP/IP client DOS configuration menus, manually set through PCTCP.INI, or automatically obtained through DHCP or Bootp.

NOTE: *For initial unit testing, it is best to explicitly set the IP address through the 6400 TCP/IP client DOS configuration menus or PCTCP.INI to eliminate the added complications due to server-provided IP addresses through DHCP or Bootp.*

- Ensure your 6400 computer's IP address has the same subnet as the computer you are trying to ping.

  If the computer you want to ping is on another subnet, a router must deliver your ping packet to it. For your 6400 computer to find the router, use one of the following methods to enter the router's IP address:

  - Open the 6400 TCP/IP client DOS configuration menus and enter the IP address for the Config Parms/router parameter (page 2-7).
  - Open PCTCP.INI and modify the setting for the following parameter, located in the [pctcp ifcust 0] file section:

    ```
    router=
    ```

  - Obtain the IP router address from a DHCP or Bootp server (page 2-46).

Increasing the ARP Timeout Value

If **ping** intermittently fails with the message "ARP failed" or "ARP timeout," you may need to set your ARP timeout parameter to a higher value. An ARP must occur before one IP node can communicate with another IP node. In a wireless LAN, more time is required to complete the ARP transaction than in a wired LAN. By extending the ARP timeout value, your 6400 computer waits longer for the ARP transaction to complete.

To set the ARP timeout:

1. Use a text editor to open PCTCP.INI.
2. Modify the setting for the following parameter, located in the [pctcp kernel] file section:

   ```
   arp-timeout=
   ```

   The range is 1 to 5000, in milliseconds. The default is 1500 milliseconds. If no timeout is specified, it is automatically set to 500 milliseconds.

Identifying Access Point Issues

Checking the Enterprise Wireless LAN Configuration

Problems with the Enterprise Wireless LAN system could cause connectivity problems. Verify that all access points are running and are properly connected and configured.

Tools such as HP OpenView or OWLView (or both) can assist in this effort and also show changes in link configuration. If these tools are not available, you can use **ping** to verify that each access point is operational (ping each access point). If an access point is down, it may be the source of a coverage loss problem.

For information about HP OpenView, refer to the *Open Wireless LAN With HP OpenView for Windows User's Guide* (P/N 961-051-009). For information on using OWLView to view Enterprise Wireless LAN network topology and device status, refer to the INCA*View for HP OpenView for Windows User's Guide* (P/N 961-051-010).

Verifying the LAN ID

▶ **NOTE:** *LAN ID applies only to the 2.4 GHz OpenAir radio.*

Verify that all access points have the correct LAN ID. If the access points and the 6400 6400 Computer TCP/IP client do not have the same LAN ID, your 6400 computer cannot connect to the access points.

You can verify the LAN ID by creating a Telnet session with each access point and using the access point configuration menus to view the LAN ID, or by using a tool such as HP OpenView or the OWLView application (or both) to view this information.

▶ **NOTE:** *The SNMP MIB object for the LAN ID is:*

norand.manage.norandNET.nBridge.brgState.bsLanId

Checking the Flooding Levels

The access point can be configured to flood packets through the radio. This is often used when traffic from non-Enterprise Wireless LAN devices needs to be moved through the wireless LAN. If network traffic is heavy, flooding decreases the throughput and response time of the radio network. In these cases it is best to decrease flooding if possible.

If the Enterprise Wireless LAN is being used only for 6400 computer client-server applications, access point flooding can be disabled. For information about flooding levels and how to set them, refer to the *21XX Universal Access Point Technical Reference Manual* (P/N 067150) or the *6710 Access Point User's Guide* (P/N 961-047-081).

Checking the Filtering Levels

If it is necessary to enable access point flooding, you can use filters to decrease the amount of data being flooded. The access point's filtering menus allow for setting filters by packet type. By allowing only the needed packet types to be flooded through the radio network, performance can be improved. For information about filtering levels and how to set them, refer to the *21XX Universal Access Point Technical Reference Manual* (P/N 067150) or the *6710 Access Point User's Guide*.

Checking the ARP Server Mode Setting

The Enterprise Wireless LAN ARP server should be enabled for 6400 computer TCP/IP client connectivity applications. The access point ships with the ARP server disabled. Enable the ARP server in the access point as follows:

- If access point flooding is disabled or set low, use the No Flooding setting for ARP Server Mode.
- If access point flooding is set high, use the Normal Flooding setting for ARP Server Mode.

For information about ARP server mode settings and how to set them, refer to the *21XX Universal Access Point Technical Reference Manual* (P/N 067150) or the *6710 Access Point User's Guide*.

Troubleshooting the DHCP Client

Following is a possible solution to a situation you may encounter when using the DHCP client to get network configuration information. The system message is described first, followed by recommended courses of action.

`DHCP servers not responding! Please contact your network administrator.`

This message appears when the DHCP client sends a broadcast request for configuration information to the DHCP server and a reply is not received within the timeout period.

- It may be necessary to reconfigure either the initial timeout period (through the **dhcp -t** option) or the initial retry count (through the **dhcp -r** option) in environments in which a DHCP (or Bootp) server takes a long time to respond.
- DHCP servers that send only broadcast frames require access point flooding. If you are using this type of DHCP server, you must set global flooding options on the access point according to the following charts.

For the 21XX UAP:

Global Flooding Option	Setting
Multicast Flood Mode	Hierarchical
Multicast Outbound to Terminals	Enabled
Multicast Outbound to Secondary LANs	Set locally
Unicast Flood Mode	Disabled

For the 6710 Access Point:

Global Flooding Option	Multicast	Unicast
Inbound	Enabled	Disabled
Outbound to Secondaries	Enabled	Disabled
Outbound to Stations	Enabled	Disabled

Filtering may be used to improve system-level performance. For information about setting filtering levels at the access point, refer to the *21XX Universal Access Point Technical Reference Manual* (P/N 067150) or the *6710 Access Point User's Guide* (P/N 961-047-081).

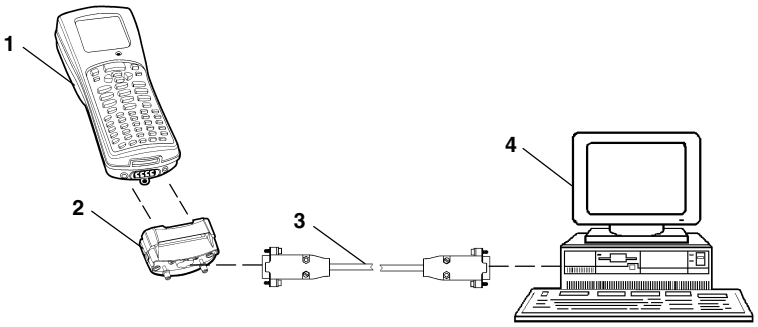
If you are using a DHCP server that can send unicast frames, access point flooding is not necessary and can be disabled. Disabling flooding can improve system-level and unit-level performance.

Appendix A

INTERSVR/INTERLNK Connection

Connecting the Computers

You can use a 6400 computer Single Dock and cable to establish an INTERSVR connection to a personal computer (desktop or laptop). You can also use a 6400 computer communication adapter endcap with a null modem cable (Figure A-1).



1. **6400 computer**
2. **Optional communication adapter endcap (P/N 705-368-001)**
3. **RS-232 null modem cable (P/N 226-106-001, 6 feet long, 9-pin to 9-pin)**
4. **Personal computer with 9-pin male COM port**

Figure A-1
INTERSVR/INTERLNK Connection

Exchanging and Editing Files

INTERLNK, a part of MS-DOS, is a device driver that connects your 6400 computer and personal computer through their serial ports. This connection enables you to exchange files and edit 6400 TCP/IP client configuration files.

To exchange and edit files:

Your personal computer must be running INTERLNK, which is part of MS-DOS.

1. Load INTERLNK as a device driver by entering the file's pathname in your personal computer's CONFIG.SYS file. For example, the following statement assumes MS-DOS is located in the C:\DOS directory on the personal computer:

   ```
   DEVICE=C:\DOS\INTERLNK.EXE  /DRIVES:3
   ```

   The "/DRIVES:3" parameter allows the mapping of three drives from your 6400 computer.

2. Insert the pathname at the end of CONFIG.SYS, after any other statement that creates a drive letter.
3. Connect your 6400 computer to the personal computer. See "Connecting the Computers" on page A-1.
4. To determine which personal computer drive corresponds to your 6400 computer's RAM (D) drive, type the following at the personal computer's DOS prompt:

   ```
   C:\>interlnk
   ```

A screen similar to the following appears:

```
Port=COM2

  This Computer              Other Computer
     (Client)                   (Server)
-------------------------------------------
F:            equals          A:
G:            equals          C: (1608Kb)
H:            equals          D:
```

5. Use DOS commands to exchange files between the personal computer and 6400 computer, and to edit 6400 TCP/IP client configuration files.

6400 TCP/IP Client Installation

Preparing for the Installation

The files on the 6400 TCP/IP client installation disk update the Flash on your 6400 computer from a previous version. The update is installed from the RAM (D) drive on your 6400 computer. You should read all instructions before installing the 6400 TCP/IP client.

For a successful installation, do the following:

- Connect your 6400 computer to an external power supply before updating Flash memory. The external power source prevents the Flash from being corrupted if all power fails during the update process.
- Ensure your 6400 computer is operating properly. You must have an operational 6400 computer to update Flash memory.
- The installation process creates a RAM (D) drive on your 6400 computer. If a RAM (D) drive already exists, save any files on the drive to another location and then delete them from the RAM (D) drive.
- Ensure your 6400 computer has at least 960 KB of disk space available for creation of the RAM (D) drive.

To prepare for the installation:

1. Copy the files on the 6400 TCP/IP client installation disk into a directory called C:\PENKEY\FLASH on your personal computer.
2. Change to C:\PENKEY\FLASH.
3. Run self-extracting file 64IPPR10.EXE (2.4 GHz OpenAir radio) or 64IPLU10.EXE (802.11 DS radio) to extract the 6400 TCP/IP client installation files.
4. After all the files have been extracted, delete 64IPPR10.EXE or 64IPLU10.EXE from C:\PENKEY\FLASH.

5. Your personal computer must be running INTERLNK, which is part of MS-DOS. Load INTERLNK as a device driver by entering the file's pathname in your personal computer's CONFIG.SYS file. For example, the following statement assumes MS-DOS is located in the C:\DOS directory on the personal computer:

   ```
   DEVICE=C:\DOS\INTERLNK.EXE  /DRIVES:3
   ```

   The "/DRIVES:3" parameter allows the mapping of three drives from your 6400 computer.

6. Insert the pathname at the end of CONFIG.SYS, after any other statement that creates a drive letter.
7. Connect your 6400 computer to your personal computer. See "Connecting the Computers" on page A-1.

Installing the 6400 TCP/IP Client

1. Begin the installation with your 6400 computer at the C:\ prompt.

▶ **NOTE:** *You may need to reboot your 6400 computer to get to the C:\ prompt. For instructions, see "Rebooting Your 6400 Computer" on page A-8.*

2. Type the following command at the prompt:

   ```
   C:\>6400.bat
   ```

   6400.BAT creates a 960 KB RAM (D) drive, adds D drive to the path, and makes your 6400 computer's A, C, and D drives available to INTERLNK.

3. To determine which personal computer drive corresponds to your 6400 computer's RAM (D) drive, type the following at the personal computer's DOS prompt:

   `C:\>interlnk`

   A screen similar to the following appears:

```
Port=COM2

  This Computer              Other Computer
     (Client)                   (Server)
-------------------------------------------
F:            equals          A:
G:            equals          C: (1608Kb)
H:            equals          D:
```

4. Copy the files in C:\PENKEY\FLASH on the personal computer to the RAM (D) drive on your 6400 computer.

▶ **NOTE:** *Before you copy the files, ensure that you have deleted self-extracting file 64IPPR10.EXE (2.4 GHz OpenAir radio) or 64IPLU10.EXE (802.11 DS radio) from C:\PENKEY\FLASH.*

   For example, in the sample screen above, H drive corresponds to your 6400 computer's RAM (D) drive. In this case, you would copy the files to H drive:

   `C:\>copy *.* h:`

5. After the files have been copied, exit INTERSVR on your 6400 computer by pressing ALT and then F4.

6. Type the following command at your 6400 computer's DOS prompt:

   `D:\>`**`124.bat`**

   This command boots your 6400 computer from the RAM (D) drive and then resets it. When your 6400 computer resets, it begins the Flash update process. You are not prompted further unless an error occurs or a file is missing.

▶ **NOTE:** *If your 6400 computer does not reset, you may need to do a 4-key reset. For instructions, see "Resetting Your 6400 Computer" on page A-8.*

   After reflashing, your 6400 computer resets and reboots to C drive.

7. To confirm the Flash version, observe the screen while your 6400 computer is booting from C drive.

   Or, you can display the version by typing the correct command at the prompt. For the 2.4 GHz OpenAir radio, type:

   `C:\>`**`64ippr10.nam`**

   For the 802.11 DS radio, type:

   `C:\>`**`64iplu10.nam`**

8. When the update is complete, COMMAND.COM, RB.BAT, and RESET.EXE are present on the RAM (D) drive. If you want, you can delete these files and the RAM (D) drive.
9. Note that AUTOEXEC.BAT has been renamed to AUTOEXEC.BAK, and CONFIG.SYS has been renamed to CONFIG.BAK.

Rebooting Your 6400 Computer

To reboot your 6400 computer:

1. Press CTRL-ALT-DEL.
2. Quickly press ALT to display the DOS 5 Boot Menu.
3. To reboot to the C:\ prompt, select this option:

   ```
   3) Flash Drive = C:
   ```

If CTRL-ALT-DEL does not reboot your 6400 computer, do a 4-key reset.

Resetting Your 6400 Computer

To do a 4-key reset:

1. Simultaneously press both ENT keys, the BLUE key, and the GOLD key for about 2 seconds.
2. Quickly press ALT to display the DOS 5 Boot Menu.
3. To reboot to the C:\ prompt, select this option:

   ```
   3) Flash Drive = C:
   ```

Cable Pin-Outs

Figure A-2 shows pin-outs for the RS-232 standard null modem cable, P/N 226-106-001.

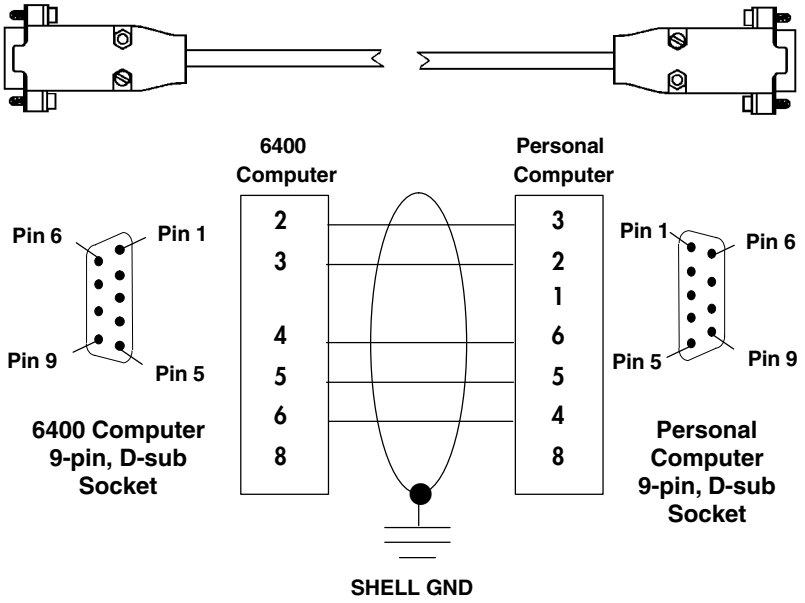


Figure A-2
Standard Null Modem Cable Pin-Outs

Appendix B

Tuning the 6400 TCP/IP Client

Components

You need the following components when tuning the 6400 TCP/IP client:

- Radio parameters in NET.CFG
- 6400 Computer BIOS parameters in AUTOEXEC.BAT and CONFIG.SYS
- TCP/IP kernel parameters in PCTCP.INI
- Available bandwidth
- Client and server configuration

Tuning Power Usage

Before you tune power usage, it may be helpful to understand the radio's power states, listed in the following chart.

Radio Power State	Description
On	Radio is fully awake and communication is fully enabled. This state consumes the most power.
Snooze	Radio is idle but switches to "on" when it needs to send or receive. The Snooze state consumes less power than the On state.
Standby	Radio is essentially "off" but can be turned "on" again if data is to be sent. The radio goes into Standby only if it cannot find an access point to synchronize with.
Off	Radio completely powers down.

2.4 GHz OpenAir Radio Parameters

For the 2.4 GHz OpenAir radio, radio power management settings are specified in NET.CFG for the parameters in the following chart.

Parameter	Description
INACTIVITY_SEC	Specifies the number of seconds the radio must be idle before it goes into its low-power snooze mode. The specified value is rounded up to the nearest 5-second increment. Default: 5 seconds (recommended for most installations).
INACTIVITY_MIN	Specifies the number of minutes the radio must be idle before it goes into its low-power snooze mode. Default: 0 seconds (recommended for most installations).

802.11 DS Radio Parameters

For the 802.11 DS radio, radio power management settings are specified in NET.CFG for the parameters in the following chart.

Parameter	Description
Card_Power_Management	Enables or disables the 6400 computer to use power management in an Extended Service Set (ESS).
Maximum_Sleep_Duration	Specifies the maximum time the 6400 computer is allowed to spend consecutively in the DOZE state, and determines the Listen Interval of the computer's power management scheme. Default: 100 ms.
Receive_All_Multicasts	Specifies whether the 6400 computer must receive all multicast frames (with addresses specified by the protocol stack) when using power management. When this is the case, the computer will have to wake up frequently to receive the multicast frames. This causes less than optimal power savings. Default: Enabled.

6400 Computer BIOS

▶ **NOTE:** *For complete details about power management, see the PEN*KEY 6400 Computer Programmer's Reference Guide (P/N 977-054-004).*

6400 computer power management settings are controlled by the ELANAPM.EXE and ELANCFG.EXE programs, typically executed in AUTOEXEC.BAT. The 6400 computer has the power states listed in the following chart.

6400 Power State	Description
High speed (ready)	Full radio communication is possible. High speed offers the best radio performance but the worst battery performance.
Low speed (idle)	Full radio communication is possible.
Doze (idle)	Full radio communication is possible.
Suspend	Radio is powered off and cannot communicate.

The following switches control the power states:

- **elanapm /Lx**

  where x is 0 or 1:

  0 = go from high speed to idle as per the /H switch for ELANCFG.
  1 = go from high speed to idle immediately.

- **elancfg /Hx /Ly /Dz**

  where:

  H = high speed; x = 0 to 16 seconds.
  L = low speed; y = 0 to 64 seconds.
  D = doze; z = 0, or 4 to 1024 in increments of 4 seconds.

▶ **NOTE:** *"0" disables a transition from one state to the next lower state.*

Tuning Throughput Performance

The following terms are important to understanding throughput performance:

- *Client-to-server* describes communication initiated by the 6400 computer. An example is when the 6400 computer's operator scans a bar code and sends it to the server. The server responds with a confirmation or denial.

  Client-to-server mode is ideally suited for the wireless LAN environment. The majority of data collection applications use client-to-server communications.

- *Server-to-client* describes communication initiated by a server. An example is a dispatch application where the server initiates the communication and sends a message to a 6400 computer for its operator to perform a task or respond (or do both).

  Server-to-client mode is not ideally suited for wireless LAN operation because it requires your 6400 computer to be awake and ready to receive an unsolicited message from the server at any time. This requirement shortens your 6400 computer's battery life and may decrease the throughput performance of the wireless LAN.

Two factors affect throughput performance: the available bandwidth, and the client and server configuration.

Available Bandwidth

Throughput performance is most affected by the available bandwidth of the network medium. The more radios communicating through a single access point, the slower the throughput performance of each radio.

The best way to achieve good throughput is to ensure enough bandwidth is available for the amount of radio traffic you generate. These factors can affect your available bandwidth:

- Insufficient radio signal coverage from the access point (your 6400 computer is too far away from the access point, or walls or other obstructions are between your 6400 computer and the access point)
- Radio interference such as microwave ovens and RF (radio frequency) ID tag readers in the same frequency range as your radio
- Flooding Ethernet traffic onto the RF medium (the wireless LAN)
- Too many 6400 computers trying to communicate through too few access points

Throughput Rate

As a general rule, a single radio communicating through a single access point with no background RF noise and a reasonable amount of Ethernet traffic (about 10 percent utilization) can complete an FTP file transfer (a "put" from the 6400 computer) at about 50 KB per second (2.4 GHz OpenAir radio). Depending on the characteristics of your network, your performance may be slightly better or worse.

For two or more 6400 computers transferring files at the same time, you can divide 50 KB (2.4 GHz OpenAir radio) or 50–60 KB (802.11 DS radio, with power management enabled) per second by the number of 6400 computers to get the approximate throughput of each computer. For example, five 6400 computers can simultaneously transfer files at about 10 KB per second each. This is the "worst case" estimate, since most communications do not occur at the same time.

▶ NOTE: *If power management is disabled on the 802.11 DS 6400 computer, use a throughput rate of 130 KB.*

If each 6400 computer takes its turn transferring a file, each computer has about a 50 KB (2.4 GHz OpenAir radio) or 50–60 KB (802.11 DS radio, with power management enabled) per second throughput rate. However, the total time required for all 6400 computers to transfer all files is still the same as if they transferred at the same time.

Flooding

Flooding Ethernet traffic onto your wireless LAN can be detrimental to your 6400 computer's communication performance. The open wireless LAN system is designed to eliminate unnecessary traffic on the wireless LAN to improve performance and efficiency. Some server-to-client applications and protocols, however, may require certain access point settings and 6400 computer radio settings that provide less than optimum wireless LAN efficiency. You must consider this trade-off carefully when designing a server-client application or installation.

Client and Server Configuration

Another factor that affects throughput performance is the TCP/IP configuration. The 6400 computer and the server must be correctly configured and tuned to achieve maximum throughput. The default configuration of the 6400 TCP/IP client has been carefully designed to achieve the optimal throughput performance for almost all situations. It is recommended that you not change the default configuration.

For file transfers, note that if your 6400 computer is doing a "get" operation to the Flash (C) drive, the transfer may be slower than a "get" to a RAM (D) drive due to the difference in the speeds of the different file systems.

Any performance tuning on a server machine depends on the specific TCP/IP software running on that machine. Intermec cannot advise on the specific settings. As a general rule, however, the server TCP/IP kernel must have the following factors for good performance:

- A sufficient number of available network connections to handle all of the simultaneous 6400 computer connections that are desired. Network connections are sometimes referred to as *sockets* or *descriptors*.

  Note that for many applications (such as FTP), two connections are required for each 6400 computer.

- A sufficient amount of adequately sized *buffers*, or memory for storing incoming data.

An adequate amount of free hard disk space and a high performance hard disk may also improve network performance.

Appendix C

6400 TCP/IP Client Bar Code Scanning

Required Hardware

Scanners enable your 6400 computer to read and interpret bar codes. You can order an integrated scanner as part of your 6400 computer, or you can attach a tethered 5-volt bar code scanner to it. Contact your Sales Representative for scanner ordering information.

Integrated Scanner

If you ordered a 6400 computer with an internal integrated scanner, you can scan data by pointing the top of your 6400 computer at the bar code and pressing the [SCAN] key. A scanning handle is optional.

For instructions on using the scanner and installing the optional scanning handle, refer to the *PEN*KEY Model 6400 Hand-Held Computer User's Guide* (P/N 961-047-093). For information on BIOS interrupt support, refer to the *PEN*KEY 6400 Computer Programmer's Reference Guide* (P/N 977-054-004).

Tethered Scanner

The tethered bar code scanner attaches to your 6400 computer at the 9-pin D-sub connector on the bottom of the optional communication adapter endcap (P/N 705-368-001). Tethered scanners are powered by your 6400 computer. For instructions on using the scanner, refer to the documentation you received with it.

Required Software

DOS scanning for your 6400 Computer is described in detail in the *PEN*KEY 6400 Computer Programmer's Reference Guide* (P/N 977-054-004). The programmer's guide includes information about scanning methods, required files, and scanning engine configuration values.

Appendix D

RFC 1156, Section 6

```
Definitions

                RFC1156-MIB

                DEFINITIONS ::= BEGIN

                IMPORTS
                        mgmt, OBJECT-TYPE, NetworkAddress, IpAddress,
                        Counter, Gauge, TimeTicks
                            FROM RFC1155-SMI;

                  mib        OBJECT IDENTIFIER ::= { mgmt 1 }

                  system     OBJECT IDENTIFIER ::= { mib 1 }
                  interfaces OBJECT IDENTIFIER ::= { mib 2 }
                  at         OBJECT IDENTIFIER ::= { mib 3 }

                  ip         OBJECT IDENTIFIER ::= { mib 4 }
                  icmp       OBJECT IDENTIFIER ::= { mib 5 }
                  tcp        OBJECT IDENTIFIER ::= { mib 6 }
                  udp        OBJECT IDENTIFIER ::= { mib 7 }
                  egp        OBJECT IDENTIFIER ::= { mib 8 }

                  -- object types

                  -- the System group

                  sysDescr OBJECT-TYPE
                          SYNTAX  OCTET STRING
                          ACCESS  read-only
                          STATUS  mandatory
                          ::= { system 1 }

                  sysObjectID OBJECT-TYPE
                          SYNTAX  OBJECT IDENTIFIER
                          ACCESS  read-only
                          STATUS  mandatory
                          ::= { system 2 }
```

```
sysUpTime OBJECT-TYPE
        SYNTAX  TimeTicks
        ACCESS  read-only
        STATUS  mandatory
        ::= { system 3 }

-- the Interfaces group

ifNumber OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        ::= { interfaces 1 }

-- the Interfaces table

ifTable OBJECT-TYPE
        SYNTAX  SEQUENCE OF IfEntry
        ACCESS  read-write
        STATUS  mandatory
        ::= { interfaces 2 }

ifEntry OBJECT-TYPE
        SYNTAX  IfEntry
        ACCESS  read-write
        STATUS  mandatory
        ::= { ifTable 1 }

IfEntry ::= SEQUENCE {
    ifIndex
        INTEGER,
    ifDescr
        OCTET STRING,
    ifType
        INTEGER,
    ifMtu
        INTEGER,
    ifSpeed
        Gauge,
    ifPhysAddress
        OCTET STRING,
    ifAdminStatus
        INTEGER,
    ifOperStatus
        INTEGER,
    ifLastChange
        TimeTicks,
    ifInOctets
        Counter,
    ifInUcastPkts
        Counter,
```

```
    ifInNUcastPkts
        Counter,
    ifInDiscards
        Counter,
    ifInErrors
        Counter,
    ifInUnknownProtos
        Counter,
    ifOutOctets
        Counter,
    ifOutUcastPkts
        Counter,
    ifOutNUcastPkts
        Counter,
    ifOutDiscards
        Counter,
    ifOutErrors
        Counter,
    ifOutQLen
        Gauge
}

ifIndex OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 1 }

ifDescr OBJECT-TYPE
        SYNTAX  OCTET STRING
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 2 }

ifType OBJECT-TYPE
        SYNTAX  INTEGER {
                other(1),     -- none of the following
                regular1822(2),
                hdh1822(3),
                ddn-x25(4),
                rfc877-x25(5),
                ethernet-csmacd(6),
                iso88023-csmacd(7),
                iso88024-tokenBus(8),
                iso88025-tokenRing(9),
                iso88026-man(10),
                starLan(11),
                proteon-10MBit(12),
                proteon-80MBit(13),
                hyperchannel(14),
                fddi(15),
                lapb(16),
```

```
                    sdlc(17),
                    t1-carrier(18),
                    cept(19),
                    basicIsdn(20),
                    primaryIsdn(21),
                                    -- proprietary serial
                    propPointToPointSerial(22)
                }
            ACCESS  read-only
            STATUS  mandatory
            ::= { ifEntry 3 }

    ifMtu OBJECT-TYPE
            SYNTAX  INTEGER
            ACCESS  read-only
            STATUS  mandatory
            ::= { ifEntry 4 }

    ifSpeed OBJECT-TYPE
            SYNTAX  Gauge
            ACCESS  read-only
            STATUS  mandatory
            ::= { ifEntry 5 }

    ifPhysAddress OBJECT-TYPE
            SYNTAX  OCTET STRING
            ACCESS  read-only
            STATUS  mandatory
            ::= { ifEntry 6 }

    ifAdminStatus OBJECT-TYPE
            SYNTAX  INTEGER {
                    up(1),          -- ready to pass packets
                    down(2),
                    testing(3)      -- in some test mode
                    }
            ACCESS  read-write
            STATUS  mandatory
            ::= { ifEntry 7 }

    ifOperStatus OBJECT-TYPE
            SYNTAX  INTEGER {
                    up(1),          -- ready to pass packets
                    down(2),
                    testing(3)      -- in some test mode
                    }
            ACCESS  read-only
            STATUS  mandatory
            ::= { ifEntry 8 }
```

```
ifLastChange OBJECT-TYPE
        SYNTAX  TimeTicks
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 9 }

ifInOctets OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 10 }

ifInUcastPkts OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::=  { ifEntry 11 }

ifInNUcastPkts OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 12 }

ifInDiscards OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 13 }

ifInErrors OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 14 }

ifInUnknownProtos OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 15 }

ifOutOctets OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 16 }
```

```
ifOutUcastPkts OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 17 }

ifOutNUcastPkts OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 18 }

ifOutDiscards OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 19 }

ifOutErrors OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 20 }

ifOutQLen OBJECT-TYPE
        SYNTAX  Gauge
        ACCESS  read-only
        STATUS  mandatory
        ::= { ifEntry 21 }

-- the Address Translation group

atTable OBJECT-TYPE
        SYNTAX  SEQUENCE OF AtEntry
        ACCESS  read-write
        STATUS  mandatory
        ::= { at 1 }

atEntry OBJECT-TYPE
        SYNTAX  AtEntry
        ACCESS  read-write
        STATUS  mandatory
        ::= { atTable 1 }

AtEntry ::= SEQUENCE {
    atIfIndex
        INTEGER,
    atPhysAddress
        OCTET STRING,
    atNetAddress
        NetworkAddress
}
```

```
atIfIndex OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-write
        STATUS  mandatory
        ::= { atEntry 1 }

atPhysAddress OBJECT-TYPE
        SYNTAX  OCTET STRING
        ACCESS  read-write
        STATUS  mandatory
        ::= { atEntry 2 }

atNetAddress OBJECT-TYPE
        SYNTAX  NetworkAddress
        ACCESS  read-write
        STATUS  mandatory
        ::= { atEntry 3 }

-- the IP group

ipForwarding OBJECT-TYPE
        SYNTAX  INTEGER {
      gateway(1), -- entity forwards datagrams
      host(2)     -- entity does NOT forward datagrams
                }
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 1 }

ipDefaultTTL OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-write
        STATUS  mandatory
        ::= { ip 2 }

ipInReceives OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 3 }

ipInHdrErrors OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 4 }

ipInAddrErrors OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 5 }
```

```
ipForwDatagrams OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 6 }

ipInUnknownProtos OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 7 }

ipInDiscards OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 8 }

ipInDelivers OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 9 }

ipOutRequests OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 10 }

ipOutDiscards OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 11 }

ipOutNoRoutes OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 12 }

ipReasmTimeout OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 13 }
```

```
ipReasmReqds OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 14 }

ipReasmOKs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 15 }

ipReasmFails OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 16 }

ipFragOKs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 17 }

ipFragFails OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 18 }

ipFragCreates OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 19 }

-- the IP Interface table

ipAddrTable OBJECT-TYPE
        SYNTAX  SEQUENCE OF IpAddrEntry
        ACCESS  read-only
        STATUS  mandatory
        ::= { ip 20 }

ipAddrEntry OBJECT-TYPE
        SYNTAX  IpAddrEntry
        ACCESS  read-only
        STATUS  mandatory
        ::= { ipAddrTable 1 }
```

```
IpAddrEntry ::= SEQUENCE {
    ipAdEntAddr
        IpAddress,
    ipAdEntIfIndex
        INTEGER,
    ipAdEntNetMask
        IpAddress,
    ipAdEntBcastAddr
        INTEGER
}

ipAdEntAddr OBJECT-TYPE
        SYNTAX  IpAddress
        ACCESS  read-only
        STATUS  mandatory
        ::=  { ipAddrEntry 1 }

ipAdEntIfIndex OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        ::=  { ipAddrEntry 2 }

ipAdEntNetMask OBJECT-TYPE
        SYNTAX  IpAddress
        ACCESS  read-only
        STATUS  mandatory
        ::=  { ipAddrEntry 3 }

ipAdEntBcastAddr OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        ::= { ipAddrEntry 4 }

-- the IP Routing table

ipRoutingTable OBJECT-TYPE
        SYNTAX  SEQUENCE OF IpRouteEntry
        ACCESS  read-write
        STATUS  mandatory
        ::= { ip 21 }

ipRouteEntry OBJECT-TYPE
        SYNTAX  IpRouteEntry
        ACCESS  read-write
        STATUS  mandatory
        ::= { ipRoutingTable 1 }
```

```
IpRouteEntry ::= SEQUENCE {
    ipRouteDest
        IpAddress,
    ipRouteIfIndex
        INTEGER,
    ipRouteMetric1
        INTEGER,
    ipRouteMetric2
        INTEGER,
    ipRouteMetric3
        INTEGER,
    ipRouteMetric4
        INTEGER,
    ipRouteNextHop
        IpAddress,
    ipRouteType
        INTEGER,
    ipRouteProto
        INTEGER,
    ipRouteAge
        INTEGER
}

ipRouteDest OBJECT-TYPE
        SYNTAX  IpAddress
        ACCESS  read-write
        STATUS  mandatory
        ::= { ipRouteEntry 1 }

ipRouteIfIndex  OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-write
        STATUS  mandatory
        ::= { ipRouteEntry 2 }

ipRouteMetric1 OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-write
        STATUS  mandatory
        ::= { ipRouteEntry 3 }

ipRouteMetric2 OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-write
        STATUS  mandatory
        ::= { ipRouteEntry 4 }
```

```
ipRouteMetric3 OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-write
        STATUS  mandatory
        ::= { ipRouteEntry 5 }

ipRouteMetric4 OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-write
        STATUS  mandatory
        ::= { ipRouteEntry 6 }

ipRouteNextHop OBJECT-TYPE
        SYNTAX  IpAddress
        ACCESS  read-write
        STATUS  mandatory
        ::= { ipRouteEntry 7 }

ipRouteType OBJECT-TYPE
        SYNTAX  INTEGER {
          other(1),       -- none of the following
          invalid(2),     -- an invalidated route

                          -- route to directly

          direct(3),      -- connected (sub-)network

                          -- route to a non-local
          remote(4),      -- host/network/sub-network
            }
        ACCESS  read-write
        STATUS  mandatory
        ::= { ipRouteEntry 8 }

ipRouteProto OBJECT-TYPE
        SYNTAX  INTEGER {
          other(1),     -- none of the following

                        -- non-protocol information
                        --   e.g., manually
          local(2),     --   configured entries

                        -- set via a network
          netmgmt(3),   --   management protocol

                        -- obtained via ICMP,
          icmp(4),      --   e.g., Redirect

                        -- the following are
                        -- gateway routing protocols
          egp(5),
          ggp(6),
```

```
            hello(7),
            rip(8),
            is-is(9),
            es-is(10),
            ciscoIgrp(11),
            bbnSpfIgp(12),
            oigp(13)
              }
          ACCESS  read-only
          STATUS  mandatory
          ::= { ipRouteEntry 9 }

ipRouteAge OBJECT-TYPE
          SYNTAX  INTEGER
          ACCESS  read-write
          STATUS  mandatory
          ::= { ipRouteEntry 10 }

-- the ICMP group

icmpInMsgs OBJECT-TYPE
          SYNTAX  Counter
          ACCESS  read-only
          STATUS  mandatory
          ::= { icmp 1 }

icmpInErrors OBJECT-TYPE
          SYNTAX  Counter
          ACCESS  read-only
          STATUS  mandatory
          ::= { icmp 2 }

icmpInDestUnreachs OBJECT-TYPE
          SYNTAX  Counter
          ACCESS  read-only
          STATUS  mandatory
          ::= { icmp 3 }

icmpInTimeExcds OBJECT-TYPE
          SYNTAX  Counter
          ACCESS  read-only
          STATUS  mandatory
          ::= { icmp 4 }

icmpInParmProbs OBJECT-TYPE
          SYNTAX  Counter
          ACCESS  read-only
          STATUS  mandatory
          ::= { icmp 5 }
```

```
icmpInSrcQuenchs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 6 }

icmpInRedirects OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 7 }

icmpInEchos OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 8 }

icmpInEchoReps OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 9 }

icmpInTimestamps OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 10 }

icmpInTimestampReps OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 11 }

icmpInAddrMasks OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 12 }

icmpInAddrMaskReps OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 13 }
```

```
icmpOutMsgs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 14 }

icmpOutErrors OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 15 }

icmpOutDestUnreachs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 16 }

icmpOutTimeExcds OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 17 }

icmpOutParmProbs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 18 }

icmpOutSrcQuenchs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 19 }

icmpOutRedirects OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 20 }

icmpOutEchos OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 21 }
```

```
icmpOutEchoReps OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 22 }

icmpOutTimestamps OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 23 }

icmpOutTimestampReps OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 24 }

icmpOutAddrMasks OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 25 }

icmpOutAddrMaskReps OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { icmp 26 }

-- the TCP group

tcpRtoAlgorithm OBJECT-TYPE
        SYNTAX  INTEGER {
        other(1),    -- none of the following
        constant(2), -- a constant rto
        rsre(3),     -- MIL-STD-1778, Appendix B
        vanj(4)      -- Van Jacobson's algorithm [15]
                }
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 1 }

tcpRtoMin OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 2 }
```

```
tcpRtoMax OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 3 }

tcpMaxConn OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 4 }

tcpActiveOpens OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 5 }

tcpPassiveOpens OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 6 }

tcpAttemptFails OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 7 }

tcpEstabResets OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 8 }

tcpCurrEstab OBJECT-TYPE
        SYNTAX  Gauge
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 9 }

tcpInSegs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 10 }
```

```
tcpOutSegs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 11 }

tcpRetransSegs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 12 }

-- the TCP connections table

tcpConnTable OBJECT-TYPE
        SYNTAX  SEQUENCE OF TcpConnEntry
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcp 13 }

tcpConnEntry OBJECT-TYPE
        SYNTAX  TcpConnEntry
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcpConnTable 1 }

TcpConnEntry ::= SEQUENCE {
    tcpConnState
        INTEGER,
    tcpConnLocalAddress
        IpAddress,
    tcpConnLocalPort
        INTEGER (0..65535),
    tcpConnRemAddress
        IpAddress,
    tcpConnRemPort
        INTEGER (0..65535)
}

tcpConnState OBJECT-TYPE
        SYNTAX  INTEGER {
                    closed(1),
                    listen(2),
                    synSent(3),
                    synReceived(4),
                    established(5),
                    finWait1(6),
                    finWait2(7),
                    closeWait(8),
                    lastAck(9),
                    closing(10),
                    timeWait(11)
```

```
                }
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcpConnEntry 1 }

tcpConnLocalAddress OBJECT-TYPE
        SYNTAX  IpAddress
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcpConnEntry 2 }

tcpConnLocalPort OBJECT-TYPE
        SYNTAX  INTEGER (0..65535)
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcpConnEntry 3 }

tcpConnRemAddress OBJECT-TYPE
        SYNTAX  IpAddress
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcpConnEntry 4 }

tcpConnRemPort OBJECT-TYPE
        SYNTAX  INTEGER (0..65535)
        ACCESS  read-only
        STATUS  mandatory
        ::= { tcpConnEntry 5 }

-- the UDP group

udpInDatagrams OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { udp 1 }

udpNoPorts OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { udp 2 }

udpInErrors OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { udp 3 }
```

```
udpOutDatagrams OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { udp 4 }

-- the EGP group

egpInMsgs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { egp 1 }

egpInErrors OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { egp 2 }

egpOutMsgs OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { egp 3 }

egpOutErrors OBJECT-TYPE
        SYNTAX  Counter
        ACCESS  read-only
        STATUS  mandatory
        ::= { egp 4 }

-- the EGP Neighbor table

egpNeighTable OBJECT-TYPE
        SYNTAX  SEQUENCE OF EgpNeighEntry
        ACCESS  read-only
        STATUS  mandatory
        ::= { egp 5 }

egpNeighEntry OBJECT-TYPE
        SYNTAX  EgpNeighEntry
        ACCESS  read-only
        STATUS  mandatory
        ::= { egpNeighTable 1 }

EgpNeighEntry ::= SEQUENCE {
    egpNeighState
        INTEGER,
    egpNeighAddr
        IpAddress
}
```

```
egpNeighState OBJECT-TYPE
        SYNTAX  INTEGER {
                    idle(1),
                    acquisition(2),
                    down(3),
                    up(4),
                    cease(5)
                }
        ACCESS  read-only
        STATUS  mandatory
        ::= { egpNeighEntry 1 }

egpNeighAddr OBJECT-TYPE
        SYNTAX  IpAddress
        ACCESS  read-only
        STATUS  mandatory
        ::= { egpNeighEntry 2 }

END
```

INDEX

C

D

I

K

L

M

N

O

P

R

S

T

U

V

W